МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Одеський національний політехнічний університет

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ МЕТОДИ В МОДЕЛЮВАННІ

INFORMATICS AND MATHEMATICAL METHODS IN SIMULATION

Том 8, № 4

Volume 8, No. 4

Одеса – 2018
Odesa – 2018

Журнал внесений до переліку наукових фахових видань України
(технічні науки)
згідно наказу Міністерства освіти і науки України № 463 від 25.04.2013 р.

Виходить 4 рази на рік

Заснований Одеським національним політехнічним університетом у 2011 році

Свідоцтво про державну реєстрацію КВ № 17610 - 6460Р від 04.04.2011р.

Published 4 times a year

Founded by Odessa National Polytechnic University in 2011

Certificate of State Registration KB № 17610 - 6460P of 04.04.2011

Друкується за рішенням редакційної колегії та Вченої ради Одеського національного політехнічного університету

Оригінал-макет виготовлено редакцією журналу

Адреса редакції: просп. Шевченка, 1, Одеса, 65044, Україна
Телефон: +38 048 705 8506
Web: http://immm.opu.ua E-mail: immm.ukraine@gmail.com

Editorial address: 1 Shevchenko Ave., Odessa, 65044, Ukraine
Tel.: +38 048 705 8506
Web: http://immm.opu.ua E-mail: immm.ukraine@gmail.com

ЗМІСТ / CONTENTS

УДК 681.514:621.029

Informatics and Mathematical Methods in Simulation
Vol. 8 (2018), No. 4, pp. 279-284

METHOD FOR DETECTING SHARPNESS AS A DIGITAL IMAGE POST-PROCESSING

V.V. Zorilo, P.S. Safronov, O.Yu. Lebedieva, I.V. Zorilo

Odessa National Polytechnic University,
1, Shevchenko avenue, Odessa, 65044, Ukraine; e-mail: vikazorilo@gmail.com, p.s.safronov@gmail.com, whiteswanhelena@gmail.com, zoriloi67@gmail.com

Due to the growth of computer crime, an important and urgent problem is the development of methods for detecting the integrity violations of a digital image. In particular, the detection of different types of the image post-processing after their possible forgery is a grey area of information security, and the detection of processing by the Sharpen Filter is an issue practically not covered in open scientific literature. The artificial sharpening of a digital image is the reverse procedure to the blurring. Previously, the authors of the paper developed the method for detecting blur of a digital image based on an analysis of the growth rate of singular values. When blurring, the growth rate of singular values is an order of magnitude smaller than before the blurring, which makes it possible to reveal a threshold value for detecting blurred images. The singular values increase accordingly to the artificially sharpening. But it is not possible to reveal the threshold value in this case. The aim of this paper is to identify the parameters of the digital image matrix, which indicate an artificial sharpening, and to develop a method for detecting sharpness as a digital image post-processing. If the contour is considered as a change in the brightness function of a digital image, then the change in the brightness function will be faster when the contours are sharpened. If two adjacent pixels had the close sharpness values before sharpening, then applying this filter will increase the difference between them. In this paper, the investigation of the close color pairs of an image is carried out when the Sharpness Filter was applied to it. It is revealed that the number of close color pairs during processing decreases. The threshold value which allows separating the processed image from the raw one is empirically established. The method of detecting sharpness as a digital image post-processing is developed based on the results obtained.

Keywords: analysis of color pairs, sharpness, digital image, image processing, image forgery.

Introduction

The use of digital images occurs in all spheres of human activity. Modern means of image processing, both in order to improve their perception, and to conceal possible unauthorized interference (forging, using a digital image (DI) as a steganographic container, etc.) are widely available and easy to use. This fact leads to the need to improve existing methods for detecting integrity violations of the digital images, as well as to create the new methods. Sharpening is one of the possible tools for a digital image post-processing in case of the image integrity violation. There are many articles on how to estimate the degree of sharpness of a digital image [1…3], but there are no any researches on how to identify an artificial increase in sharpness with a graphic editor. Along with such a tool as image blur, which was previously studied in [4 ... 5], sharpness affects mainly the contours of a digital image. At the moment, the problem of detecting sharpening by means of graphic editors is practically not covered in the sources available in the open scientific literature. In [6], a computing experiment, where the singular values of blocks of digital image matrices are used as the analyzed parameters, is carried out. This tool was chosen for the reasons described in [7], as well as in many other papers of the author. As a result of the experiment, it was established that the application of Sharpen Tool to an image, like the application of Blur Tool, affects the growth rate of singular values, namely, it is established that the growth rate

increases. However, studies have led to the fact that the analysis of the growth rate of the corresponding image parameters, which gave positive results for detecting blurring, did not lead to success in detecting sharpness since it is in principle not possible to identify the threshold value that allows separating the processed image from the raw one. This indicates the need to search for a tool the sensitivity of which would allow developing a method for detecting sharpness as a forged image post-processing.

The aim of the paper is to identify the parameters of the digital image matrix, which indicate an artificial increase in the sharpness of an image, and to develop a method for detecting sharpness as a digital image post-processing.

Related works

As already noted, the sharpness affects mainly the high-frequency component of the digital image signal. In fact, sharpness is nothing more than an increase in the difference between the brightness values of adjacent pixels. This means that if adjacent pixels (color pairs) could be close to or equal in brightness values before processing, then the number of such pairs will be much less after processing. Earlier, color pairs were studied for images for steganographic analysis, where an image was considered as a steganographic container [8]. In this paper, such terms as “close color pairs” and “unique color pairs” are used.

In the context of the problem addressed, the definition of a close color pair is introduced by analogy with [8]. The two colors (R_1, G_1, B_1) and (R_2, G_2, B_2) will be considered close color pair if they belong to the pixels which sequentially arranged vertically or horizontally, and satisfy the following condition:

$$(R_1 - R_2) + (G_1 - G_2) + (B_1 - B_2) \le 3. \quad (1)$$

An experiment in which the effect of sharpness on the change in the number of close color pairs in the analyzed images was conduct. For the experiment, 300 jpeg images of different sizes from the NRSC image database were used [9]. Each image was processed using Adobe Photoshop graphic editor, namely, the Gaussian Sharpen Filter with a radius of 1 pixel. This corresponds to the least noticeable sharpening and, accordingly, the most difficult to detect situation. The result was saved in jpeg format with a maximum quality factor, that is, with minimal compression. For convenience, the image was split into a standard 16 × 16 block size. The number of close color pairs (CCPs) was found before and after processing for each block. Some of the experimental results are presented in table 1, where all the blocks taken belong to different images.

As you can see, the assumption about the reduction of close color pairs under the effect of the Gaussian Sharpen Filter is confirmed by a computing experiment. Consider these indicators relative to the total number of color pairs in the block, which we define as follows. Let F be an n×n-block of the DI matrix. Then the total number of color pairs S in the block is determined by the formula:

$$S = 2n(n-1).$$

Also the ratio *(K)* of the number of close color pairs *(P)* to the total number of color pairs in the block:

$$K = \frac{P}{S}. \quad (2)$$

Table 1.

The Effect of Sharpening on the Number of Close Color Pairs in the DI Blocks

DI No.	Block size	Number of CCPs before processing	Number of CCPs after processing
1	16×16	232	79
2	16×16	227	75
3	16×16	252	55
4	16×16	97	33
5	16×16	209	47
6	16×16	276	80
7	16×16	232	67
8	16×16	297	73
9	16×16	181	38
10	16×16	118	29
11	16×16	388	216
12	16×16	373	217
13	16×16	66	22
14	16×16	450	324
15	16×16	189	77
16	16×16	212	96
17	16×16	112	42
18	16×16	239	114
19	16×16	164	58
20	16×16	102	30

The results of the calculations are shown in the table 2.

By analyzing the obtained ratios before and after processing, it was established that the average value of the ratios of the number of close color pairs before processing to the total number of color pairs in a block is $K_b = 0,5$, in turn, the average value of these relations after processing is $K_a = 0,2$. Consider the threshold value of 0.35 as the median for the average values obtained. The number of errors of the first kind (skipping the processed image) is 20%. But at the same time the number of errors of the second kind (false alarm) reaches 32%. It was established experimentally that the optimal value is a threshold value of 0.3.In this case, the errors of the first kind do not increase, and the errors of the second kind decrease and amount to 20%.

The method for detecting sharpness as a digital image processing is proposed based on the research data. The main steps of the method are presented below.

Let A be the analyzed color digital image, where *R*, *G*, *B* are the m × n matrices of the red, green, and blue components of the image, respectively.

Step 1. The matrices *R*, *G*, *B* is split into 16 × 16 blocks in a standard manner.

Step 2. For the each block, the number of close color pairs *P* is found by expression (1).

Step 3. For the each block, the ratio of the number of close color pairs to the total number of color pairs is found by expression (2).

Step 4. The average value of the coefficients K_{avg} obtained at the previous stage is founded.

Step 5. If a

K_{avg} *<0,3, then*

The image is considered a processed by Gaussian Sharpen Filter, Otherwise, the image is not processed by the Gaussian Sharpen Filter.

Table 2.

Calculation Results

No.	Block size	Total number of pairs	Number of CCPs before processing	Ratio of CCPs to S before processing (K_b)	The number of CCPs after processing	Ratio of CCPs colors to S after processing (K_a)
1	16×16	480	232	0.48333333	79	0.16458333
2	16×16	480	227	0.47291667	75	0.15625000
3	16×16	480	252	0.52500000	55	0.11458333
4	16×16	480	97	0.20208333	33	0.06875000
5	16×16	480	209	0.43541667	47	0.09791667
6	16×16	480	276	0.57500000	80	0.16666667
7	16×16	480	232	0.48333333	67	0.13958333
8	16×16	480	297	0.61875000	73	0.15208333
9	16×16	480	181	0.37708333	38	0.07916667
10	16×16	480	118	0.24583333	29	0.06041667
11	16×16	480	388	0.80833333	216	0.45000000
12	16×16	480	373	0.77708333	217	0.45208333
13	16×16	480	66	0.13750000	22	0.04583333
14	16×16	480	450	0.93750000	325	0.67708333
15	16×16	480	189	0.39375000	77	0.16041667
16	16×16	480	212	0.44166667	96	0.20000000
17	16×16	480	112	0.23333333	42	0.08750000
18	16×16	480	239	0.49791667	114	0.23750000
19	16×16	480	164	0.34166667	58	0.12083333
20	16×16	480	102	0.21250000	30	0.06250000

Conclusions

In this paper, the question of the behavior of close pair pairs of image is investigated in a situation when an image is processed by means of a graphic editor. The Gaussian Sharpen Filter was selected as an impact on the image. In the course of research it was revealed that the number of close color pairs decreases during the processing of the said filter. And also the threshold value which allows separating the processed image from the raw one is empirically revealed. Based on the results, the method for detecting sharpness as a post-processing of a digital image is developed .The developed method has following features: images before and

after processing must be saved in jpeg format, otherwise it is extremely difficult to reveal a threshold value. The number of errors of the first kind, as well as the number of errors of the second kind, is 20%.

The efforts of the authors are currently aimed at conducting additional research in order to improve the developed method.

References

1. Kanjar, De. Image Sharpness Measure for Blurred Images in Frequency Domain / De. Kanjar, V. Masilamani // Procedia Engineering. – 2013. – No. 64. – Pp. 149-158.
2. Ashirbani, S. High frequency content based framework for perceptual sharpness assessment in natural images / S. Ashirbani, Q.M. Jonathan Wu // International Conference on Computers, Communications and Systems (ICCCS). – 2015. – Pp.1-13.
3. Hassen, R. Image Sharpness Assessment Based on Local Phase Coherence / R. Hassen, Z. Wang, M. Salama // IEEE Transactions on Image Processing. – 2013. – Vol. 22, No. 7. – Pp. 2798-2810.
4. Зорило, В.В. Методы повышения эффективности выявления нарушения целостности цифрового изображения / В.В. Зорило // Науково-технічний збірник «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні». – 2013. – №1(25). – С. 75-81.
5. Zorilo, V.V. Detection of digital image blurring traces / V.V. Zorilo, V.A. Mokritskiy // Informatics and mathematical methods in simulation. – 2012. – No. 3. – Pp. 220-226.
6. Зорило, В.В. Влияние повышения резкости на математические параметры цифрового изображения / В.В. Зорило, Е.Ю. Лебедева, А.И. Матвеева, А.А. Ефименко, В.А. Мокрицкий // Сучасна спеціальна техніка. – 2017. – № 2. – С. 67-73.
7. Кобозева, А.А. Основы общего подхода к решению проблемы обнаружения фальсификации цифрового сигнала / А.А. Кобозева // Електромашинобудування та електрообладнання. – 2009. – № 72. – С. 35-41.
8. Узун, И.А. Стеганоанализ цифровых изображений, хранящихся в произвольных форматах / И.А. Узун // Информатика и математические методы в моделировании. – 2013. – Том 3, № 2. – С. 179-189.
9. NRCS Photo Gallery. Mode of access: https://photogallery.sc.egov.usda.gov/res/sites/PhotoGallery/index.html.

МЕТОД ВИЯВЛЕННЯ РІЗКОСТІ ЯК ПОСТОБРОБКИ ЦИФРОВОГО ЗОБРАЖЕННЯ

В.В. Зоріло, П.С. Сафронов, О.Ю. Лебедєва, І.В. Зоріло

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: vikazorilo@gmail.com,
p.s.safronov@gmail.com, whiteswanhelena@gmail.com, zoriloi67@gmail.com

Розробка методів виявлення порушень цілісності цифрових зображень є важливою і актуальною задачею у зв'язку з ростом комп'ютерної злочинності. Зокрема, виявлення різних видів постобработки зображень після їх можливої фальсифікації – мало розкрита область захисту інформації, а виявлення обробки фільтром «різкість» – практично неосвітлене питання у літературі. Штучне підвищення різкості цифрового зображення – процедура, зворотна розмиттю. Раніше авторами статті було розроблено метод виявлення розмиття цифрового зображення, заснований на аналізі швидкості росту сингулярних чисел. При розмитті швидкість росту сингулярних чисел на порядок менша, ніж до розмиття, що дозволяє виділити порогове значення для виявлення розмитих зображень. При штучному підвищенні різкості сингулярні числа, відповідно, збільшуються. Але виділити порогове значення в цьому випадку не є можливим. Мета даної роботи – виявлення параметрів матриці цифрового зображення, які вказують на штучне підвищення його різкості, і розробка методу виявлення різкості як постобработки цифрового зображення. Якщо розглядати контур як зміну функції яскравості зображення у цифровому форматі, то при підвищенні різкості контурів функція яскравості буде змінюватись швидше. Якщо два пікселі, що розташовані один біля одного, до підвищення різкості мали близькі значення, то застосування даного фільтру збільшить різницю між ними. В

роботі проведені дослідження близьких пар кольорів зображення під впливом на нього фільтру «Різкість». Виявлено, що кількість близьких пар кольорів після обробки зменшується. Емпірично встановлено порогове значення, що дозволяє відокремити оброблене зображення від необробленого. На основі отриманих результатів розроблено метод виявлення різкості як постобробки цифрового зображення.
Ключові слова: аналіз пар кольорів, різкість, цифрове зображення, обробка зображення, фальсифікація зображення.

МЕТОД ВЫЯВЛЕНИЯ РЕЗКОСТИ КАК ПОСТОБРАБОТКИ ЦИФРОВОГО ИЗОБРАЖЕНИЯ

В.В. Зорило, П.С. Сафронов, О.Ю. Лебедева, И.В. Зорило

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одеса, 65044, Украина; e-mail: vikazorilo@gmail.com,
p.s.safronov@gmail.com, whiteswanhelena@gmail.com , zoriloi67@gmail.com

Разработка методов выявления нарушений целостности цифровых изображений является важной и актуальной задачей в связи с ростом компьютерной преступности. В частности, выявление разных видов постобработки изображений после их возможной фальсификации – мало раскрытая область защиты информации, а выявление обработки фильтром «резкость» – практически неосвещенный вопрос в открытой литературе. Искусственное повышение резкости цифрового изображения – процедура, обратная размытию. Ранее авторами статьи был разработан метод выявления размытия цифрового изображения, основанный на анализе скорости роста сингулярных чисел. При размытии скорость роста сингулярных чисел на порядок меньше, чем до размытия, что позволяет выделить пороговое значение для выявления размытых изображений. При искусственном повышении резкости сингулярные числа, соответственно, увеличиваются. Но выделить пороговое значение в этом случае не представляется возможным. Цель данной работы – выявление параметров матрицы цифрового изображения, указывающих на искусственное повышение его резкости, и разработка метода выявления резкости как постобработки цифрового изображения. Если рассматривать контур как изменение функции яркости цифрового изображения, то при повышении резкости контуров изменение функции яркости будет происходить быстрее. Если два рядом стоящих пикселя до повышения резкости имели близкие значения, то применение данного фильтра увеличит разницу между ними. В работе проведены исследования близких пар цветов изображения под воздействием на него фильтром «Резкость». Выявлено, что количество близких пар цветов при обработке уменьшается. Эмпирически установлено пороговое значение, позволяющее отделить обработанное изображение от необработанного. На основе полученных результатов разработан метод выявления резкости как постобработки цифрового изображения.
Ключевые слова: анализ пар цветов, резкость, цифровое изображение, обработка изображения, фальсификация изображения.

УДК 681.323

Informatics and Mathematical Methods in Simulation
Vol. 8 (2018), No. 4, pp. 285-294

ПРОВЕРКА ПРАВИЛЬНОСТИ ПРИНЯТИЯ РЕШЕНИЙ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ ПРИ РАСПОЗНОВАНИИ ОБЪЕКТОВ

В.О. Хорошко[1], Ю.Е. Хохлачева[1], С.В. Калантаевская[2]

[1]Национальный авиационный университет,
пр-т Космонавта Комарова, 1, Киев, 03058, Украина;
[2]Военный институт телекоммуникаций та информатизации,
ул. Московская, 45/1, Киев, 01011, Украина;
e-mail: professor_va@ukr.net, hohlachova@gmail.com

В данной работе предлагается решение задачи оптимизации процессов обработки поступающей информации с беспилотных летательных аппаратов (БПЛА) для распознавания объектов при отсутствии необходимого объема исходной информации. Предложенные частные методы распознавания объектов можно легко реализовать на средствах вычислительной техники, которые располагаются как на борту БПЛА, так и на наземном пункте. Эти методы позволяют оперативно получать ответ на правильность принятых решений относительно разведываемого объекта. При практическом построении систем распознавания, которые используются в БПЛА, необходимо применять большие массивы данных о признаках объектов. Построение логических систем распознавания объектов, содержащих большое число классов и признаков, и оценка их эффективности связаны со значительными трудностями. Наиболее существенным показателем эффективности системы распознавания является вероятность правильного решения ею задач распознавания неизвестных объектов. При прочих равных условиях, в частности, в условиях оптимальной обработки апостериорной информации, величина этого показателя тем выше, чем больший объем поступающей информации используется при распознавании данного объекта. Более того, при определенных ограничениях, накладываемых признаками, используемыми при распознавании, возрастает и увеличивается вероятность однозначного решения задачи распознавания. Реализация приоритетов в области создания и применения БПЛА должна осуществляться на основе использования достижения высоких технологий и мирового опыта применения беспилотников, с учетом состояния развития национальной научно-производственной базы и реализации накопленного научно-технического и технологического потенциалов Украины в информационной, авиационной, космической, телекоммуникационной и смежных областях, наличия в Украине соответствующей инфраструктуры, а также с учетом реальных экономических, геополитических и военных требований и возможностей.

Ключевые слова: беспилотные летательные аппараты, правильность принятия решений, проверка правильности, распознавание объектов.

Введение

В настоящее время беспилотные летательные аппараты (БПЛА) являются одним из основных элементов информационно-разведывательного обеспечения и дистанционного воздействия на объекты противника во время боевых действий, а также обеспечения внутренней безопасности государства [1].

Первые разведывательные БПЛА применялись в боевых условиях США во время войны в Корее (1950-1953 гг.). Во время войны во Вьетнаме беспилотники использовались, главным образом, для аэрофотосъемки объектов на территории страны: населенных пунктов, позиций подразделений противовоздушной обороны, мостов и т.п. [2].

Реальным способом ведения воздушной разведки, которая отвечает современным требованиям, стали только БПЛА второго поколения. Их принципиальное отличие

заключается в установке на них портативных телекамер и возможности продолжительное время патрулировать требуемый район, передавая на наземный пункт как общую картинку местности, так и картины отдельных участков для более детального обследования. Круг задач, которые решали БПЛА, расширился с применением оптико-электронной разведки. Этапу способствовало наличие на борту БПЛА различного разведывательного оборудования: телевизионных камер, аэрофотоаппарата, ИК-камер лазерного дальномера-целеуказателя, аппаратуры постановки помех и аппаратуры обработки информации [2].

Дальнейшее применение БПЛА было осуществлено Израилем в ходе ливанского военного конфликта (1982 г.) и США «Буря в Пустыне» в зоне Персидского залива (1991 г.).

Если в операции «Буря в пустыне» разведывательные БПЛА все еще применялись эпизодично, то в небе Югославии они уже играли одну из важных ролей по сбору и верификации информации.

Наиболее характерными чертами операции «Свобода Ирана» (2003 г.) было комплексное широкомасштабное применение БПЛА с задачами избирательных ударов и локализации наземных объектов, которые подлежали сохранению (нефтепромыслы) [2].

Следует отметить широкое применение БПЛА на юго-востоке Украины как вооруженными силами Украины, так и российскими наемниками. При этом современные БПЛА должны отвечать требованиям, исходя из прогнозируемых перспективных операций, и обязательно оцениваться на предмет возможности использования во всех структурах государства. По мнению экспертов, выполнение таких требований позволит значительно повысить эффективность боевого применения БПЛА.

Важными акцентами развития БПЛА является [2,3]:

- развитие и усовершенствование систем видеоизображения;
- разработка бортовых систем обработки и передачи информации;
- разработка систем обработки информации в наземных пунктах;
- разработка и внедрение новых концепций, которые обеспечат информацией, достаточной для принятия решений.

Эффективность БПЛА значительно зависит от качества подсистемы информационного обмена, которая в реальном масштабе времени должна осуществлять формирование и передачу информационных потоков, которые включают в себя видеосигналы (статических и динамических изображений), а также команды управления. По качеству видеоизображения и по реально достигаемому разрешению видеосигнала современные БПЛА приближаются к интеллектуальным компьютерным системам, что позволяет создать очень гибкие системы обеспечения информацией операторов и приблизиться по своим функциям и возможностям к системам поддержки принятия решений [1,4,5].

Построение и функционирование систем распознавания объектов связано с накоплением и анализом априорной информации. Анализ характера задачи распознавания объектов, когда характер признаков вероятностный, т.е. когда между признаками объектов и классами, к которым они могут быть отнесены, существуют вероятностные связи, может быть основан на результатах теории статистических решений. При полной исходной информации эти результаты могут быть использованы непосредственно. При неполной исходной информации распознавание может быть основано на результатах теории статистических решений, хотя в данном случае эти результаты могут быть использованы лишь путем реализации процедуры самообучения [6]. При практическом построении систем распознавания, которые используются в БПЛА, необходимо применять большие массивы данных о признаках объектов. Построение логических систем распознавания объектов, содержащих большое число

классов и признаков, и оценка их эффективности связаны со значительными трудностями.

Наиболее существенным показателем эффективности системы распознавания является вероятность правильного решения ею задач распознавания неизвестных объектов. При прочих равных условиях, в частности, в условиях оптимальной обработки апостериорной информации, величина этого показателя тем выше, чем больший объем поступающей информации используется при распознавании данного объекта. Более того, при определенных ограничениях, накладываемых признаками, используемыми при распознавании, возрастает и увеличивается вероятность однозначного решения задачи распознавания [6,7].

Цель работы

Целью данной работы является решение задачи оптимизации процессов распознавания различных объектов при отсутствии необходимого объема исходной информации.

Основная часть

Одним из наиболее существенных показателей применения БПЛА с бортовой цифровой системой видеонаблюдения наработки (ЦСВН) является вероятность правильного распознавания неизвестного (наблюдаемого) объекта. Для решения этой задачи введем в рассмотрение следующего понятия и определения.

Пусть $\Omega = \{\omega\}$ – множество, каждый элемент ω которого – объект. Произведена классификация объектов, в результате которой множество Ω подразделено на классы $\Omega_i, i = 1, 2..., r$.

Каждый объект обладает определенной совокупностью признаков x_j, $j = 1, 2, ..., N$.

Признаки объектов могут быть определены путем предварительной обработки информации, получаемой с помощью ЦСВН: $T_\beta, \beta = 1, 2..., r$.

Для определения признаков распознаваемого объекта необходимо с помощью ЦСВН провести наблюдения. Обозначим множество наблюдений через $A = \{a\}$. Провести наблюдение a – значит указать, какой признак и с помощью какого средства необходимо определить.

Каждое наблюдение имеет определенный результат. Введем в рассмотрение множество возможных результатов $x = \{x_a\}$ (здесь x_a – общее обозначение результата наблюдения a). Результат наблюдения – определение факта либо назначения соответствующего признака объекта наблюдения, либо отсутствия объекта. Когда a является наблюдением по проверке логического признака объекта, то x_a принимает одно из трех возможных значений: 0 или 1, или Ψ, которые означают соответственно отсутствие у объекта наблюдения признака либо его наличие, а также то, что при проведении наблюдения не удалось установить у объекта наблюдения признаков, которые бы соответствовали известным признакам.

На наблюдение при помощи БПЛА накладываются определенные ограничения, которые обуславливаются рядом обстоятельств: невозможностью использования некоторых оптических систем в определенное время (ночное, туман, дождь, снег, активное электронное противодействие), выход из строя одного из технических средств или ограниченность ресурсов беспилотника, а также время проведения наблюдения.

Таким образом, на множество $A=\{a\}$ накладывается система последовательных ограничений Γ, которая, будем считать, задана, если для каждой Γ – допустимой цепочки результатов $x_{a_1}, x_{a_2}, ..., x_{ak}$, т.е. цепочки $a_1 \in A^{\Gamma}, a_2 \in A_2^{\Gamma}(x_1), ..., a_k \in A_k^{\Gamma}(x_{a_1}, ..., x_{ak-1})$, определено множество наблюдений $(k+1)$-й стадии $A_{k=1}(x_{a_1}, ..., x_{ak})$ допустимых после цепочки результатов $x_{a_1}, x_{a_2}, ..., x_{ak}$ наблюдений $a_1, a_2, ..., a_k$.

Совокупность наблюдений A, заданной системой ограничений Γ, обозначим A^{Γ}.

Информация, полученная при помощи БПЛА, обрабатывается ЦСВН и на приемном пункте при помощи алгоритма распознавания для принятия решения о принадлежности объекта наблюдения к одному из классов классификации объектов. Обозначим через $z=\{z\}$ множество окончательных решений. Оно распадается на подмножества $z_i=\{z_i^k\}$ элементы которого z_i^k означают, что после проведения k-й стадии наблюдения принято окончательное решение о принадлежности объекта к Ω_i-му классу.

Принятие окончательных решений сопряжено с определенным риском правильности принятия решения. Если проведенные наблюдения $a_1, a_2, ..., a_k$ завершились результатами $x_1, x_2, ..., x_k$, и принято окончательное решение z_i^k, то будем полагать, что величина риска принятия окончательного решения равна $C_{\omega}\left[z_i^k(x_{a_1}, x_{a_2}, ..., x_{ak})\right]$.

Введенные определения и понятия позволяют сформулировать задачу принятию решений при распознавании объектов.

Проведение наблюдений, как и принятие окончательного решения о принадлежности объекта ω к какому-либо классу, по информации, полученной в результате этих наблюдений, сопряжено с определенными расходами U_w. Величина этих расходов, усредненная по всем возможным цепочкам развития наблюдений U_0, определяется последовательным правилом R, в соответствии с которым осуществляется планирование наблюдений [7,8]: $\overline{U_w}=\overline{U_w}(R)$.

Каждое из последовательных правил R может строиться лишь с учетом ограничений Γ, накладываемых на возможность проведения наблюдений. Ввиду того, что заранее неизвестно, какой объект подвергается распознаванию, величина $\overline{U_w}$ должна быть усреднена с помощью априорной вероятности появления объектов $P(\Omega_i)$.

Качество каждого алгоритма, определяющего последовательное правило R, в соответствии с которым реализуется процесс распознавания, может быть охарактеризовано функционалом, представляющим собой математическое ожидание от величины средних расходов:

$$\overline{U}_{\bar{w}}(R)=M\left[u_w(R)\right]=\sum_i^m \overline{u_w}(R)P(\Omega_i). \qquad (1)$$

Требуется определить оптимальное правило R, обеспечивающее минимум функционала (1), т.е. минимизацию математического ожидания расходов, связанных с реализацией процесса наблюдения. В физически реализуемых системах распознавания число используемых признаков ограничено. Более того, при распознавании конкретных объектов подчас нецелесообразно использовать весь набор признаков рабочего словаря. Связано это с тем, что определение каждого признака требует проведение соответствующего обоснования и, следовательно, сопряжено с некоторыми

материальными затратами и затратами времени [9]. В то же время объекты некоторых классов могут распознаваться с заданным уровнем вероятности правильного решения при использовании лишь части признаков рабочего словаря. В подобной ситуации предельно возможное накопление информации неоправданно, а рационально процесс определения признаков распознаваемого объекта завершить в каждом конкретном случае на определенном шаге. Именно в связи с этим и возникает задача оптимизации процесса распознавания.

Решение задачи оптимизации процесса распознавания требует наличия определенных данных. В случае, когда необходимый объем исходной информации отсутствует, что имеет место в реальной жизни, приходиться пользоваться частными подходами к принятию решений. Остановимся на некоторых из них.

Первый метод. Положим, что в результате наблюдения определены значения ν признаков объекта $x_i = x_1^0, ..., x_v = x_v^0$ и установлены условные апостериорные вероятности отнесения его к классам Ω_i, $i = 1,2,...,m$, т.е. величины $P(\Omega_i / a_v)$, где $a_v = \left\{ x_1 = x_1^0, ..., x_v = x_v^0 \right\}$.

Решение о принадлежности этого объекта к тому или другому классу в соответствии с рассматриваемым критерием производится на основании соотношения

$$P\left(\Omega_i / a_v\right) \geq a_{ij} P(\Omega_j / a_v),$$

где a_{ij} – некоторые числа для какого-либо фиксированного класса i при всех $j \neq i$, $j = 1,2,...,m$.

При выполнении этого условия принимается гипотеза H_i: «Объект принадлежит классу Ω_i». Величины a_{ij} связаны с вероятностями ошибочного решения следующим образом.

Обозначим через δ_i вероятность принять гипотезу H_i, в то время, как справедлива гипотеза H_j:

$$\delta_{ij} = P(H_j / H_i). \tag{2}$$

Тогда вероятность a_{ij} отклонить гипотезу H_i, в то время, как она справедлива, равна $a_i = P\left(\frac{\bar{H}_i}{H_i}\right) = \sum_{j \neq i} \delta_{ij}$.

Так как в соответствии с принятым критерием вероятность не совершить ошибку при гипотезе H_i должна быть в a_{ij} раз больше вероятности совершить ошибку при том же условии о принятии гипотезы H_i, то $a_{ij} \leq \frac{1 - a_i}{\sum_{j \neq i} \delta_{ji}} = \frac{1 - \sum_{j \neq i} \delta_{ji}}{\delta_{ji}}$.

Пусть для каждого i-го класса величины вероятностей ошибочных решений δ_{ji} равны между собой, т.е. $\beta_{1i} = \beta_{2i} = ... = \beta_{(m-1)}$, $\beta_{1i} = a_i / (m-1)$.

Если, кроме того, положить, $a_1 = a_2 = ... = a_m = a$, то $\beta_{1i} = a / (m-1)$, $1 \leq i$, где m – число классов, для которых $P(\Omega_i / a_v) \neq 0$. Следовательно: $a_{ij} \leq (m-1)(1-a)/a$, $i \neq j$, $1 \leq i$, $j \leq m$.

Положим, что $a_{ij} \leq (m-1)(1-a)/a$.

Тогда если a_0 – выбранное значение вероятности ошибочного решения, то в соответствии с (2) гипотеза H_i принимается, когда неравенство

$$\frac{P\left(\frac{\Omega_i}{a_v}\right)}{P\left(\frac{\Omega_j}{a_v}\right)} \geq \frac{(m-1)(1-m)}{a_0}$$

выполняется для всех $j \neq i,\ 1 \leq i,\ j \leq m$. В противном случае необходимо учитывать $(v+1)$-й признак, поскольку при ν признаках не обеспечивается уровень доверительной вероятности $(1-a_0)$. Значение ошибочного решения a_0 может быть выбрано из следующих соображений. Пусть при использовании ν признаков получено r исключающих друг друга гипотез $H_j, j = 1,2,...r$. Предположим, что C_i – стоимость ошибки при принятии гипотезы H_j, и при правильном ответе плата не производится. Тогда математическое ожидание платы за одно решение будет

$$\overline{C} = \sum_{j=1}^{r} C_j a_j P\left(\frac{\Omega_i}{a_v}\right),$$

где $P\left(\frac{\Omega_i}{a_v}\right)$ – вероятность гипотезы H_j; a_j – соответствующая вероятность ошибки. Обозначим через $C^{(v+1)}$ стоимость определения $(v+1)$-го признака, а P^* – вероятность того, что на $(v+1)$-м шаге процесс закончится принятием определенного решения (например, однозначного решения). Тогда после проведения $(v+1)$-го наблюдения средняя плата за ошибки, включая стоимость этого наблюдения, $C^{(v+1)} + (1-P^*)\overline{C}$.

При

$$C^{(v+1)} + (1-P^*)\overline{C} \geq \overline{C} \qquad (3)$$

рационально принять решение ν – й стадии наблюдения, а при $C^{(v+1)} + (1-P^*)\overline{C} < C$ рационально проводить $(v+1)$-ое наблюдение.

Перепишем (3) в виде: $C^{(v+1)} - P^* \sum_{j=1}^{r} C_j a_j P\left(\frac{\Omega_i}{a_{v=1}}\right) \geq 0$ и положим, $a_j = a_0$ при всех $j = 1, 2, ..., r$.

Тогда

$$a_0 \leq \frac{C^{(v+1)}}{P^* \sum_{j=1}^{r} C_j P\left(\frac{\Omega_j}{a_{v+1}}\right)}.$$

Второй метод. В случае, когда нет возможности определить числа a_{ij}, решение принадлежности объекта к тому или другому классу может быть принято на основе критерия идеальности наблюдателя, обеспечивающего минимум ошибочных решений.

Пусть все множество объектов подразделено на классы Ω_1 и Ω_2 и априорные вероятности появления объектов этих классов равно $P(\Omega_1)$ и $P(\Omega_2)$

соответственно, кроме того, стоимости правильных решений $C_{11} = C_{22} = 0$, а стоимости ошибочных решений равны между собой, т.е. $C_{12} = C_{21}$.

Критическое (пороговое) значение отношения или коэффициента правдоподобия в этом случае равно отношению априорных вероятностей: $\lambda_0 = P(\Omega_1) / P(\Omega_2)$.

Пусть экспериментально установлено, что значение признака у распознаваемого объекта $x = x^0$. Тогда коэффициент правдоподобия $\lambda(x = x^0) = f_2(x^0) / f_1(x^0)$.

В соответствии с критерием идеального наблюдателя объект относиться к классу Ω_1, если $\lambda(x^0) < \lambda_0$, и относится к классу Ω_2, если $\lambda(x^0) > \lambda_0$.

Если установлено значение x_0, при котором имеет место равенство $P(\Omega_1) f_1(x_0) = P(\Omega_2) f_2(x_0)$, то в соответствии с рассматриваемым критерием объект относиться к классу Ω_1, если значение признака этого объекта $x^0 < x_0$ и к классу Ω_2, если $x^0 > x_0$.

Критерий идеального наблюдателя совпадает с критерием максимума апостериорной вероятности, когда число классов $m = 2$. В соответствии с критерием максимума апостериорной вероятности решение о принадлежности объекта к классу Ω_r, $r = 1,2,\ldots,m$, принимается тогда, когда апостериорная вероятность отнесения объекта к этому классу больше, чем апостериорная вероятность отнесения его ко всем остальным классам: $\omega \in \Omega_r$, если $P(\Omega_2 / x^0) = \max P(\Omega_i / x^0)$, $i = 1,2,...,m$.

Апостериорные вероятности того, что объект относится к классам Ω_1 и Ω_2, соответственно равны: $P(\Omega_1 / x^0) = \dfrac{P(\Omega_2) f_1(x^0)}{P(\Omega_1) f_1(x^0) + P(\Omega_2) f_2(x^0)}$,

$$P(\Omega_2 / x^0) = \frac{P(\Omega_2) f_2(x^0)}{P(\Omega_1) f_1(x^0) + P(\Omega_2) f_2(x^0)}. \qquad (4)$$

Объект относиться к классу Ω_1, если

$$P(\Omega_1 / x^0) > P(\Omega_2 / x^0) \qquad (5)$$

и к классу Ω_2, если $P(\Omega_2 / x^0) > P(\Omega_2 / x^0)$.

Граница соответствует равенству $P(\Omega_1 / x^0) = P(\Omega_2 / x^0)$ или с учетом (4) и (5) – равенству $f_2(x^0) / f_1(x^0) = P(\Omega_1) / P(\Omega_2) = \lambda_0$.

Таким образом, критерий максимума апостериорной вероятности, как и критерий идеального наблюдателя, предусматривает в качестве порога критическое значение коэффициента правдоподобия.

Третий метод. Пусть в результате проведения наблюдений установлены значения признаков распознаваемого объекта $x_1 = x_1^0$, $x_2 = x_2^0, ..., x_N = x_N^0 = x_N^0$ и пусть, кроме того, $P(\Omega_r / x_1^0, ..., x_N^0) = \max P(\Omega_i / x_1^0, ..., x_N^0)$.

В соответствии с рассматриваемым критерием решение о принадлежности распознаваемого объекта к классу Ω_r, $r = 1,2,\ldots,m$, принимается в случае, если

$$P(\Omega_r / x) > a \sum_{\substack{i=1 \\ i \neq r}}^{m-1} P\left(\frac{\Omega_i}{x}\right).$$

Применение подобного критерия оправдано в случаях, когда решение о принадлежности распознаваемого объекта к Ω_r -му классу сопряжено со значительным риском. Методы принятия решений при неполных данных в ряде практически важных случаях не представляют возможным выявить всю совокупность признаков, используемых для описания объектов. Подобная ситуация имеет место из-за самых разнообразных причин. Например, применение на объекте наблюдения средств маскировки как визуальной, так и радиоэлектронной, или разное изменение погодных условий (туман, осадки), а также применение дымовых завес или постановки активных помех, которые влияют на работу электронных средств БПЛА или на канал связи БПЛА – оператор. Как уже отмечалось, в самом общем случае планирование работы системы распознавания объекта, которая используется в БПЛА, сводится к решению вопроса о продолжении наблюдения за объектом или прекращении наблюдения, производится при анализе полученных данных, которые имеют лишь часть признаков, характеризующих распознаваемый объект. В подобных ситуациях решающее правило может быть основано на критерии максимума апостериорной информации.

Рассмотрим основные методы решения этой задачи.

Четвертый метод. Этот метод может быть использован, когда известна условная плотность вероятности значений любого наперед заданного подмножества, принадлежащего множеству признаков рабочего словаря. Положим, что задан алфавит классов Ω_1, $\mathrm{i}=1,2,\ldots,\mathrm{m}$, априорные вероятности $P(\Omega_1)$, рабочий словарь признаков $x=\{x_1,x_2,...,x_N\}$, условные плотности вероятности $f_1=(x_{j1},x_{j2},...,x_{jk})$, где $\{j_1,j_2,...,j_k\}\in\{1,2,...,N\}$, $k\le N$.

Пусть в результате проведения наблюдений установлены значения некоторых признаков распознаваемого объекта $(x_{j1}=x_{j1}^0,x_{j2}=x_{j2}^0,...,x_{jk}=x_{jk}=x_{jk}^0)$. Обозначим это событие через β и определим значения апостериорной вероятности принадлежности объекта ω классам: $P\left(\frac{\Omega_i}{\beta}\right)=\frac{P(\Omega_i)\,f(x_{j1}^0,x_{j2}^0...x_{jk}^0)}{\sum_{i=1}^m P(\Omega_i)\,f(x_{j1}^0,x_{j2}^0...x_{jk}^0)}$.

Решающее правило, основанное на критерии максимума апостериорной вероятности, состоит в следующем: $\omega\in\Omega_r$, если $P\left(\frac{\Omega_r}{\beta}\right)\max_{i\ P\left(\frac{\Omega_i}{\beta}\right)}$, $i,r=1,2,...,m$.

Пятый метод. Метод может быть применен, когда удается определить наиболее вероятные значения признаков, не определенных наблюдением. Обозначим через β событие, состоящее в том, что в результате наблюдений установлены значения признаков объекта ω $x_1=x_1^0,x_2=x_2^0,...,x_{N-1}=x_{N-k}^0$ и, кроме того, $x_{N-k+1}=x_{N-k+1}^*,...,x_N=x_N^*$, где $x_{N-k+1}^*,...,x_N^0$ – наиболее вероятные значения признаков объекта, которые в результате наблюдения не определены. Значения апостериорной вероятности принадлежности объекта Ω классам таковы: $P\left(\frac{\Omega_i}{\beta}\right)=\frac{P(\Omega_i)\,f_i(x_1^0,...,x_{N-k}^0,x_{N-k+1}^*,...,x_N^*)}{\sum_{i=1}^m P(\Omega_i)\,f_1(x_1^0,...,x_{N-k}^0,x_{N-k}^*,...,x_N^*)}$.

Решающее правило, основанное на критерии максимума апостериорной вероятности, состоит в следующем: $\omega\in\Omega_r$ если $P\left(\frac{\Omega_r}{\beta}\right)\max_{i\ P\left(\frac{\Omega_i}{\beta}\right)}$, $i,r=1,2,...,m$.

Выводы

Поставленная задача оптимизации процессов обработки поступающей информации с БПЛА для распознавания объектов при отсутствии необходимого объема исходной информации, на наш взгляд, решена. Предложенные частные методы распознавания объектов легко реализуются на средствах вычислительной техники, которые располагаются как на борту БПЛА, так и на наземном пункте. Эти методы позволяют оперативно получать ответ на правильность принятых решений относительно разведываемого объекта.

Реализация приоритетов в области создания и применения БПЛА должна осуществляться на основе использования достижения высоких технологий и мирового опыта применения беспилотников с учетом состояния развития национальной научно-производственной базы и реализации накопленного научно-технического и технологического потенциалов Украины в информационной, авиационной, космической, телекоммуникационной и смежных областях, наличия в Украине соответствующей инфраструктуры, а также с учетом реальных экономических, геополитических и военных требований и возможностей.

Список литературы

1. Хорошко, В.А. Алгоритм восстановления изображений, получаемых с беспилотных летательных аппаратов / В.А. Хорошко, Н.А. Дуксенко // Інформатика та математичні методи в моделюванні. – 2016. – Том 6, № 1. – С. 5-96.
2. Алексеєв, С.В. Безпілотні летальні засоби: історія та перпективи розвиту / С.В. Алексеєв // Сучасна спеціальна техніка. – 2014. – №3(39). – С. 89-99.
3. Василин Н.Я. Беспилотные летательные аппараты / Н.Я. Василин. – Минск: ООО «Попурри», 2003. – 272 с.
4. Хорошко, В.О. Метод корекції зображення, отримуємого з БПЛА при наявності шумів і завад / В.О. Хорошко, С.В. Калантаєвська // Збірник наукових праць ВІТІ. – 2018. – №3. – С. 123-131.
5. Красильников, Н.Н. Статистическая теория передачи изображений /Н.Н. Красильников. – М.: Связь, 2006. – 194 с.
6. Фу, К. Структурные методы распознавания образов / К. Фу. – М.: Мир, 2006. – 329 с.
7. Фукунача, К. Введение в статистическую теорию распознавания образов. Изд. 2-е доп. / К. Фукунача. – М.: Наука, 2009. – 367 с.
8. Хорошко, В.О. Розпізнавання об'єктів безпілотними літаючими апаратами в умовах протидії / В.О. Хорошко, Ю.Є. Хохлачова, С.В. Паламарчук // Збірник наукових праць ВІТІ. – 2017. – №4. – С. 91-96.
9. Хорошко, В.А. Распознавание видеоинформационных потоков, передаваемых беспилотными летательными аппаратами / В.А. Хорошко, Ю.Е. Хохлачева // Сучасна спеціальна техніка. – 2016. – №3. – С. 132-143.

ПЕРЕВІРКА ВІРНОСТІ ПРИЙНЯТТЯ РІШЕНЬ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ ПРИ РОЗПІЗНАВАННІ ОБ'ЄКТІВ

[1]В.О. Хорошко, [1] Ю.Є. Хохлачова, [2] С.В. Калантаєвська

[1]Національний авіаційний університет,
пр-т Космонавта Комарова, 1, Київ, 03058, Україна;
[2]Військовий інститут телекомунікацій та інформатизації,
вул. Московська, 45/1, Київ, 01011, Україна;
e-mail: professor_va@ukr.net, hohlachova@gmail.com

У даній роботі пропонується рішення задачі оптимізації процесів обробки інформації, що надходить з БПЛА для розпізнавання об'єктів при відсутності необхідного обсягу вихідної інформації. Запропоновані приватні методи розпізнавання об'єктів можна легко реалізувати на засобах обчислювальної техніки, які розташовуються як на борту БПЛА, так і на наземному пункті. Ці методи дозволяють оперативно отримувати відповідь на правильність прийнятих рішень щодо розвідувати об'єкта. При

практичному побудові систем розпізнавання, які використовуються в БПЛА, необхідно застосовувати великі масиви даних про ознаки об'єктів. Побудова логічних систем розпізнавання об'єктів, що містять велику кількість класів і ознак, і оцінка їх ефективності пов'язаний зі значними труднощами. Найбільш істотним показником ефективності системи розпізнавання -ймовірність правильного рішення нею завдань розпізнавання невідомих об'єктів. За інших рівних умов зокрема в умовах оптимальної обробки апостеріорної інформації, величина цього показника тим вище, чим більшою обсяг інформації, що надходить використовується при розпізнаванні даного об'єкта. Більш того, при певних обмеженнях, що накладаються ознаками, які використовуються при розпізнаванні, зростає і збільшується ймовірність однозначного вирішення задачі розпізнавання. Реалізація пріоритетів в області створення і застосування БПЛА повинна здійснюватися на основі використання досягнення високих технологій і світового досвіду застосування безпілотників, з урахуванням стану розвитку національної науково-виробничої бази та реалізації накопиченого науково-технічного і технологічного потенціалів України в інформаційній, авіаційній, космічній, телекомунікаційної та суміжних областях, наявності в Україні відповідної інфраструктури, а також з урахуванням реальних економічних, геополітичних та військово их вимог і можливостей.
Ключові слова: безпілотні літальні апарати, правильність прийняття рішень, перевірка правильності, розпізнавання об'єктів.

CHECKING THE CORRECTNESS OF MAKING A UAV DECISION WHEN RECOGNIZING OBJECTS

[1] V.O. Khoroshko, [1] Yu.Ye.Khokhlachova, [2] S.V. Kalantayevska

[1]National Aviation University,
prosp. Kosmonavta Komarova, 1, Kyiv, 03058, Ukraine;
[2]Military Institute of Telecommunications and Information,
st. Moskovska, 45/1, Kiev, 01011, Ukraine;
e-mail: professor_va@ukr.net, hohlachova@gmail.com

This paper proposes a solution to the problem of optimizing the processing of incoming information from a UAV for object recognition in the absence of the necessary amount of initial information. The proposed private methods of object recognition can be easily implemented on computer equipment, which are located both on board the UAV and at a ground station. These methods make it possible to promptly receive an answer to the correctness of the decisions made regarding the object being explored. In the practical construction of recognition systems that are used in UAVs, it is necessary to use large amounts of data on the signs of objects. The construction of logical systems of recognition of objects containing a large number of classes and features, and the evaluation of their effectiveness is associated with considerable difficulties. The most significant indicator of the effectiveness of the recognition system is the probability of the correct solution of problems of recognition of unknown objects. With other things being equal, in particular, under conditions of optimal processing of a posteriori information, the value of this indicator is the higher, the greater the amount of incoming information is used in the recognition of this object. Moreover, under certain restrictions imposed by the signs used in recognition, the probability of a unique solution to the recognition problem increases and increases. The implementation of priorities in the field of creation and use of UAVs should be based on the use of high-tech achievements and world experience in the use of UAVs, taking into account the state of development of the national research and production base and the realization of the accumulated scientific, technical and technological potential of Ukraine in the information, aviation, space, telecommunications and related areas, the availability of appropriate infrastructure in Ukraine, and also taking into account the real economic, geopolitical and military requirements and capabilities.
Keywords: unmanned aerial vehicles, correctness of decision making, validation, object recognition.

УДК 62-50

Informatics and Mathematical Methods in Simulation
Vol. 8 (2018), No. 4, pp. 295-301

СИНТЕЗ И МОДЕЛИРОВАНИЕ УПРАВЛЯЮЩЕГО УСТРОЙСТВА ДЛЯ НЕСТАЦИОНАРНОГО ОБЪЕКТА С ЗАПАЗДЫВАНИЕМ

С.А. Бобриков, Е.Д. Пичугин, М.В. Сависько, В.И. Тимохин

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Україна; e-mail: bobrikov1932@gmail.com

Проведен синтез системы управления нестационарным объектом, в котором есть звено с транспортным запаздыванием. Заданная часть системы представляется двумя звеньями: усилитель мощности – звено первого порядка с неизменяющимися параметрами, и объект управления – последовательно включенные звено первого порядка и интегратор. Принято условие: постоянная времени объекта может изменяться в процессе нормального режима работы системы в пределах 1:10, коэффициент усиления объекта может изменяться в пределах 1:2. При этом показатели качества управления – максимальное перерегулирование в переходной характеристике и время переходного процесса остаются практически постоянными при любых значениях параметров объекта в заданных интервалах. В структурной схеме управляющего устройства использовано два дифференцирующих звена и нелинейное звено типа «насыщение». Экспериментальным путем найдены соотношения между запаздыванием, коэффициентом усиления системы и параметрами объекта, обеспечивающие постоянство показателей качества управления при изменении параметров объекта в заданных пределах. Приведен график зависимости максимальной величины коэффициента усиления системы от величины запаздывания. Выполнен анализ устойчивости системы при любых значениях параметров объекта в указанных пределах. Для определения запаса устойчивости системы по фазе приведена программа для расчета запаса устойчивости в системе MATLAB. Приведены примеры расчета управляющего устройства при заданных параметрах неизменяемой части системы и предельно допустимых значениях изменяемых параметров объекта управления.

Ключевые слова: моделирование, система управления, передаточная функция, запаздывание, переходная характеристика, показатели качества управления, объект управления, исполнительное устройство, насыщение, устойчивость, запас устойчивости по фазе.

Введение

Известны системы управления объектами, в которых параметры могут изменяться в широких пределах (нестационарные объекты), например, крупнотоннажные морские суда (с грузом и без груза), управляемая ракета и др. Для обеспечения высоких показателей качества процесса управления при построении подобных систем используют методы адаптивного управления, что приводит, как правило, к существенному усложнению управляющего устройства [1-5]. В работах [6-9] рассмотрены системы управления нестационарными объектами, построенные без использования методов, свойственных адаптивным системам и, вместе с тем, позволяющие получить требуемые показатели качества управления при условии, что параметры объекта управления изменяются в широких пределах. Особенностью регуляторов, рассмотренных в указанных работах, является использование дифференцирующих звеньев, которые частично компенсируют постоянные времени в звеньях заданной части системы, и нелинейного звена типа «насыщение», которое гасит пики напряжений на выходе регулятора, вызванные дифференцирующими звеньями.

Цель работы

Целью работы является синтез и моделирование системы управления объектом с изменяющимися параметрами при наличии в системе управления звена с запаздыванием.

В данной работе используется тот же принцип построения управляющего устройства, как и в работах [7-9], но с учетом запаздывания. Устройство обеспечивает заданные показатели качества в пределах заданного диапазона изменения параметров объекта. В качестве показателей принято минимальное перерегулирование в переходной характеристике при заданной верхней границе времени переходного процесса.

Обобщенная структурная схема разрабатываемой системы показана на рисунке 1, где приняты следующие обозначения: $K_{уу}(p)$ – передаточная функция управляющего устройства, $K_{им}(p)$ – передаточная функция усилителя мощности (исполнительного механизма), $K_{оу}(p)$ – передаточная функция объекта управления. Полагаем, что заданная часть системы (исполнительное устройство и объект управления) описываются следующими передаточными функциями:

$$K_{ум}(p)=\frac{K_1}{T_1p+1},\quad K_{оу}(p)=\frac{K_2e^{-p\tau}}{(T_2p+1)p}.$$

Принимаем условие, что параметры объекта K_2 и T_2 в процессе работы системы могут изменяться в заданных пределах.

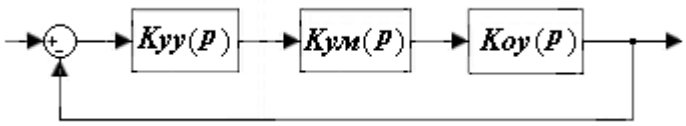


Рис. 1. Обобщенная структурная схема системы управления

Разрабатываемое управляющее устройство должно обеспечить работу системы с заданными показателями качества при любых возможных значениях параметров объекта.

Основная часть

Структурная схема системы приведена на рисунке 2. Принимаем условие, что параметры объекта могут изменяться в заданных пределах:

$$K_{2\min}\le K_2\le K_{2\max}=2K_{2\min},\quad T_{2\min}\le T_2\le T_{2\max}=10T_{2\min}.$$

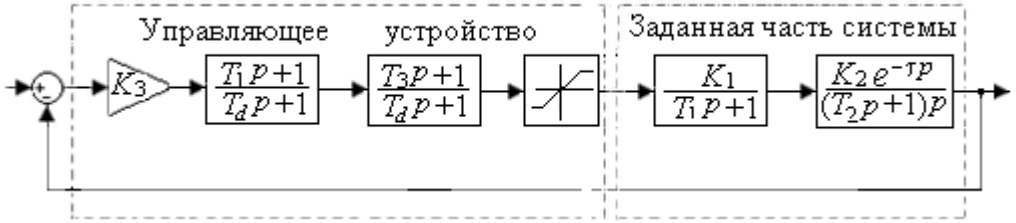


Рис. 2. Структурная схема системы

Принимаем, что постоянная времени T_1 и коэффициент усиления K_1 в процессе работы системы не меняются. Постоянная времени T_3 и коэффициент K_3 в

управляющем устройстве определяются по заданным параметрам объекта управления (см. далее). Постоянные времени T_d введены для обеспечения физической реализуемости управляющего устройства. Их величина должна быть на порядок меньше наименьшей постоянной времени в заданной части системы, при этом наличие в системе этих постоянных времени практически не сказывается на динамических свойствах системы. В нелинейном звене (насыщение) линейная часть имеет коэффициент 1, а насыщение наступает при входной величине, равной ±1.

Экспериментальным путём установлено, что величина постоянной времени T_3 в управляющем устройстве связана с постоянной времени объекта управления T_2 следующим выражением:

$$T_3 = 0,5T_{2\max}, \tag{1}$$

где $T_{2\max}$ – максимальное значение постоянной времени объекта управления.

Общий коэффициент усиления системы обозначим через K_c (рис.2):

$$K_c = K_3K_1K_2. \tag{2}$$

Путем моделирования в системе MATLAB-Simulink определена зависимость максимального значения коэффициента усиления разомкнутой системы K_c от запаздывания при условии, что показатели качества не превышают заданных значений: максимальное перерегулирование в переходной характеристике $\sigma_{\max}\leq 5\%$, время переходного процесса $t_p\leq(4\text{-}5)T_{2\max}$ (рис.3).

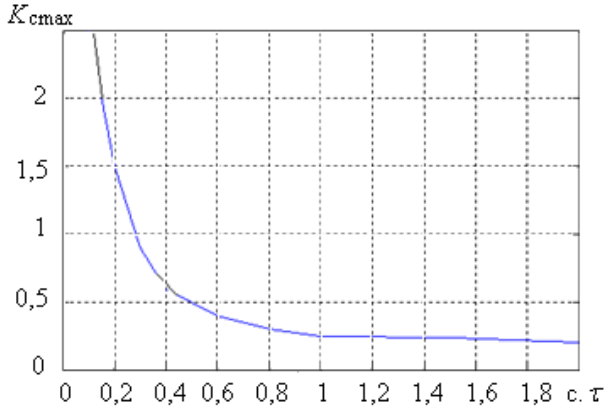


Рис. 3. Зависимость максимального значения общего коэффициента усиления системы от величины запаздывания

Наличие в системе звена типа «насыщение» делает данную систему существенно нелинейной. Автоколебания в такой системе будут отсутствовать в том случае, если линейная модель системы устойчива. При исследовании такой системы на устойчивость (отсутствие автоколебаний) принимаем нелинейное звено как линейное с коэффициентом усиления, равным 1.

Для исследования системы на устойчивость воспользуемся частотным критерием устойчивости. Для этого сделаем оценку запаса устойчивости по фазе.

Передаточная функция разомкнутой системы (рис.2) равна:

$$K(p) = \frac{K_3(T_1p+1)(T_3p+1)K_1K_2e^{-p\tau}}{(T_dp+1)^2(T_1p+1)(T_2p+1)p} = \frac{K_c(T_3p+1)e^{-p\tau}}{(T_dp+1)^2(T_2p+1)p}.$$

Пренебрегая малыми величинами T_d и сделав подстановку $p = j\omega$, получим упрощенное выражение для комплексной частотной передаточной функции разомкнутой системы:

$$K(j\omega) = \frac{K_c(T_3 j\omega + 1)e^{-j\omega\tau}}{(T_2 j\omega + 1)\, j\omega}. \qquad (3)$$

Определим модуль функции (3):

$$\left|K(j\omega)\right| = \frac{K_c\sqrt{T_3^2\omega^2 + 1}}{\omega\sqrt{T_2^2\omega^2 + 1}}.$$

На частоте среза ω_c модуль равен 1, при этом имеем:

$$\frac{K_c\sqrt{T_3^2\omega_c^2 + 1}}{\omega_c\sqrt{T_2^2\omega_c^2 + 1}} = 1. \qquad (4)$$

Откуда следует:

$$T_2^2\omega_c^4 + (1 - K_c^2T_3^2)\omega_c^2 - K_c^2 = 0.$$

Решив биквадратное уравнение, определим ω_c^2, а затем частоту среза ω_c:

$$\omega_c^2 = \frac{K_c^2T_3^2 - 1 + \sqrt{(K_c^2T_3^2 - 1)^2 + 4T_2^2K_c^2}}{2T_2^2}. \qquad (5)$$

В формуле (5) перед квадратным корнем следует брать знак «+», так как это соответствует большему значению ω_c, а значит и большему значению произведения $\tau\omega_c$ в формуле $\varphi(\omega_c)$ (см.далее).

Запас устойчивости системы по фазе определяется следующим выражением:

$$\Delta\varphi = 3{,}14 - \left[\varphi(\omega_c)\right], \qquad (6)$$

где $\varphi(\omega_c)$ – значение аргумента комплексной частотной передаточной функции разомкнутой системы (3) на частоте среза,

$$\varphi(\omega_c) = arctg(T_3\omega_c) - arctg(T_2\omega_c) - 1{,}57 - \tau\omega_c \ \ рад. \qquad (7)$$

***Пример* 1**. Заданная часть системы определяется следующим образом:

K_1=2,5; T_1=0,01с. ; 0,4≤K_2≤0,8; 0,2≤T_2≤2; τ=0,6с.

По графику (рис.3) определяем максимальное значение коэффициента K_c. Для $\tau = 0,6c - K_{c\max} = 0,4$.

Из условия (2) находим значение коэффициента K_3:

$$K_3 = \frac{K_{c\max}}{K_1K_{2\max}} = \frac{0{,}4}{2{,}5\times 0{,}8} = 0{,}2.$$

Постоянную времени T_3 определяем по формуле (1): $T_3 = 0,5*2 = 1$.

Запас устойчивости (6) равен $\Delta\varphi$=1,6 рад. Автоколебания отсутствуют.

Схема набора модели в системе Simulink [10] приведена на рисунке 4. Результат моделирования – на рисунке 5.

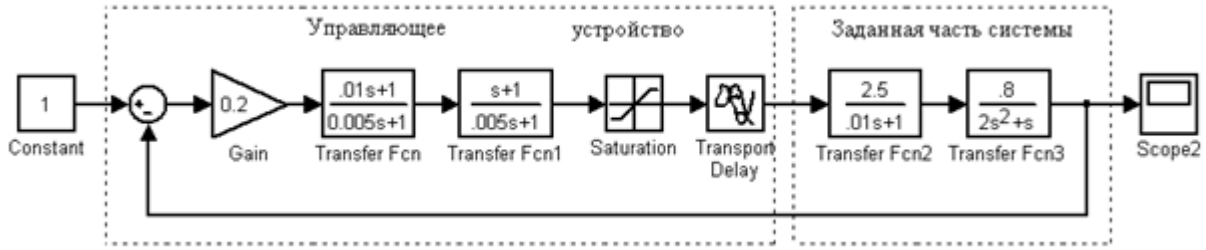


Рис. 4. Схема модели системы

***Пример* 2.** Объект управления – морское судно. Исполнительный механизм выполнен с использованием гидравлического усилителя [6]. Передаточная функция исполнительного механизма равна

$$K_1(p) = \frac{K_1 e^{-p\tau}}{T_1 p + 1}.$$

Передаточная функция судна имеет вид:

$$K_2(p) = \frac{K_2}{p(T_2 p + 1)}.$$

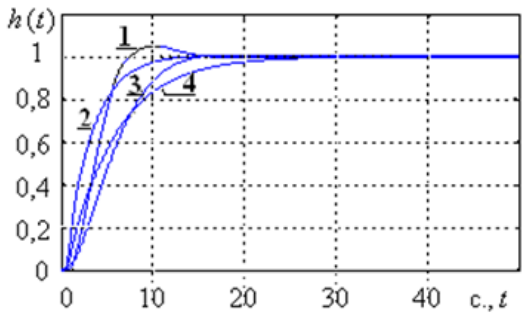


Рис. 5. Результат моделирования системы по примеру 1:
1 - K_2=0,8; T_2=2; 2 - K_2=0,8; T_2=0,2;
3 - K_2=0,4; T_2=0,2; 4 - K_2=0,4; T_2=2

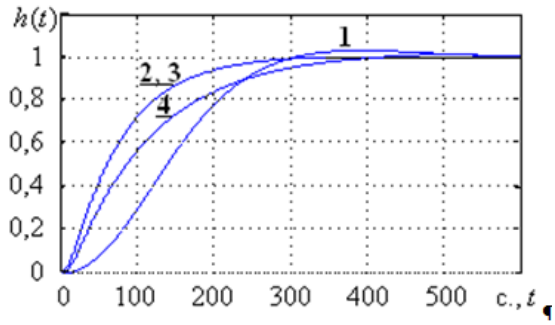


Рис. 6. Результат моделирования системы по примеру 2:
1 - K_2=0,012;T_2=150; 2 - K_2=0,12; T_2=150;
3 - K_2=0,12; T_2=15; 4 - K_2=0,012; T_2=15

Параметры передаточной функции исполнительного механизма [6]: K_1=1; T_1=3с.; τ=1,6с. Параметры передаточной функции судна: 0,012≤K_2≤0,12; 15≤T_2≤150.

Определим параметры регулятора. По графику (рис.3) для τ=1,6 – $K_{c\max}$=0,25. Коэффициент K_3 равен (2): $K_3 = \frac{K_{c\max}}{K_1 K_{2\max}} = \frac{0,25}{1 \times 0,12} = 2,1$.

Постоянная времени T_3 равна: $T_3 = \frac{T_{2\max}}{2} = \frac{150}{2} = 75$.

Запас устойчивости (6) равен $\Delta\varphi$=0,7 рад. Автоколебания отсутствуют.

Результат моделирования приведен на рисунке 6. Из графиков (рис. 6) видно, что требования по быстродействию в данном случае выполнено при изменении коэффициента усиления объекта управления в 10 раз (0,012-0,12).

Выводы

Разработано устройство управления нестационарным объектом при наличии в заданной части системы транспортного запаздывания. Представлена структурная схема управляющего устройства и системы управления. Принято условие, что объект представляет собой звено первого порядка с интегратором. Объект, либо исполнительный механизм имеют запаздывание. Разработан метод определения параметров регулятора по заданным допустимым значениям постоянной времени, коэффициента усиления объекта и величины запаздывания. Приведены примеры расчета системы по предлагаемой методике. Примеры подтверждают возможность проводить расчет управляющего устройства для нестационарного объекта с запаздыванием. Предлагаемая методика расчета управляющего устройства отличается сравнительной простотой.

Список литературы

1. Ядыкин, И.Б. Оптимальное адаптивное управление на основе беспоисковой самонастраивающейся системы с обучаемой эталонной моделью / И.Б. Ядыкин // Автоматика и телемеханика. – 1979. – № 2. – С. 65-79.
2. Уткин, В.А. Задача слежения в линейных системах с параметрическими неопределенностями при неустойчивой нулевой динамике / В.А. Уткин, А.В. Уткин // Автоматика и телемеханика. – 2014. – № 9. – С. 45-64.
3. Рутковский, В.Ю. Стабилизация упругих колебаний конструкции крупногабаритных спутников с переменными параметрами методами адаптации / В.Ю. Рутковский, В.М. Суханов, В.М. Глумов // Автоматика и телемеханика. – 2011. – № 12. – С. 91-103.
4. Земляков, С.Д. Алгоритм функционирования адаптивной системы с эталонной моделью, гарантирующий заданную динамическую точность управления нестационарным динамическим объектом в условиях неопределенности / С.Д. Земляков, В.Ю. Рутковский // Автоматика и телемеханика. – 2009. – № 10. – С. 35-44.
5. Глумов, В.М. Адаптивное управление ориентацией деформируемых космических аппаратов с изменяющимися параметрами / В.М. Глумов, В.Ю. Рутковский, В.М. Суханов // Автоматика и телемеханика. – 1999. – № 4. – С. 90-102.
6. Кринецкий, И.И. Исследование автоматического управления курсом судна с учетом нелинейных характеристик системы / И.И. Кринецкий, Е.Д. Пичугин // Судовождение и связь. Труды ЦНИИ морского флота. – Л.: Транспорт, 1967. – № 83. – С. 13-16.
7. Бобриков, С.А. Синтез и моделирование регулятора для объекта с изменяющимися параметрами / С.А. Бобриков, Е.Д. Пичугин, С.И. Кысса // Информатика и математические методы в моделировании. – 2017. – №1-2. – С. 54-61.
8. Бобриков, С.А. Синтез и моделирование цифрового управляющего устройства для нестационарного объекта / С.А. Бобриков, Е.Д. Пичугин, Н.Н. Дикий // Информатика и математические методы в моделировании. – 2017. – №3. – С. 220-227.
9. Бобриков, С.А. Модельно-ориентированный синтез комбинированной системы управления нестационарным объектом / С.А. Бобриков // Информатика и математические методы в моделировании. – 2018. – №2. – С. 174-183.
10. Краснопрошина, А.А. Современный анализ систем управления с применением MATLAB, Simulink, ControlSistem / А.А. Краснопрошина, Н.Б. Репникова, А.А. Ильченко. – К.: Корнійчук, 1999. – 141 с.

СИНТЕЗ І МОДЕЛЮВАННЯ УПРАВЛЯЮЧОГО ПРИСТРОЮ ДЛЯ НЕСТАЦІОНАРНОГО ОБ'ЄКТА З ЗАПІЗНЕННЯМ

С.О. Бобріков, Є.Д. Пичугин, М.В. Сависько, В.І.Тимохін

Одеський національний політехнічний університет,
Просп. Шевченко, 1, Одеса, 65044, Україна; e-mail: bobrikov1932@gmail.com

Проведено синтез системи управління нестаціонарним об'єктом, в якому є ланка з транспортним запізненням. Задана частина системи представляється двома ланками: підсилювач потужності - ланка першого порядку з не змінними параметрами, і об'єкт управління - послідовно включені ланка першого порядку і інтегратор. Прийнято умова: постійна часу об'єкта може змінюватися в процесі нормального режиму роботи системи в межах 1:10, коефіцієнт посилення об'єкту може змінюватися в межах 1: 2. При цьому показники якості управління - максимальне перерегулювання в перехідній характеристиці і час перехідного процесу залишаються майже незмінними за будь-яких значеннях параметрів об'єкта в заданих інтервалах. У структурній схемі керуючого пристрою використано дві диференціючих ланки і нелінійна ланка типу «насичення». Експериментальним шляхом знайдені співвідношення між запізненням, коефіцієнтом посилення системи і параметрами об'єкта, що забезпечують сталість показників якості управління при зміні параметрів об'єкта в заданих межах. Наведено графік залежності максимальної величини коефіцієнта посилення системи від величини запізнювання. Виконано аналіз стійкості системи при будь-яких значеннях параметрів об'єкта в зазначених межах. Для визначення запасу стійкості системи по фазі наведена програма для розрахунку запасу стійкості в системі MATLAB. Наведені приклади розрахунку керуючого пристрою при заданих параметрах незмінної частини системи і гранично допустимих значеннях змінних параметрів об'єкта управління.

Ключові слова: моделювання, система управління, передавальна функція, запізнювання, перехідна характеристика, показники якості управління, об'єкт управління, виконавчий пристрій, насичення, стійкість, запас стійкості по фазі.

SYNTHESIS AND MODELING OF THE CONTROL DEVICE FOR NON-STATIONARY OBJECT WITH LATE

S.A. Bobrikov, E.D. Pichugin, M.V. Savisko, V.I. Timohin

Odesa National Polytechnic University,
1 Shevchenko Ave., Odesa, 65044, Ukraine; e-mail: bobrikov1932@gmail.com

The synthesis of the control system of a non-stationary object, in which there is a link with transport delay, has been carried out. The specified part of the system is represented by two links: the power amplifier is a first-order link with unchanged parameters, and the control object is a sequentially-connected first-order link and an integrator. The following condition is accepted: the time constant of an object can change during normal operation of the system within 1:10, the gain of the object can vary within 1: 2. At the same time, the quality control indicators - the maximum overshoot in the transient response and the transient process time remain almost constant for any values of the object parameters at specified intervals. In the block diagram of the control device, two differentiating links and a nonlinear link of the “saturation” type are used. Experimentally found the relationship between the delay, the gain of the system and the parameters of the object, ensuring the constancy of the indicators of quality control when changing the parameters of the object within the specified limits. A graph of the maximum magnitude of the gain of the system on the magnitude of the delay. The analysis of the stability of the system for any values of the parameters of the object within the specified limits. To determine the stability margin of a system by phase, a program is given for calculating the stability margin in the MATLAB system. Examples of calculating the control device with given parameters of the unchanged part of the system and the maximum allowable values of the variable parameters of the control object are given.

Keywords: modeling, control system, transfer function, delay, transient response, control quality indicators, control object, actuator, saturation, stability, phase stability margin null.

УДК 519.6:004.4

Informatics and Mathematical Methods in Simulation
Vol. 8 (2018), No. 4, pp. 302-312

СИСТЕМА РОЗПОДІЛУ ЗАСАДЖЕНЬ НА ЗЕМЕЛЬНИХ ДІЛЯНКАХ НА ОСНОВІ МАТЕМАТИЧНОЇ МОДЕЛІ ВРОЖАЙНОСТІ КУЛЬТУРИ, ЗАЛЕЖНОЇ ВІД ПОПЕРЕДНІХ СІВОЗМІН

С.Я. Крепич, І.Я. Співак, А.Р. Баюрський

Тернопільський національний економічний університет,
вул. Чехова, 6, Тернопіль, 46000, Україна; e-mail: msya220189@gmail.com

Робота присвячена проблемі якості вирощування культурних рослин для власних потреб держави чи потреб зовнішнього ринку. Продукти, вирощені на території України, чи товари, отримані з переробки відповідних культур, є привабливими в багатьох країнах світу. Тому доцільно зробити акцент на покращенні вирощування культур, тобто збільшення їх врожайності, для відповідного підвищення показника експорту наших товарів закордон. Проте відповідне збільшення показника врожайності необхідно забезпечити із одночасною підтримкою земельних ділянок у родючому стані без застосування різного роду пестицидів, які негативно впливають як на структуру ґрунту, так і погіршують екологічний стан навколишнього середовища. Цінність роботи полягає у розробці методики засаджування полів, яка б дозволила з одного боку аграріям отримувати постійний прибуток, пропонуючи свої поля під засів, а з іншого боку замовнику (для прикладу державі) мати постійний обсяг експорту та в той же час економити на закупівлі продукції, а також розробці математичної моделі врожайності культури, залежної від сівозміни, в межах конкретної ділянки. Результатом є спроектована та реалізована інтелектуалізована програмна система для якісного засаджування земельних ділянок під культури, які замовлені на імпорт або експорт, згідно виграних тендерів.

Ключові слова: математична модель, прогнозована врожайність, сівозміна, земельна ділянка, аграрій.

Вступ

Процес вирощування культурних рослин для власних потреб держави чи потреб ринку завжди буде актуальним питанням. Зовнішня торгівля відіграє важливу роль в економіці України. Наведемо пару цифр, що прояснять ситуацію України на міжнародному ринку. Отож, тенденцією останніх 5 років є скорочення виручки від експорту товарів з одночасним скороченням експорту агропромислової продукції. Проте, не дивлячись на загальний негативний тренд, у 2016 році спостерігається зростання експорту сільськогосподарської продукції. Подібна тенденція зберіглась і в 2017 році. За перше півріччя 2017 року експорт сільськогосподарської продукції склав 8,7 млрд. дол. США, що на 28,1% більше ніж за аналогічний період 2016 року [1]. Продукти, вирощені на території України, чи товари, отримані з переробки відповідних культур, є привабливими в багатьох країнах світу. Тому доцільно зробити акцент на покращенні вирощування культур для підвищення показника експорту наших товарів закордон. Розробка відповідного програмного комплексу, який би поєднав інтереси держави та аграріїв, для підвищення показника врожайності культур і відповідно збільшення кількості врожаю, є невід'ємною частиною покращення роботи агропромислової гілки держави.

Об'єктом дослідження є процеси вирощування культур на земельних ділянках. Родючість ґрунтів залежить від багатьох чинників, зокрема типу ґрунтів, міри удобреності ґрунтів за попередні роки засаджування та історії попередніх засаджень. Державі кожного року протягом певного періоду часу необхідно виконати обсяг робіт по засадженню полів певними культурами.

Один такий тендер опрацьовується надто довго. Аналіз діяльності аграріїв та характеристики їх полів відбувається в ручному режимі, що припускає можливість допущення помилки на будь-якому з етапів. Або ж, що є більш розповсюдженим випадком, поля засаджуються одними і тими ж культурами, одними і тими ж аграріями, які для забезпечення відповідного рівня врожайності використовують велику кількість різного роду пестицидів та гербіцидів для удобрення полів, чим погіршують як структуру ґрунту так і, що є значно гіршим, стан ґрунтових вод, що своїм чином погіршує здоров'я людей. Звідси основним питанням дослідження є максимально ефективний розподіл замовлення на засадження певними культурами між аграріями з метою покращення отриманої врожайності екологічно чистим та правильним шляхом.

На першому етапі такого розподілу постає проблема у вигляді банальної відсутності бази аграрників та інформації про тендери. У роботі будемо використовувати змодельовану схему розподілу тендерів на основі вхідних даних, що максимально приближені до справжніх на прикладі Тернопільської області

Відповідно до усіх вище перерахованих проблем, створення системи аналізу якості засаджування ґрунтових ділянок стане надзвичайним проривом в галузі агрономії, оскільки це дозволить максимально ефективно вирощувати різні культури, а також отримувати максимальний прибуток як державі, так і аграрникам, які використовуватимуть пропоновану систему.

Основна частина

Основна ідея розробки програмної системи засаджування земельних ділянок – це покращення родючості ґрунту шляхом такої сівозміни культур, яка, по-перше, менш висушуватиме ґрунт, по-друге, підвищуватиме показник врожайності культури, і, по-третє, вимагатиме меншого застосування різного роду гербіцидів, пестицидів, добавок, стимуляторів росту тощо [1]. В кінцевому результаті це ще позитивно впливатиме на екологію, адже менше хімічних речовин потраплятиме до ґрунту і, відповідно, до водойм.

Іншим позитивним аспектом розробки такої програмної системи є її банальна відсутність в Україні на сьогодні. Монополістами на експортному ринку України виступають великі аграрні комплекси, які мають довгострокові домовленості з державою на постачання тієї чи іншої культури. Відповідно вони зацікавлені в тому, щоб врожайність постійно була, так би мовити, на «стабільному» рівні. Однак ця «стабільність» дуже поганий вплив має на якість ґрунту. Так само і державі вигідно мати аграріїв-монополістів, адже це менше домовленостей, стабільний обсяг товару тощо.

Розробка програмної системи дозволить в певній мірі збалансувати стосунки «держава-аграрій-держава», а також надасть можливість розширити як ринок попиту, так і ринок пропозицій.

Опишемо програмний комплекс в дії для аграріїв Тернопільської області.

Основними сільськогосподарськими культурами, які вирощують у Тернопільській області є сонях, кукурудза, ріпак, цукровий буряк та озимі культури – пшениця та ячмінь. Ці культури є експортним товаром в межах нашої держави, і деякі з них, зокрема сонях та пшениця, є частиною експортованих товарів закордон.

Середній показник врожайності описаних культур для Тернопільської області 2016 року склав:

- 3,8т з 1га для пшениці;
- 2,4т з 1га для соняху;
- 30 т з 1га для цукрового буряка;
- 4,7т з 1га для кукурудзи;

- 3,6т з 1га для ячменю;
- 1,8т з 1га для ріпаку.

Для визначення того, яку культуру і на яку ділянку краще засаджувати, щоб отримати якомога більшого врожаю без надлишкових удобрювань, приймемо вказані показники за еталонні показники врожайності культур. Звісно, виходячи з вище зазначеного, на посадку культури тоді впливатиме інформація про культуру, яка була засаджена на цьому полі минулого року, і кількість років, які пропонована під засаджування культура не вирощувалась на цій ділянці. Найбільш виснажувальними для ґрунту, зокрема з тих культур, що вирощують у Тернопільській області, є сонях та кукурудза. Після соняшнику земля повинна відпочивати 7 років, щоб знову набрати попередньої родючої сили і наснаги, а після кукурудзи – 3 роки. Цей термін агровиробники не завжди витримують або не витримують взагалі. Особливо це стосується соняшнику, тому в системі запропоновано розглядати засаджування ділянки соняхом мінімум через 4 роки.

У таблиці 1 зведені показники засаджування культур із врахуванням останнього року висаджування, сівозміни, а також отриманий показник середньої врожайності культури з 1 га земельної ділянки. Введемо умовні позначення та змінні, зокрема:

- y – максимальна кількість років, які культура не повинна вирощуватись на ділянці;
- v_{pr_i} – середня врожайність культури, яка була останньою посаджена на ділянці, в межах пропонованої ділянки за останню посадку;
- v_i - середня врожайність культури, яка готується до засаджування на ділянку, в межах пропонованої ділянки за останню посадку;
- v_{res_i} - середня врожайність вирощеної культури.

Доцільно побудувати модель залежності врожайності культури від її сівозміни в межах конкретної ділянки. На початковому етапі оберемо лінійну структура моделі виду [2]:

$$v_{res_i} = k_1 \cdot y_i + k_2 \cdot v_{pr_i} + k_3 \cdot v_i + k_4,$$

де $k_i, i = \overline{1..4}$ – невідомі коефіцієнти, значення яких необхідно оцінити на основі аналізу даних, наведених в таблиці 1.

Згідно табличних даних складемо систему лінійних алгебричних рівнянь (СЛАР) у такому вигляді:

$$\begin{cases} k_1 \cdot y_1 + k_2 \cdot v_{pr1} + k_3 \cdot v_1 + k_4 = v_{res1} \\ \dots \\ k_1 \cdot y_i + k_2 \cdot v_{pri} + k_3 \cdot v_i + k_4 = v_{resi} \\ \dots \\ k_1 \cdot y_{30} + k_2 \cdot v_{pr30} + k_3 \cdot v_{30} + k_4 = v_{res30} \end{cases} . \quad (1)$$

Розв’язком системи (1) є область коефіцієнтів моделі. Використавши метод найменших квадратів для знаходження оцінок коефіцієнтів моделі з СЛАР (1), отримаємо таку модель [3]:

$$v_{res_i} = 0,008 \cdot y_i + 0,006 \cdot v_{pr_i} + 0,99 \cdot v_i - 0,04. \quad (2)$$

Отриманий за формулою (2) показник середньої врожайності пропонованої для посадки на вказаній ділянці культури є прогнозований відносно історії засаджень.

Однак для більш адекватної побудови стратегії засаджень потрібно врахувати ризики, які можуть занизити цей показник.

Таблиця 1.

Показники середньої врожайності сільськогосподарських культур згідно попередньої сівозміни та останнього року вирощування

Вид культури	y	v_{pr_i}	v_i	v_{res_i}
Соняшник	3	4,7	2,4	2,2
	3	3,6	2,4	2,4
	3	1,8	2,4	2,5
	3	3,8	2,4	2,3
	3	30	2,4	2,6
Кукурудза	2	3,4	4,7	4,4
	2	3,6	4,7	4,7
	2	1,8	4,7	4,8
	2	3,8	4,7	4,7
	2	30	4,7	4,8
Ячмінь	1	4,7	3,6	3,5
	1	2,4	3,6	3,4
	1	1,8	3,6	3,7
	1	3,8	3,6	3,6
	1	30	3,6	3,7
Ріпак	1	4,7	1,8	1,7
	1	2,4	1,8	1,6
	1	3,6	1,8	1,8
	1	3,8	1,8	1,8
	1	30	1,8	1,9
Пшениця	1	4,7	3,8	3,7
	1	2,4	3,8	3,6
	1	3,6	3,8	3,8
	1	1,8	3,8	3,9
	1	30	3,8	4
Цукровий буряк	1	4,7	30	28
	1	2,4	30	27
	1	3,6	30	30
	1	1,8	30	32
	1	3,8	30	31

Встановимо 5% відхилення від прогнозованого показника врожайності для можливості врахування різних ризиків погіршення врожайності культури. В результаті прогнозована врожайність культури подаватиметься в інтервалі [4-7]: $[v_{res_i}^{-}; v_{res_i}^{+}] = [v_{res_i} - 0,05 \cdot v_{res_i}; v_{res_i}]$.

Замовлення держави на певну культуру представляється в інтервалі:

$$[V_{coni}^{-};V_{coni}^{+}], \tag{3}$$

де V_{coni}^{-} - мінімальний обсяг врожаю культури, який необхідний державі для покриття ринку внутрішніх потреб і потреб експорту закордон; V_{coni}^{+} - максимальний обсяг врожаю культури, який держава може понаднормово викупити в аграріїв [5].

Функція розподілу засаджування культури між ділянками в межах одного замовлення (3) представлена виразом:

$$[f(V_i)] = \sum_{i=1} (S_i \cdot [v_{res_i}^{-}; v_{res_i}^{+}]),$$

де S_i - площа поля, обраного під засадження обраної культури на i -ій ітерації.

Кількість ітерацій визначається відповідно до покращення функції мети F_i, значення якої визначається за формулою:

$$F_i = \min_{i=1,..,N} \left\{ mid([V_{con_i}^{-};V_{con_i}^{+}]) - mid([f(V_i)]) \right\},$$

де $F_i \geq 0$, тобто вибір полів під засадження продовжуватиметься до тих пір, доки функція F_i прийматиме додатні значення з множини можливих значень [5].

Перейдемо до опису програмного комплексу якості засаджування земельних ділянок, розробленого на основі математичної моделі врожайності культури, залежної від сівозмін.

Розглянемо детально основні процеси системи, які реалізовують поставлені у меті цієї роботи задачі.

Крок 1. Формування замовлення. Цей процес включає в себе вибір необхідних культур, їх сортування за пріоритетом та зазначення інтервалу замовлення (3).

Крок 2. Участь у розіграші. Для того, щоб користувач типу «Виконавець», мав змогу взяти участь у тендерному розіграші, йому необхідно виконати операцію «Менеджмент профілю» та додати інформацію про усі свої поля. Після того, як у користувача буде хоча б одне вільне поле, він зможе переглядати тендери та брати в них участь.

Крок 3. Калькуляція засадження. Програмна система аналізує історію засаджень полів, які були зареєстровані на участь в розіграші, та видає список полів з максимально ефективним способом засадження, тобто ті поля, які в результаті покажуть саму найкращу врожайність по культурі з врахуванням сівозміни. Детальніше цей процес проілюстровано на рисунку 1.

Крок 4. Видача результату. Після проведення калькуляції користувачу типу «Виконавець» буде доступне результуюче вікно. На цьому вікні відображатиметься перелік аграріїв та обраховані системою показники прогнозованої середньої врожайності, попередньої врожайності та інші показники. Окрім цього тут можна переглянути контактну інформацію аграріїв, для того, щоб можна було з ними зв’язатись та погодити деталі виконання тендеру.

Діаграма варіантів використання відображає основних користувачів системи, а також доступний функціонал для цих користувачів. На рисунку 2 проілюстровано діаграму варіантів використання для користувачів двох типів «Виконавець» та «Замовник».

Рис. 1. Блок-схема процесу «Калькуляція засадження»

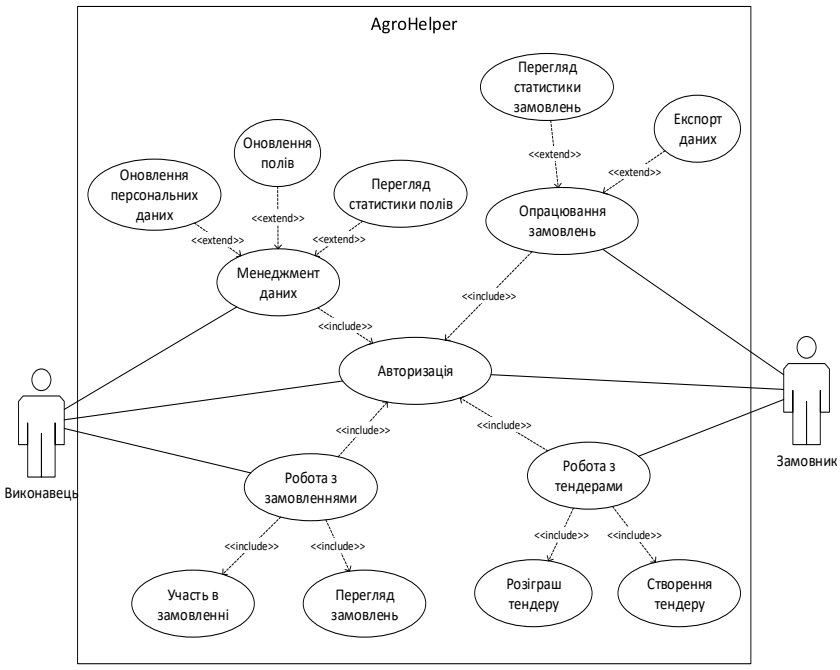


Рис. 2. Діаграма варіантів використання

База даних програмної системи представлена на рисунку 3.

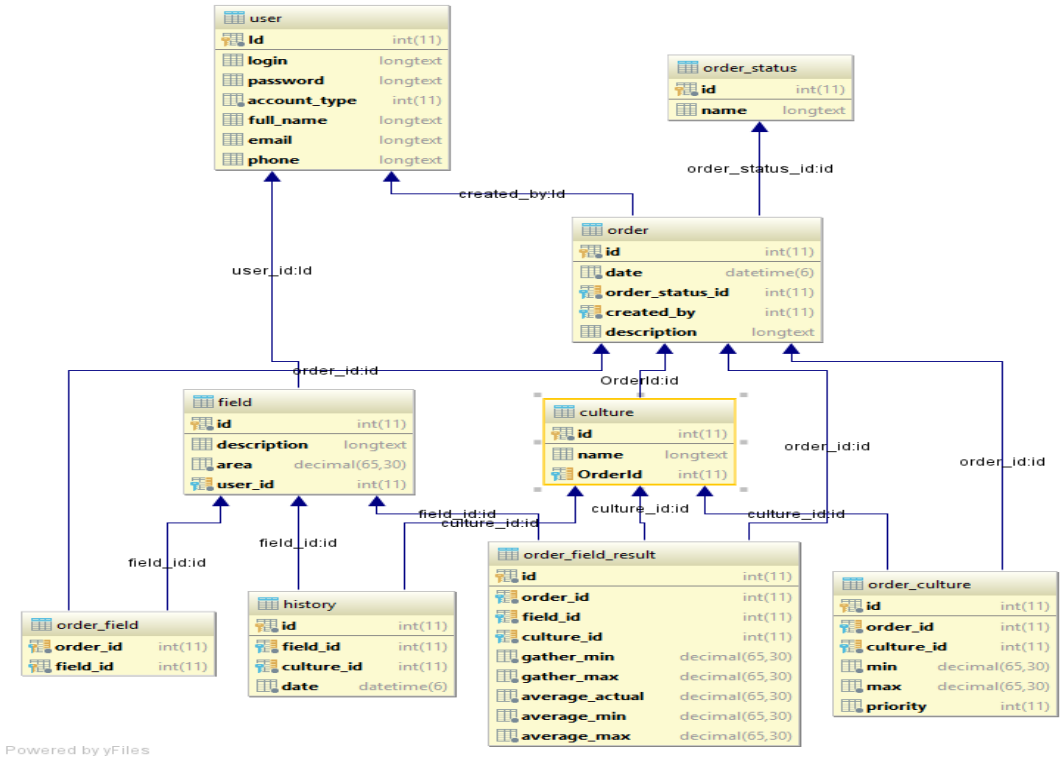


Рис. 3. ER-діаграма бази даних

Розроблена система десктоп-орієнтована, під операційну систему Windows і вимагає встановленого Microsoft .NET Framework версії 4.6. Для розробки цієї системи було вирішено використовувати мову програмування C# [8]. Це строго типізована мова програмування, на якій можна писати будь-які рішення під будь-який тип систем Windows, Linux, Android, IOS. Розглянемо основні вікна програмної системи. Основна робоча сторінка користувача типу «Виконавець» представлена на рисунку 4.

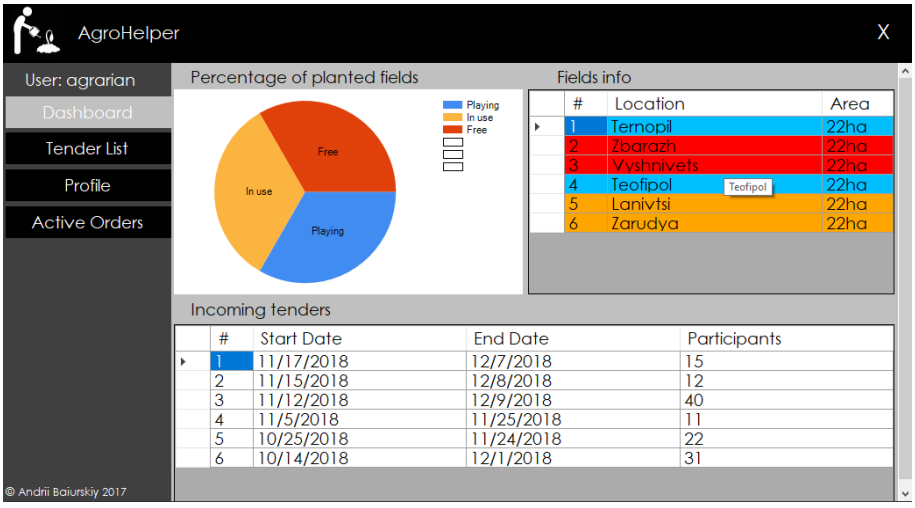


Рис. 4. Вікно «Dashboard»

У цьому вікні відображені статистичні показники аграрія в системі, зокрема:

- процент засадження полів - співвідношення загальної кількості полів до кількості полів, які знаходяться в експлуатації або в розіграші; помаранчевим кольором відображаються поля, які вже виграли в тендері, синім – ті, що беруть участь у розіграші та червоним – вільні;

- перелік полів та їх інформація, а саме місце дислокації, площа та статус;
- перелік найближчих тендерних розіграшів, які найбільше підходять для можливого засадження культурами полів певного користувача.

Перед тим, як прийняти участь у тендерному розіграші, у користувача повинні бути вільні поля для засадження. Менеджмент полів, а також управління персональними даними користувача відбувається у профілі, представленому на рисунку 5.

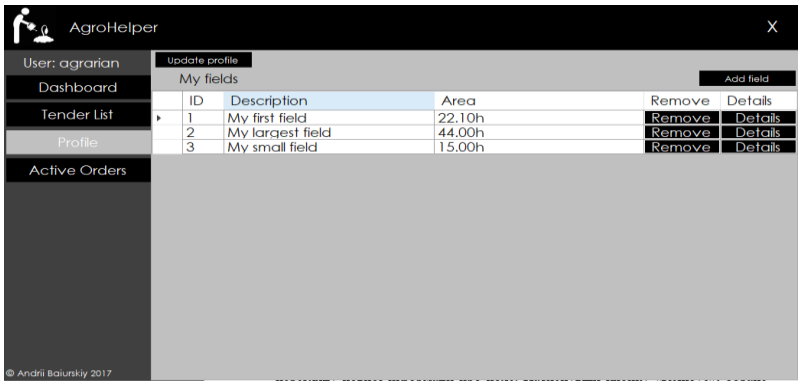


Рис. 5. Вікно «Profile»

При наявності хоча б одного вільного поля користувач може подати заявку на участь в тендерному розіграші. Після натиснення кнопки «TenderList» відкриється форма з переліком доступних розіграшів (рис. 6). Зеленим кольором підсвічуються розіграші, в яких користувач вже бере участь.

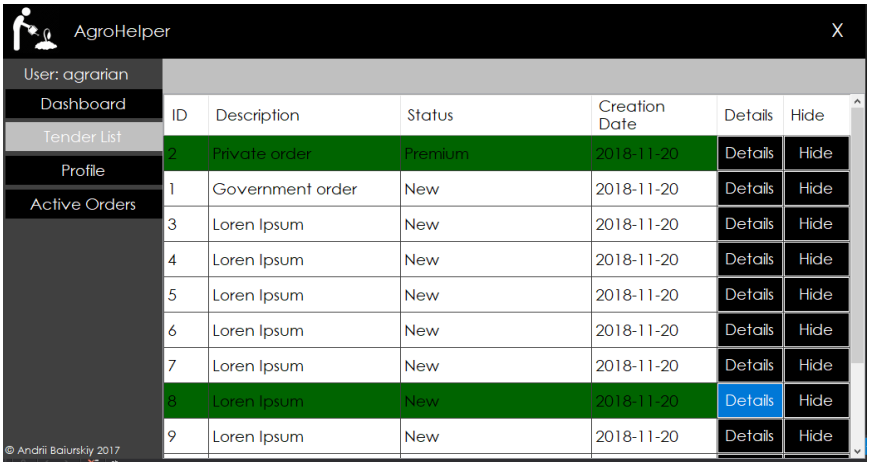


Рис. 6. Вікно «TenderList»

Розглянемо основні компоненти системи для користувача типу «Замовник». Вікно «Dashboard», зображене на рисунку 7, містить статистичну інформацію про:

- тендерну інформацію – відношення усіх учасників розіграного тендеру до учасників, які підтвердили участь, де червоним відображаються учасники, які ще не підтвердили свою участь, а жовтим учасники, які погодились;
- інформацію по культурах – відображає відношення культури (кількість із замовлення) та її заповнення (кількість обраховується як добуток врожайності культури з поля аграрія, який підтвердив участь, на площу цього поля);
- список тендерних замовлень користувача, які повинні бути розіграні найближчим часом.

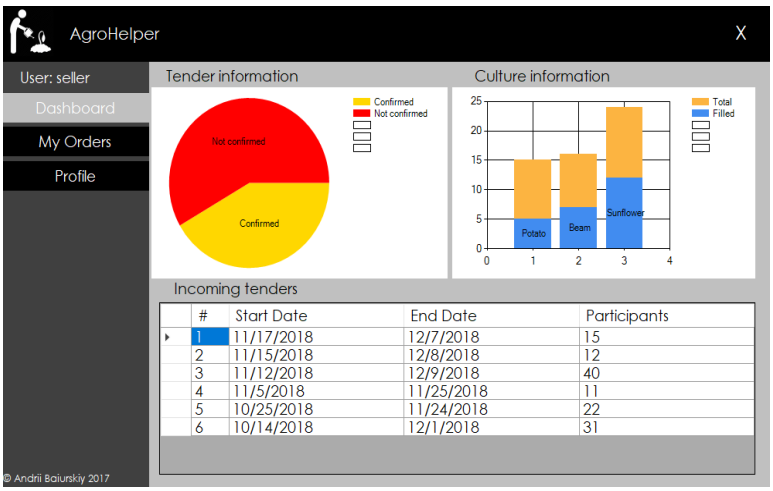


Рис. 7. Вікно «Dashboard» замовника

Основний функціонал для покупців сконцентрований у вкладці «MyOrders», яка зображена на рисунку 8. У цьому вікні відображається перелік замовлень користувача, кількість учасників, а точніше полів, які беруть участь в розіграші, а також їх статус. Перелік статусів тендеру: Active – новий; ManualClosed – закритий без розіграшу; Complete – завершений, підібрано перелік виконавців; Expired – завершений, потребує уваги замовника для проведення калькуляції найкращих виконавців.

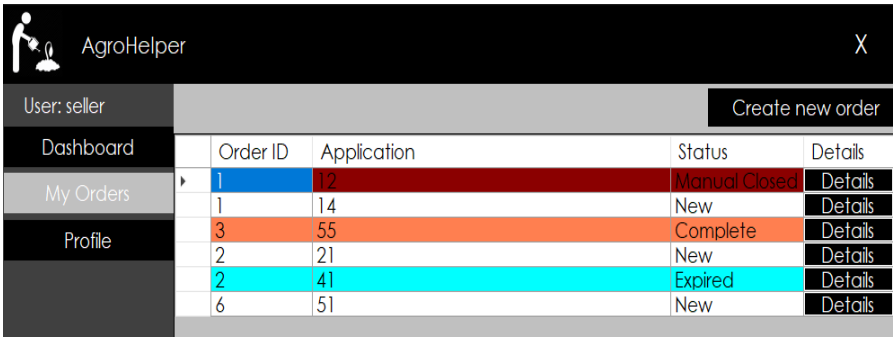


Рис. 8. Вікно «My Orders»

Результуюча форма розіграних тендерів представлена на рисунку 9. На цій формі відображена наступна інформація: назва аграрія, який є власником поля; площа поля; культура, яка буде засаджена на обраному полі; відображення інформації про те, чи покупець отримав підтвердження від виконавця.

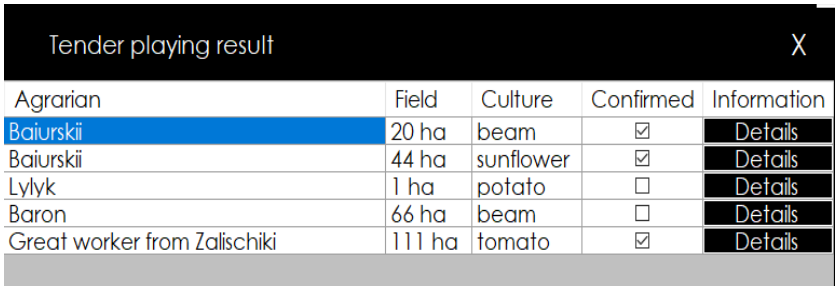


Рис. 9. Вікно відображення результатів розіграшу тендера

На цій формі зображена інформація про аграрія та поле, яке було б ефективно задіяти при засаджуванні певною культурою. Для того, щоб переглянути інформацію про аграрія, поле та прогнозовану врожайність, необхідно натиснути кнопку «Details» (рис.10).

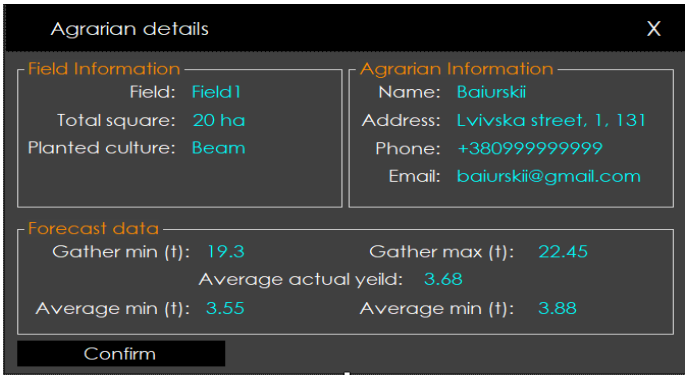


Рис. 10. Перегляд інформації прогнозованої врожайності культури з даного поля

Висновки

Під час аналізу предметної області виявлено, що на сьогодні основний акцент забезпечення держави експортними товарами у сфері аграрної промисловості зорієнтований на аграрниках монополістах. Між ними та державою укладаються основні тендерні домовленості. В межах цих домовленостей основний акцент направлено на отримання максимального врожаю культури з поля, що в результаті призводить до погіршення стану ґрунтів. Стан ґрунтів, відповідно, намагаються поліпшити за допомогою вживання великої кількості добрив неорганічного походження, які в свою чергу, негативно впливають на екологічний стан середовища. У роботі запропоновано задля покращення врожайності культур та зменшення кількості внесення неорганічних добрив враховувати при висаджуванні культури попередню сівозміну, яка може значно покращити показники врожайності пропонованої для посадки культури. В межах запропонованого підходу розроблена математична модель залежності врожайності культури від попередньої сівозміни в межах конкретної ділянки.

Розроблено програмний комплекс якості засаджування земельних ділянок, який дозволить покращити зв'язок «держава-аграрій-держава». Надасть можливість приватним підприємцям виходити на великий ринок продаж та в результаті при правильному і правомірному застосуванні програмного комплексу покращити якість земель і екологічного стану навколишнього середовища.

Список літератури

1. Стратегія розвитку аграрного сектору економіки України на період до 2020 року [Електроний ресурс] // Режим доступу: http://minagro.gov.ua/node/7644.
2. Крепич, С.Я. Програмний комплекс оцінювання функціональної придатності пристроїв при заданих допустимих значеннях вихідних характеристик та допусків на параметри їх елементів / С.Я. Крепич // Сучасні комп'ютерні інформаційні технології: Матеріали VBсеукраїнської школи-семінару молодих вчених і студентів ACIT'2015. – Тернопіль: ТНЕУ, 2015. – С. 23-25.
3. Крепич, С.Я. Порівняння часової складності реалізації процедур випадкового пошуку в задачі синтезу фільтра та допусків на параметри його елементів / С.Я. Крепич, М.П. Дивак // Інформаційні технології та комп'ютерна інженерія, 2015. – Том 33, № 2. – С.47-57.
4. Kumkov, S. Interval approach to identification of parameters of experimental process model / S. Kumkov // 15th GAMM-IMACS International Symposium on Scientific Computing, Computer Arithmetics and Verified Numerics. – 2012. – Pp. 90-93.
5. Bayurskii, A. Intelligent System Analyzing Quality of Land Plots / A. Bayurskii, S. Krepych // International Conference «Advanced Computer Information Technologies» ACIT'2018. – Ceske Budejovice, Czech Republic, 2018. – Pp. 166-169.
6. Крепич, С.Я. Моделювання та забезпечення функціональної придатності статичних систем

методами аналізу інтервальних даних / С.Я. Крепич // НУ «Львівська політехніка», Львів, 2016. – 166 с.
7. Krepych, S. The method of providing of functional suitability of elements of the device of formation of signal in electrophysiological way of classification tissues surgical wound / S. Krepych, A. Dyvak, M. Dyvak, I. Spivak // XIIIth International Conference on Perspective Technologies and Methods in MEMS Design (MEMSTECH), 2017. – Pp. 183-186.
8. Герберт Шилдт. «Полный справочник по C#, 4-е издание: Пер. с англ. – М.: Издательский дом «Вильямс», 2010. – 800с.

СИСТЕМА РАСПРЕДЕЛЕНИЯ ЗАСАЖИВАНИЙ НА ЗЕМЕЛЬНЫХ УЧАСТКАХ НА ОСНОВЕ МАТЕМАТИЧЕСКОЙ МОДЕЛИ УРОЖАЙНОСТИ КУЛЬТУР, ОТНОСИТЕЛЬНО ИХ ПРЕДЫДУЩЕГО СЕВООБОРОТА

С.Я. Крепыч, И.Я. Спивак, А.Р. Баюрский

Тернопольский национальный экономический университет,
ул. Чехова, 6, Тернополь, 46000, Украина; e-mail: msya220189@gmail.com

Работа посвящена проблеме качества выращивания культурных растений для собственных нужд государства или потребностей внешнего рынка. Продукты выращенные на территории Украины или товары, полученные по переработке соответствующих культур, являются привлекательными во многих странах мира. Поэтому целесообразно сделать акцент на улучшении выращивания культур, тоесть увеличение их урожайности для соответствующего повышения показателя экспорта наших товаров за границу. Однако соответствующее увеличение показателя урожайности необходимо обеспечить с одновременной поддержкой земельных участков в плодородном состоянии без применения различного рода пестицидов, которые негативно влияют как на структуру почвы, так и ухудшают экологическое состояние окружающей среды. Ценность работы заключается в разработке методики засаживания полей, которая позволила с одной стороны аграриям получать постоянный доход, предлагая свои поля под засев, а с другой стороны заказчику (например государству) иметь постоянный объем экспорта и в то же время экономить на закупке продукции, а также разработке математической модели урожайности культуры зависимой от севооборота в пределах конкретного участка. Результатом работы есть спроектирована и реализована интеллектуализированая программная система для качественного засаживания земельных участков под культуры, которые заказаны на импорт или экспорт, согласно выигранных тендеров.
Ключевые слова: математическая модель, прогнозная урожайность, севооборот, земельный участок, аграрий.

SYSTEM OF SEEDING PARTITION ON THE LAND PLOTS BASED ON A MATHEMATICAL MODEL FOR PREVIOUS CROPS ROTATION EFFECTS ON YIELD

S.Ya. Krepych, I.Ya. Spivak, A.R. Bayurskii

Ternopil national economic university,
Chehova St., 6, Ternopil, 46000, Ukraine; e-mail: msya220189@gmail.com

The work is devoted to the problem of the quality of cultivation of plants for the needs of the state or the needs of the external market. Products grown on the territory of Ukraine or goods obtained from the processing of the crops are attractive in many countries of the world. In order to increase the rate of export our goods abroad it is advisable to focus on improving crop growth that increase their yields. However, an appropriate increase in yield must be provided with the simultaneous support of land plots in a fertile state without the use of various types of pesticides, which have a negative effect on both the structure of the soil and the environmental condition of the environment. The value of the work is to develop a method for planting fields, which would allow farmers on the one hand to receive permanent income by offering their fields under the planting, and on the other hand, the customer (for example the state) have a constant export volume and at the same time save on purchases of products. In addition, the value is a development of a mathematical model of crop yield dependent on crop rotation within a specific area. The result is an intelligent software system designed and implemented that allow to use most quality land plots under cultivation, which are ordered for import or export in accordance with the winning tender.
Keywords: mathematical model, forecast yield, crop rotation, land, agrarian.

УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 8 (2018), No. 4, pp. 313-323

МЕТОД ВСТРАИВАНИЯ ИНФОРМАЦИИ В ЦИФРОВЫЕ ИЗОБРАЖЕНИЯ JPEG, МИНИМИЗИРУЮЩИЙ ПСИХОВИЗУАЛЬНЫЕ ИСКАЖЕНИЯ ДЛЯ МАЛЫХ ОБЪЕМОВ ВСТРОЕННОЙ ИНФОРМАЦИИ

А.С. Кирмичиева, Н.И. Кушниренко, А.А. Яковенко, Н.В. Калашников, А.Э. Лозан

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: nasananastia@ukr.net

Цифровые фотографии традиционно являются одним из наиболее распространенных типов стеганографических контейнеров. Подавляющее большинство цифровых фотографий хранится в сжатом виде с использованием алгоритмов семейства JPEG, или алгоритма webP, который структурно отличается от JPEG лишь в малозначительных деталях. Поскольку указанные алгоритмы не сохраняют точные значения пикселей, добавление скрытой информации в файлы такого типа предполагает добавление информации в т.н. пространстве преобразований (transform domain), другими словами, изменению подлежат квантованные коэффициенты дискретного косинусного преобразования (ДКП), именно те данные, которые остаются неизменными в процессе сжатия изображения. В широко распространенных стеганографических алгоритмах, работающих с такими форматами, обычно изменяются младшие значащие биты (LSB) квантованных компонентов ДКП блоков изображения. При этом внедрение обычно проводится последовательно, начиная с начальных блоков изображения. Исходя из этого, следует, что для усовершенствования метода необходимо изменение последовательности внедрения битов информации. В данной статье разработан стеганографический алгоритм для изображений JPEG, функционирующий в области квантованных ДКП-компонентов, который позволяет оценить психовизуальную заметность внедрения для каждого ДКП-компонента каждого блока изображения-носителя и произвести внедрение в те ДКП-компоненты, для которых заметность является минимальной. Для проверки эффективности стеганографического алгоритма используются объективные критерии, которые позволяют получить просто вычисляемую характеристику изображения разностного сигнала между двумя изображениями: исходным и преобразованным.

Ключевые слова: цифровая стеганография, JPEG, дискретное косинусное преобразование, квантование, DCT-коэффициенты, психовизуальная модель, IJG.

Введение

Цифровые фотографии традиционно являются одним из наиболее распространенных типов стеганографических контейнеров. Разработано множество алгоритмов, позволяющих добавлять скрытые данные к цифровым изображениям, а также множество алгоритмов, позволяющих детектировать внедрение по тому или иному алгоритму.

Подавляющее большинство цифровых фотографий хранится в сжатом виде с использованием алгоритмов семейства JPEG, или алгоритма webP, который структурно отличается от JPEG лишь в малозначительных деталях. Поскольку указанные алгоритмы не сохраняют точные значение пикселей, добавление скрытой информации в файлы такого типа предполагает добавление информации в т.н. пространстве преобразований (transform domain), другими словами, изменению подлежат квантованные коэффициенты дискретного косинусного преобразования (ДКП), именно те данные, которые остаются неизменными в процессе сжатия изображения.

В широко распространенных стеганографических алгоритмах, работающих с такими форматами, обычно изменяются младшие значащие биты (LSB) квантованных

компонентов ДКП блоков изображения. При этом внедрение обычно проводится последовательно, начиная с начальных блоков изображения.

Назовем компоненты ДКП блоков изображения, в которые может быть произведено внедрение, точками внедрения.

Если количество информации, которая должна быть добавлена в изображение, невелико по сравнению с количеством таких точек внедрения в изображении, то в распространенных алгоритмах заполняются только точки внедрения в начале изображения.

Цель работы

Целью данной статьи является разработка алгоритма, который позволяет создать карту точек внедрения в изображении, оценить каждую точку внедрения на предмет того, насколько заметно будет внедрение в эту точку согласно психовизуальной модели JPEG, и произвести внедрение в точки, начиная с самых «незаметных».

Таким образом, если размер внедряемого сообщения меньше количества точек внедрения, данные будут добавляться в те точки, которые приведут к наименьшей заметности внедрения. Если размер внедряемого сообщения равен количеству точек внедрения, то заметность внедрения будет соответствовать распространенным алгоритмам, например, JSTEG.

Основная часть

В первую очередь, необходимо провести анализ существующих стеганографических методов.

Методы замены в пространственной области. Метод замены младших бит (LSB-метод) основан на том, что младшие разряды графических, аудио- и видеоформатов несут мало информации и их изменение фактически не сказывается на качестве передаваемого изображения или звука. Это дает возможность использовать их для сокрытия конфиденциальной информации [1]. Основным преимуществом этого метода является простота реализации и возможность тайной передачи большого объема информации. Однако за счет введения дополнительной информации искажаются статистические характеристики файла-контейнера и скрытое сообщение легко обнаружить с помощью статистических методов стеганоанализа, таких как оценка энтропии и коэффициентов корреляции. Для снижения компрометирующих признаков требуется корректировка статистических характеристик. Недостатком метода является также его чувствительность к операциям цифровой обработки: сжатие, применение фильтрации, конвертации цветов, геометрических преобразований, дополнительного зашумления и изменения формата контейнера [2].

В методах, действующих в частотной области, данные скрываются в коэффициентах ортоганального преобразования контейнера. Для этого чаще всего используются преобразования, применяемые в современных алгоритмах сжатия с потерями (дискретное косинусное преобразование в стандарте JPEG и вейвлет-преобразование - в JPEG2000) [3]. Сокрытие информации может проводиться как в исходное изображение, так и одновременно с осуществлением сжатия изображения-контейнера. Важно, что стеганосистемы, в которых учтены особенности алгоритма сжатия, могут быть нечувствительны к дальнейшей компрессии контейнера [4]. Также они обеспечивают большую устойчивость к геометрическим преобразованиям и выявлению канала передачи (по сравнению с методом LSB), поскольку есть возможность в широком диапазоне варьировать качество сжатого изображения, что делает невозможным определение происхождения искажения.

В данной статье рассматривается один из методов, использующих частотную область, а именно, метод, основанный на внедрении битов сообщения в наименее заметные места на этапе дискретного косинусного преобразования, в связи с его стойкостью к различного рода превращениям и операциям цифровой обработки.

Рассмотрим подробно алгоритм сжатия изображения JPEG.

Алгоритм JPEG оперирует областями 8x8, на которых яркость меняется сравнительно плавно. Алгоритм разработан группой экспертов в области фотографии [5]. JPEG – Joint Photographic Expert Group – подразделение в рамках ISO – Международной организации по стандартизации. Шаги алгоритма изображены на рисунке 1.

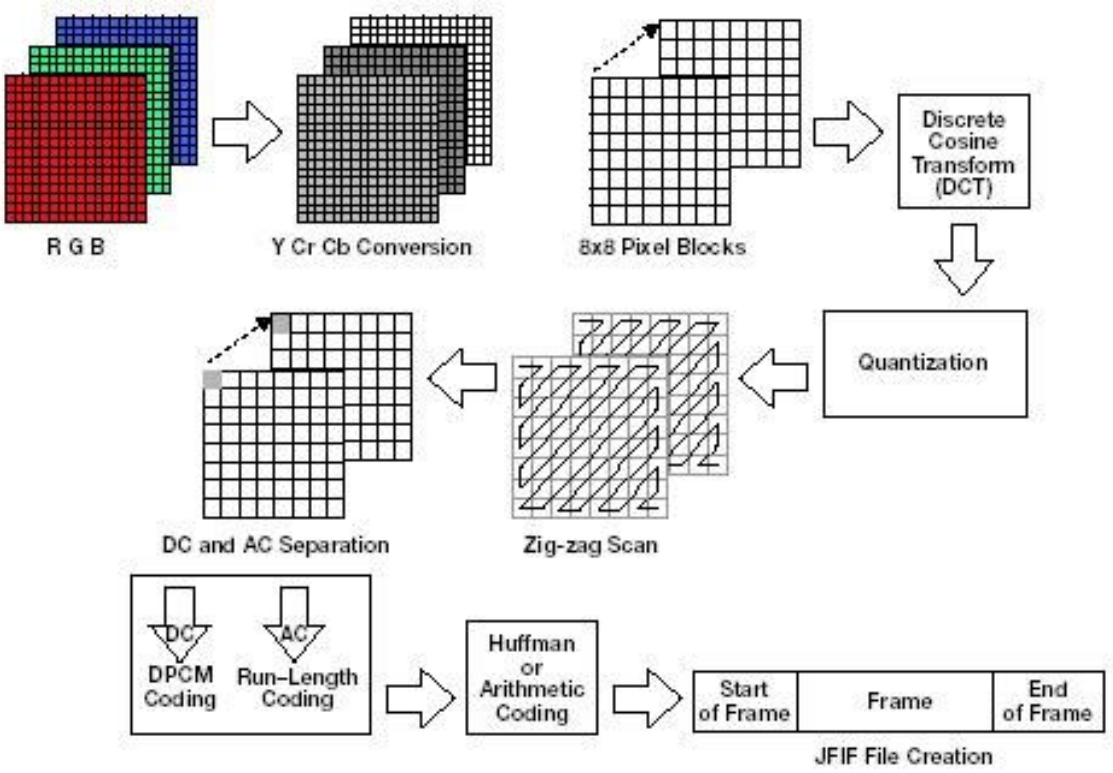


Рис. 1. Алгоритм сжатия изображения формата JPEG

В этом алгоритме изображение преобразуется из цветового пространства RGB в YCbCr, где Y – компонента яркости, а Cb и Cr – компоненты цветности. Поэтому важнее сохранить большую точность при передаче Y, чем при передаче Cb и Cr. Затем значения каналов разбиваются на блоки 8x8. Каждый блок подвергается дискретному косинусному преобразованию (ДКП), являющемуся разновидностью дискретного преобразования Фурье [6]. Таким образом, при преобразовании получается матрица, элементы которой соответствуют интенсивности различных пространственных частот исходного блока.

Для каждого элемента матрицы дискретного косинусного преобразования существует соответствующий элемент матрицы квантования. Результирующая матрица получается делением каждого элемента матрицы дискретного косинусного преобразования на соответствующий элемент матрицы квантования и последующим округлением результата до ближайшего целого числа. Как правило, значения элементов матрицы квантования растут в направлении слева направо и сверху вниз [7]. Для разработки алгоритма была выбрана стандартная матрица квантования стандарта IJG (рис. 2).

```
16, 11, 10, 16, 24, 40, 51, 61,
12, 12, 14, 19, 26, 58, 60, 55,
14, 13, 16, 24, 40, 57, 69, 56,
14, 17, 22, 29, 51, 87, 80, 62,
18, 22, 37, 56, 68, 109, 103, 77,
24, 35, 55, 64, 81, 104, 113, 92,
49, 64, 78, 87, 103, 121, 120, 101,
72, 92, 95, 98, 112, 100, 103, 99
```

Рис. 2. Матрица квантования IJG

Полученная матрица преобразуется в 64-элементный вектор при помощи «зигзаг»-преобразования. Таким образом, в начале вектора располагаются коэффициенты матрицы, соответствующие низким частотам, а в конце – высоким. Полученный вектор сворачивается с помощью алгоритма группового кодирования RLE, а затем кодируется кодами Хаффмана.

Чтобы сделать факт внедрения наименее заметным с точки зрения психовизуальной модели JPEG, необходимо выбрать для внедрения такие ДКП-компоненты блоков изображения, которые будут наименее заметны для человека.

Для определения степени незаметности изменения компонента, для каждого компонента рассчитывается рейтинг эффективности внедрения S.

Для подсчета рейтинга S используются два соображения:

- внедрение наименее заметно в том частотном компоненте, который наименее заметен для человеческого зрения. Для определения частотной незаметности используется рейтинг S_{HF};
- внедрение наименее заметно в тех компонентах, которые имеют высокое абсолютное значение, в них относительная мощность изменения будет минимальна. Для определения незаметности по значению используется рейтинг S_v.

Для того чтобы определить, какие частотные компоненты наименее заметны, используется психовизуальная модель JPEG, в частности, матрицы квантования IJG. Высокие числа в матрице квантования соответствуют частотным компонентам, которые с точки зрения психовизуальной модели JPEG являются наименее ценными для восприятия, то есть, наименее заметными. Внедрение в такие компоненты приведет к меньшим психовизуальным искажениям. Согласно подавляющему большинству матриц квантования JPEG, наименее заметными являются высокочастотные компоненты ДКП.

На базе матрицы квантования IJG, создается матрица S_{HF}, сопоставляющая каждому из 64 спектральных компонентов ДКП индекс заметности этого компонента S_{HF}.

С другой стороны, наименьшие визуальные искажения будут достигнуты в том случае, если абсолютная величина спектрального компонента велика, в таком случае изменение младшего значащего бита будет иметь наименьший психовизуальный эффект. Следовательно, рейтинг значения S_v должен быть тем больше, чем больше абсолютное значение компонента. Также надо учитывать, что в результате внедрения компонент может быть изменен вследствие изменения его младшего значащего бита. Для того, чтобы сохранить точное значение рейтинга до и после внедрения, используется среднее значение между парой чисел, которые отличаются только

младшим значащим битом. Например, для компонентов со значением 2 и 3, рейтинг S_v составляет 2.5, для значений 4 и 5 рейтинг S_v составляет 4.5 (рис. 3).

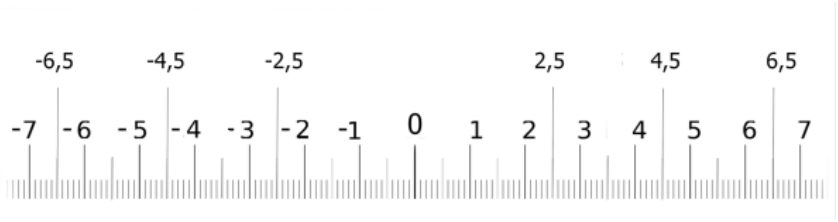


Рис. 3. Оптимизация рейтинга

Суммарный рейтинг незаметности в таком случае определяется следующим образом:

$$S = \sum (S_{HF} S_V).$$

Проведём непосредственное внедрение информации. Для проведения эксперимента было выбрано изображения с разрешением 780x507 пикселей (рис. 4). Текст внедряемого сообщения представлен в виде двоичного вектора.

Рис. 4. Исходное изображение

Основные шаги разработанного метода внедрения сообщения в контейнер изображение формата JPEG.

Шаг 1. Переход из пространства RGB в пространство YCrCb.

Шаг 2. Разделение изображение на блоки – октеты 8x8 пикселей.

Шаг 3. К каждому октету применяется двумерное дискретное косинусное преобразование. В результате получается вещественный спектр октета - spectrum.

Шаг 4. Сформированные блоки поддаются квантованию. Далее из них формируется многомерный массив.

Шаг 5. Для каждого компонента spectrum вычисляется рейтинг – S. Рейтинг указывает, насколько удачен тот или иной компонент, для встраивания в него бита сообщения.

Таким образом, берутся все спектральные компоненты всех октетов изображения, и для каждого из них находится значение S. Далее производится сортировка компонентов по уменьшению его S. В полученном списке будет указываться величина компонента и его местонахождение.

Результатом этого является способ создания рейтинга значений спектрального компонента, который не зависит от того, было проведено внедрение в этот компонент или нет.

Внедрение сообщения в наименее заметные места. Сообщение представляется в виде последовательности бит, и эти биты заменяют младшие значащие биты выбранных частотных компонентов изображения, начиная с самых благоприятных согласно рейтингу S (рис. 5).

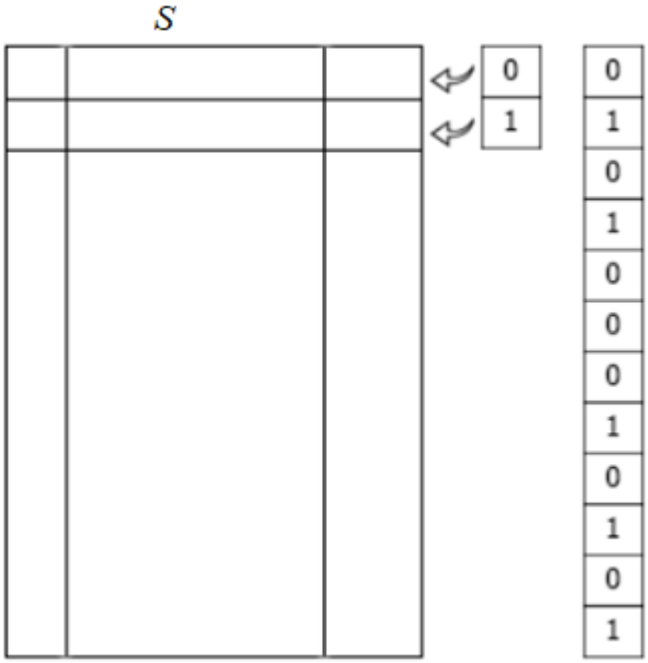


Рис. 5. Внедрение сообщения

Завершается сжатие изображения (рис. 6).

Рис. 6. Результат алгоритма

Как видно, на первый взгляд, изображения идентичны. Однако, при выделении и усилении разницы между изображениями, можно заметить незначительные, незаметные различия (рис. 7).

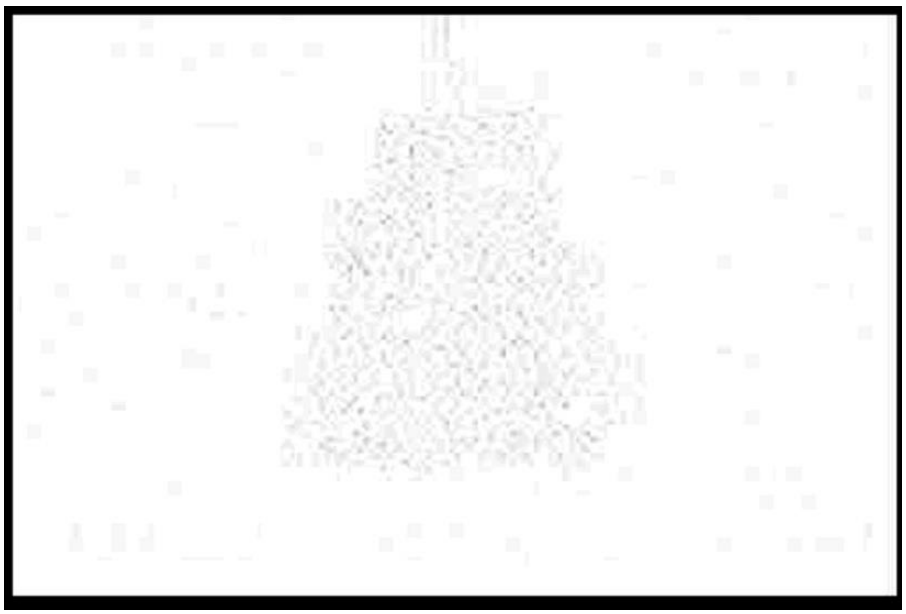


Рис. 7. Разница изображений

Реализация рассмотренного метода осуществлялась в среде математических вычислений Matlab. Для наглядности изменений сравниваются статистические показатели контейнера в исследуемом методе в зависимости от внедрения различной длины сообщения.

При изучении действия разработанного метода проводилось сравнение цветных изображений, в которые вводились сообщения различной длины (рис. 8, рис. 9, рис. 10).

При разности этих изображений с оригиналом можно рассмотреть значительные изменения количества мест внедрения информации.

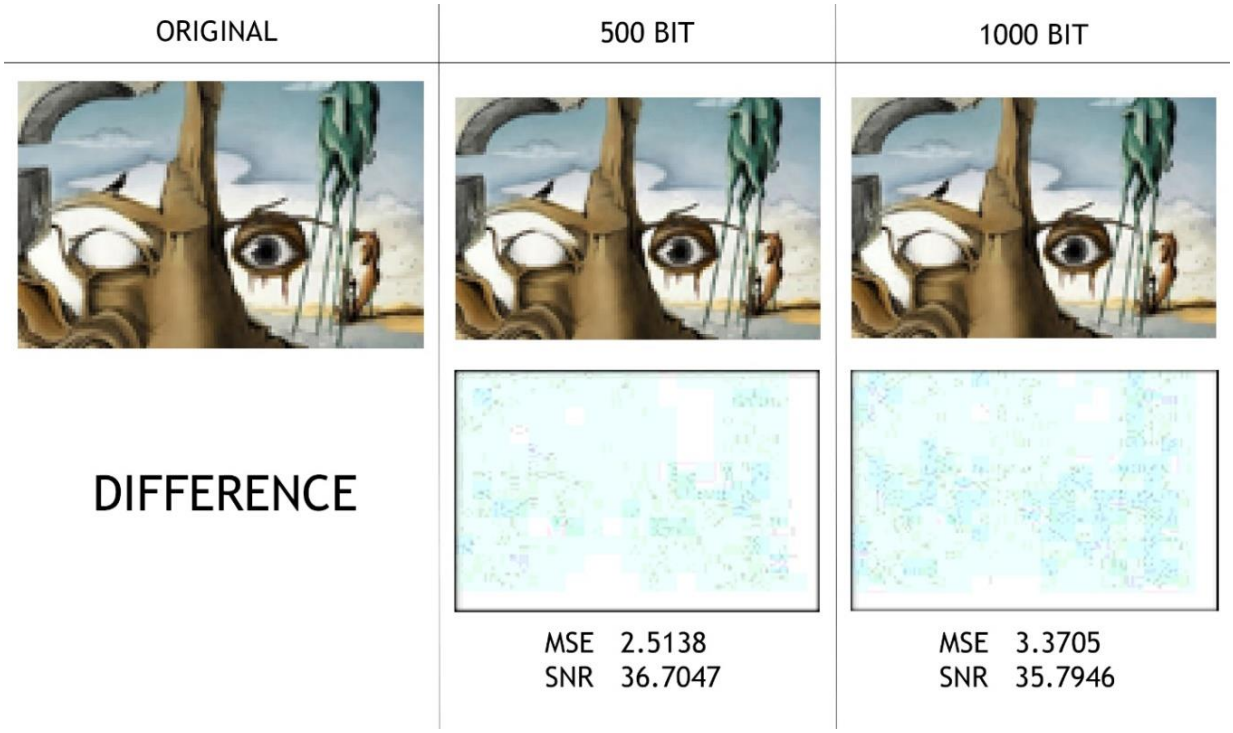


Рис. 8. Первое цветное изображение

Рис. 9. Второе цветное изображение

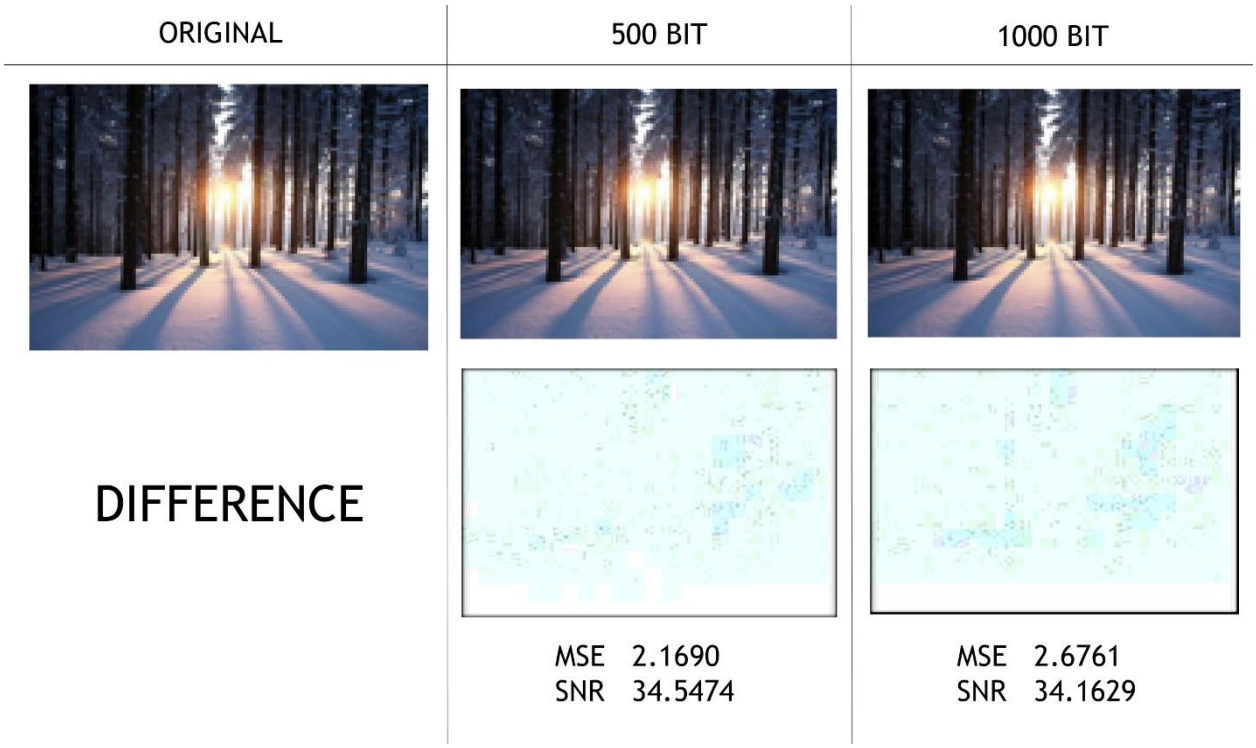


Рис. 10. Третье цветное изображение

Для оценки качества изображения воспользуемся объективными критериями, которые позволяют получить просто вычисляемую характеристику изображения разностного сигнала между двумя изображениями: исходным и преобразованным. Данные критерии позволяют оценивать количественные изменения значений яркости, уровень искажений изображений при их преобразованиях (фильтрации, сжатии данных и т.д.), то есть, по существу, качество самого средства преобразования – алгоритма или системы.

К таким критериям относится, прежде всего, среднеквадратический критерий (MSE). По нему мерой различия двух изображений является среднеквадратическое значение разностного сигнала двух изображений [8].

Ниже представлен график изменения среднеквадратической ошибки в зависимости от количества внедряемых бит сообщения (рис. 11).

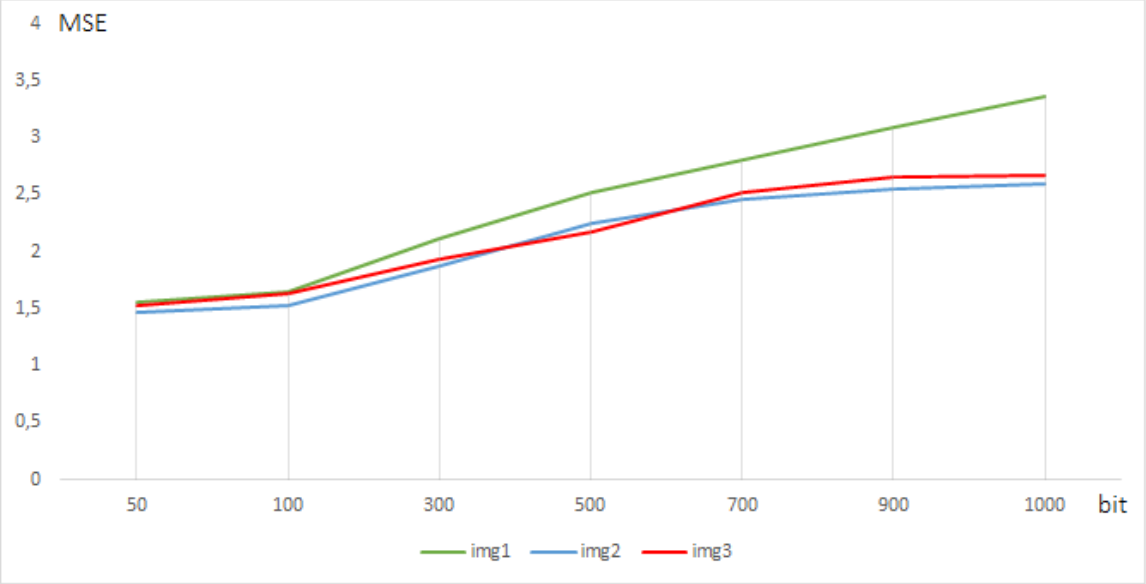


Рис. 11. График изменения среднеквадратической ошибки

Так, при увеличении длины встраиваемого сообщения нормированная среднеквадратическая ошибка увеличивается.

Для анализа уровня искажений, которые вносятся в контейнер во время сокрытия в нем информации, воспользуемся соотношением «сигнал/шум» – SNR [9].

На графике наблюдается уменьшение SNR, что означает увеличение шума и показывает изменения в статистических характеристиках контейнера (рис. 12).

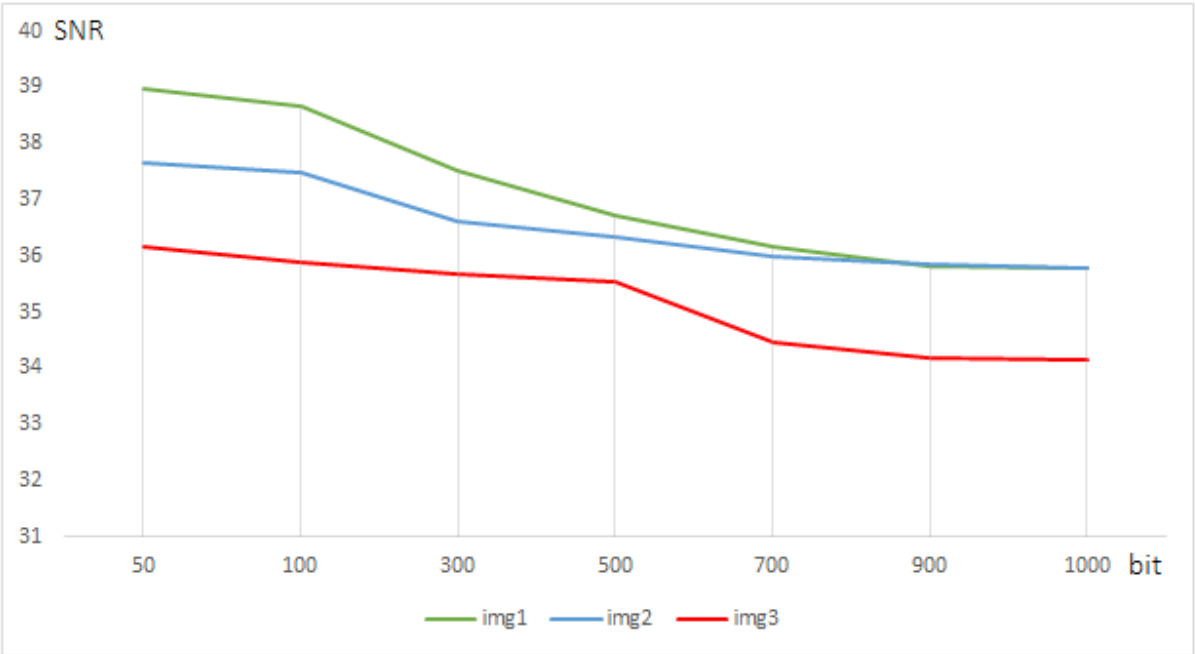


Рис. 12. График отношения сигнал/шум

Благодаря тому, что данный метод внедряет биты информации именно в статистически наиболее «удачные» места, изменения среднеквадратической ошибки и значения шума увеличиваются незначительно.

Выводы

В данной работе был разработан стеганографический алгоритм сокрытия информации в спектре изображения файла JPEG с учётом рейтинга значений спектральных компонентов. В статье были описаны основные принципы сжатия формата JPEG. Был произведён анализ методов цифровой стеганографии. На основе этого анализа, был разработан альтернативный метод внедрения, который находит наименее заметные места в изображении. Проведён статистический анализ зависимости искажений изображения от количества внедряемых бит информации.

Список литературы

1. Грибунин, В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. — М.: Солон-Пресс, 2009. – 272 с.
2. Fridrich, J. Steganography in Digital Media: Principles, Algorithms, and Applications // Cambridge University Press; 1 edition. – 2009. – Pp. 352-356.
3. Yang, C.N. Steganography and Watermarking / C.N. Yang, C.C. Lin, C.C. Chang // Nova Science Publishers Inc. – 2013. – 200 p.
4. Таранчук, А.А. Стеганографічний метод приховування даних в області частотних перетворень зображень / А.А. Таранчук, Л.Г. Гальпер // Вісник Хмельницького національного Університету, 2009. – № 2. – С. 197-201.
5. Raggo, M.R. Data Hiding: Exposing Concealed Data in Multimedia, Operating Systems, Mobile Devices and Network Protocols / M.T. Raggo, Chet Hosmer // Syngress. – 2012. – Pp. 115-117.
6. Калашніков, М.В. Статистичне виявлення стеганографічних повідомлень у зображеннях формату JPEG / М.В. Калашніков, О.О. Яковенко, Н.І. Кушніренко // Електротехнічні та комп'ютерні системи. – 2017. – № 25(101). – С. 310-316.
7. Wang, Y. Steganalysis of block-DCT image steganography / Y. Wang, P. Moulin // University of Illinois at Urbana-Champaign; Beckman Institute, CSL&ECE Dept., Urbana, USA.
8. Фисенко, В.Т. Компьютерная обработка и распознавание изображений / В.Т. Фисенко, Т.Ю. Фисенко // Санкт-Петербургский государственный университет информационных технологий, механики и оптики. – 2009. – 192 с.
9. Кушніренко, Н.І. Урахування статистичних властивостей контейнеру для стеганографічного алгоритму / Н.І. Кушніренко, В.Я. Чечельницький, М.В. Калашніков, О.О. Яковенко // Електротехнічні та комп'ютерні системи. – 2016. – № 23(99). – С. 83-87.

METHOD OF INTRODUCING INFORMATION IN DIGITAL IMAGES JPEG, MINIMIZING PSYCHO-VISUAL DISTORTIONS FOR SMALL VOLUMES OF IMPROVED INFORMATION

A.S. Kirmichiieva, N.I. Kushnirenko, O.O. Iakovenko, M.V. Kalashnikov, A.E. Lozan

Odessa National Polytechnic University,
Shevchenko Avenue, 1, Odessa, 65044, Ukraine; e-mail: nasananastia@ukr.net

Digital photos are traditionally one of the most common types of steganographic containers. The vast majority of digital photographs are stored in a compressed form using algorithms of the JPEG family, or the webP algorithm, which is structurally different from JPEG only in minor details. Since these algorithms do not preserve the exact value of the pixels, adding hidden information to files of this type implies adding information to the so-called. transform domain (transform domain), in other words, quantized coefficients of discrete cosine transform (DCT) are subject to change, namely the data that remains unchanged during image compression. In the widespread steganographic algorithms working with such formats, the least significant bits (LSB) of quantized DCT components of image blocks usually change. In this case, the introduction is usually carried out

sequentially, starting with the initial blocks of the image. On this basis, it follows that in order to improve the method, it is necessary to change the sequence of implementation of the information bits. This article has developed a steganographic algorithm for JPEG images, which functions in the area of quantized DCT components, which allows us to evaluate the psycho-visual conspicuity of embedding for each DCT component of each block of the image carrier and embed them into those DCT components for which the visibility is minimal. To verify the effectiveness of the steganographic algorithm, objective criteria are used that allow one to obtain simply a calculated characteristic of the image of a difference signal between two images: the original and the transformed one.
Keywords: digital steganography, JPEG, discrete cosine transform, quantization, DCT coefficients, psycho-visual model, IJG.

МЕТОД ВБУДОВИ ІНФОРМАЦІЇ В ЦИФРОВІ ЗОБРАЖЕННЯ JPEG, ЩО МІНІМІЗУЄ ПСИХОВІЗУАЛЬНІ СПОТВОРЕННЯ ДЛЯ МАЛИХ ОБСЯГІВ ВБУДОВАНОЇ ІНФОРМАЦІЇ

А.С. Кірмічієва, Н.І. Кушніренко, О.О. Яковенко, М.В. Калашніков, А.Е. Лозан

Одеський національний політехнічний університет,
проспект Шевченка, 1, Одеса, 65044, Україна; e-mail: nasananastia@ukr.net

Цифрові фотографії традиційно є одним з найбільш поширених типів стеганографічних контейнерів. Переважна більшість цифрових фотографій зберігається в стислому вигляді з використанням алгоритмів сімейства JPEG, або алгоритму webP, який структурно відрізняється від JPEG лише в незначних деталях. Оскільки зазначені алгоритми не зберігають точні значення пікселів, додавання прихованої інформації в файли такого типу передбачає додавання інформації в т.зв. просторі перетворень (transform domain), іншими словами, зміні підлягають квантовані коефіцієнти дискретного косинусного перетворення (ДКП), саме ті дані, які залишаються незмінними в процесі стиснення зображення. В широко поширених стеганографічних алгоритмах, які працюють з такими форматами, як правило змінюються молодші значущі біти (LSB) квантованих компонентів ДКП блоків зображення. При цьому впровадження зазвичай проводиться послідовно, починаючи з початкових блоків зображення. Виходячи з цього, можна сказати, що для удосконалення методу необхідна зміна послідовності впровадження бітів інформації. У даній статті розроблено стеганографічний алгоритм для зображень JPEG, що функціонує в області квантових ДКП-компонентів, який дозволяє оцінити психовізуальну помітність впровадження для кожного ДКП-компонента кожного блоку зображення-носія, і зробити впровадження в ті ДКП-компоненти, для яких помітність є мінімальною. Для перевірки ефективності стеганографічного алгоритму використовуються об'єктивні критерії, які дозволяють отримати просто обчислювану характеристику зображення від'ємного сигналу між двома зображеннями: вихідним і перетвореним.
Ключові слова: цифрова стеганографія, JPEG, дискретне косинусное перетворення, квантування, DCT коефіцієнти, психовізуальна модель, IJG.

УДК 581.3

Informatics and Mathematical Methods in Simulation
Vol. 8 (2018), No. 4, pp. 324-333

АЛГОРИТМИ ПОШУКУ ЗАЛИШКІВ ДОВГИХ ЧИСЕЛ ДЛЯ ЗАДАЧ АСИМЕТРИЧНОЇ КРИПТОГРАФІЇ

Л.М. Тимошенко[1], С.В. Івасьєв[2], О.Я. Лотоцький[3], В.М. Гаврилей[1]

[1]Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: lmt0902@gmail.com
[2]Тернопільський національний економічний університет, вул. Львівська, 11, Тернопіль, 46020, Україна;
e-mail: stepan.ivasiev@gmail.com
[3]Національний авіаційний університет,
просп. Космонавта Комарова,1, Київ, 03058, Україна, e-mail: zyzik2323@gmail.com

На сучасному етапі забезпечення інформаційної безпеки держави важливим є засекречування мереж зв'язку військового призначення, одним із ключових напрямів якого є застосування криптографічних методів захисту інформації, зокрема, асиметричної криптографії. Одним із шляхів удосконалення алгоритмів асиметричної криптографії є знаходження залишків довгих чисел. Відомі алгоритми пошуку залишків довгих чисел мають ряд суттєвих недоліків при їх реалізації. В роботі проводиться аналіз заявлених двох нових методів пошуку залишків довгих чисел, їх недоліків та обчислювальних складностей. Описано запропонований авторами метод, наведено його алгоритм та блок-схема. Досліджуються обчислювальні складності трьох розглянутих методів пошуку залишків. Чисельний експеримент оцінки складностей показує, що при виконанні модульних операцій, які використовуються в асиметричних криптоалгоритмах, при переведенні чисел з десяткової системи в систему числення залишкових класів слід використовувати запропонований метод, який характеризується меншою складністю. Для подальшого розгляду залишаються два. Виграш в ефективності запропонованого алгоритму відносно відомого визначається як співвідношення обчислювальних складностей і дорівнює 2. Розроблений на мові програмування високого рівня C++ додаток дозволяє дослідити часові характеристики виконання двох методів. В роботі наведено фрагмент тестування додатку для подвійних чисел Мерсенна та графічне зображення залежності часу знаходження залишків великих чисел від простого числа, для якого знаходиться залишок. Розроблений алгоритм пошуку залишків великих чисел дозволив підвищити швидкодію порівняно з відомим за рахунок використання властивостей залишків та числового базису Радемахера. Це зменшило обчислювальну складність та підвищило виграш у ефективності роботи алгоритму у порівнянні з відомим у два рази, що доводить доцільність його використання при опрацюванні довгих чисел в асиметричних криптографічних системах захисту інформації для підвищення швидкодії процесів шифрування та криптоаналізу.

Ключові слова: асиметрична криптографія, довга арифметика, система залишкових класів, обчислювальна складність, залишки довгих чисел.

Вступ

На жаль, сьогодні триває гібридна війна та військова агресія проти України, тому забезпечення захисту інформації є надважливим завданням інформаційної безпеки держави на даному етапі її розвитку. Перемога у сучасній війні залежить, зокрема, і від засекречування мереж зв'язку військового призначення у системі військового управління [1,2] в процесі переходу системи зв'язку Збройних сил України з аналогових на цифрові телекомунікаційні засоби.

На сучасному етапі розвитку інформаційно-технічних засобів передачі та зберігання інформації одним із шляхів захисту інформації є застосування криптографічних методів, заснованих на принципі Керкгоффза, згідно з яким стійкість криптографічного алгоритму ґрунтується на секретності ключа, а не на таємності

алгоритму шифрування [3,4]. В мережах зв'язку, як правило, використовують альтернативу шифрування з симетричними ключами – криптографічні системи, що поєднують використання пари ключів – відкритого і закритого. Один з них публікують у відкритих джерелах і використовують для шифрування даних, інший ключ тримають в секреті і застосовують для декодування повідомлення. Основна перевага асиметричних шифрів – відсутність необхідності передачі секретного ключа. Вони використовують так звані незворотні чи односторонні функції з властивістю: при заданому значенні x досить легко обчислити значення $f(x)$, проте, якщо $y = f(x)$, то немає простого шляху для обчислення значення x. Зокрема, алгоритм Діффі-Хеллмана побудовано на обчисленні дискретного логарифма у скінченному полі простих чисел, а алгоритм *RSA* – на задачі факторизації. Такі алгоритми використовують арифметику довгих чисел, причому з метою запобігання відомих атак розміри чисел повинні перевищувати 10^{309} [5-7].

Одним із шляхів удосконалення алгоритмів асиметричної криптографії (зокрема, алгоритмів *RSA*, Рабіна, Ель-Гамаля, з використанням еліптичних кривих, електронного цифрового підпису, дослідження порядку еліптичної кривої за допомогою алгоритму Шуфа тощо) є застосування системи залишкових класів [8, 9], і звідси – знаходження залишків довгих чисел [10]. У зв'язку з цим актуальною задачею, яка розглядається в даній роботі, є дослідження існуючих алгоритмів пошуку залишків довгих чисел та розробка нових ефективних алгоритмів.

Розповсюдженим методом пошуку залишків довгих чисел можна вважати такий алгоритм. Для знаходження залишку необхідно виконати ділення, виділити цілу частину від ділення, знайти добуток цілої частини на модуль, та знайти різницю числа і знайденого добутку. Також можна від великого числа віднімати модуль, доки різниця не стане меншою від'ємника. Оскільки числа, над якими виконуються операції, на кожному кроці зменшуються, то такий процес закінчиться через певну кількість кроків [11,12]. Дані алгоритми можна програмно реалізувати, але їх часова складність велика, оскільки операція ділення досить трудомістка. Іншим недоліком алгоритмів пошуку залишків великих чисел є послідовний порядок виконання операцій, тобто неможливість розпаралелення.

Мета роботи

Метою роботи є підвищення ефективності алгоритму пошуку залишків довгих чисел для зростання швидкодії виконання операцій над довгими числами, що використовуються в асиметричних криптосистемах захисту інформації. Ефективність алгоритмів пошуку залишків великих чисел в даній роботі оцінюється їх обчислювальною складністю.

Об'єкт дослідження – процеси програмного опрацювання довгих чисел в криптографічних системах захисту інформації. Предмет дослідження – алгоритми та методи опрацювання довгих чисел, що використовуються в процесах шифрування та криптоаналізу.

Основна частина

Для знаходження залишку великого двійкового числа Y по великому цілочисельному модулю P, який представлено у доповняльному коді для виконання операції віднімання, авторами у [13] запропоновано метод, який ґрунтується на рекурсивному співвідношенні:

$$b_i = [P]_{мд} + 2b_{i-1} + a_i,\ i = n-1,...,0, \quad (1)$$

де n – розрядність числа Y, для якого визначають залишок b_i; a_i – біти двійкового числа $Y = \sum_{i=0}^{n-1} a_i 2^i$, починаючи зі старшого розряду a_{n-1}; $[P]_{мд}$ – $(k+1)$-розрядна мантиса доповняльного коду модуля P; b_i – поточне кодове значення залишку $(b_{i-1} = 0)$.

Функціональним обмеженням даного методу є наявність операцій додавання доповняльних кодів двійкового числа для визначення залишку по модулю P, що знижує швидкодію, тобто потребує n додавань n - розрядних чисел. Обчислювальна складність даного методу складе $O(n^2)$.

У [14] запропоновано метод пошуку залишку b_i двійкового числа $Y = \sum_{i=0}^{n-1} y_i 2^i$, який починається з його старшого розряду y_{n-1}, по модулю P, де y_i – значення i-го біта числа, в основу якого покладено рекурентне співвідношення:

$$b_i = (a_i + 2b_{i-1}) \bmod P_j, \quad (2)$$

де b_{i-1} – значення залишку $(i-1)$-го біта двійкового числа.

Двійковий код порозрядно зчитують, починаючи зі старших розрядів, підсумовують його з подвоєним кодом попереднього залишку, починаючи з його нульового значення та формують новий код залишку по модулю з постійної пам'яті, який після n повторень таких операцій зчитується як кінцевий код залишку, починаючи зі старшого розряду. Шуканий кінцевий залишок b_0 отримують згідно виразу $b_0 = resY (\bmod P)$, де *res* - символ операції визначення найменшого невід'ємного залишку. У випадку, якщо двійкове число буде займати 512 біт, а модуль, за яким обчислюють залишок, буде від 2 до 128 біт, то швидкодія в порівнянні з попереднім способом, зросте від 2-х до 48-ми разів.

Функціональним обмеженням даного алгоритму є постійне звертання до пам'яті, яке призводить до значних затрат часу, окрім лінійного зростання часової складності виконання операції міжбазисного перетворення Рademахера та десяткової системи числення пропорційно розрядності двійкових чисел, що обмежує можливості його використання при опрацюванні довгих чисел. Загальна часова складність запропонованого у роботі [14] методу складає $O1 = O(2n \cdot \log_2 n)$.

Загальний недолік розглянутих в [13, 14] схем пошуку залишків є отримання не завжди найменших залишків та надлишковість порівнянь.

В основу запропонованого методу покладено наступні ідеї. Якщо від числа *Y* відняти число, кратне модулю *P*, то його залишок по цьому модулю не зміниться. Та друга – у двійковій арифметиці множення на $2_{(10)}=10_{(2)}$ – це дописування нуля зправа до числа.

Для знаходження залишку *L* великого числа *Y* по великому цілочисельному модулю *P* подамо числа *Y* та *P* у вигляді:

$$Y = \sum_{i=0}^{n-1} y_i 2^i,\ де\ y_i = 0,1,\ P = \sum_{i=0}^{k-1} p_i 2^i,\ де\ p_i = 0,1.$$

Тут *n* – кількість цифр (знаків) числа, *i* – порядковий номер цифри.

Необхідно знайти $Y \bmod P = L$.

Виділяємо $(n-k-2)$ молодших розрядів числа Y і доповнюємо модуль нулями. Одержимо число S у двійковому поданні:

$$S = (p_{k-1}, p_{k-2}, ..., p_{0,} 0, ..., 0). \quad (3)$$

Якщо $(k-1)$ старших розрядів $Y \geq P$, знаходимо $Y \bmod S$, шляхом віднімання: $Y - S = M$. Подаємо число $M = \sum_{i=1}^{n-k-2} M_i 2^i$, , звідси

$$M = (M_{n-k-2}, M_{n-k-3}, ..., M_1, M_0). \quad (4)$$

Якщо $M \geq P$, то формуємо наступне число шляхом дописування в молодший розряд $P(n-2k-3)$ нулів – $L = (p_{k-1}, p_{k-2}, ..., p_{0,} 0, ..., 0)$.

Якщо $M \geq L$, то обчислюємо значення $M \bmod L = M - L$, де

$$U = (U_{n-2k-3}, U_{n-2k-4}, ..., U_1, U_0).$$

Якщо $U \geq P$, то дописуємо в молодший розряд $P(n-3k-4)$ нулів – $F = (p_{k-1}, p_{k-2}, ..., p_1, p_0, 0, ..., 0)$.

Якщо $U \geq F$, то обчислюємо значення $U \bmod F = U - F = H$.

Описану процедуру продовжуємо доти, доки двійкове число $H = (H_{n-3k-4}, H_{n-3k-5}, ..., H_1, H_0)$ не буде менше за P.

Для знаходження залишку числа обчислюємо:

$$Y \bmod P = U \bmod F = H.$$

Алгоритм знаходження залишку великого числа за певним модулем представимо такими кроками.

Вхід: Y, P.

Крок 1. Двійкове подання числа P: $P(p_n ... p_0)$.

Крок 2. Зменшення розрядності n подання числа P на кількість одиниць від p_n до p_i (поки $p_i = 0$), запис у двійкове число $K(k_m ... k_0)$.

Крок 3. Зміна $Y = Y - n - 1$.

Крок 4. Додавання числа K у двійковому поданні до числа P з урахуванням позиції бітів.

Крок 5. Зменшення бітової розрядності m числа K на кількість одиниць від k_m до k_i, і запис у число K.

Крок 6. Зміна $Y = Y - m - j$.

Крок 7. Перехід на крок 5, доки $Y \geq P$.

Вихід: $K = resY \bmod P$.

На рисунку 1 подано блок-схему алгоритму пошуку залишків великих чисел.

Основними перевагами даного алгоритму в порівнянні з описаними в роботах [13,14] є зменшення надлишкового використання пам'яті та кількості порівнянь, і зменшення кількості операцій додавання пропорційно розрядності чисел. Часова складність даного алгоритму становить $O2 = O(n \cdot \log_2 n)$.

На рисунку 2 представлено графічні залежності обчислювальних складностей методів, описаних в [13, 14], та запропонованого вище методу.

Ефективність алгоритмів пошуку залишків великих чисел в даній роботі оцінюється їх обчислювальною складністю. Виходячи з графіка, далі покажемо порівняння ефективностей методу з [14] та вищеописаного методу.

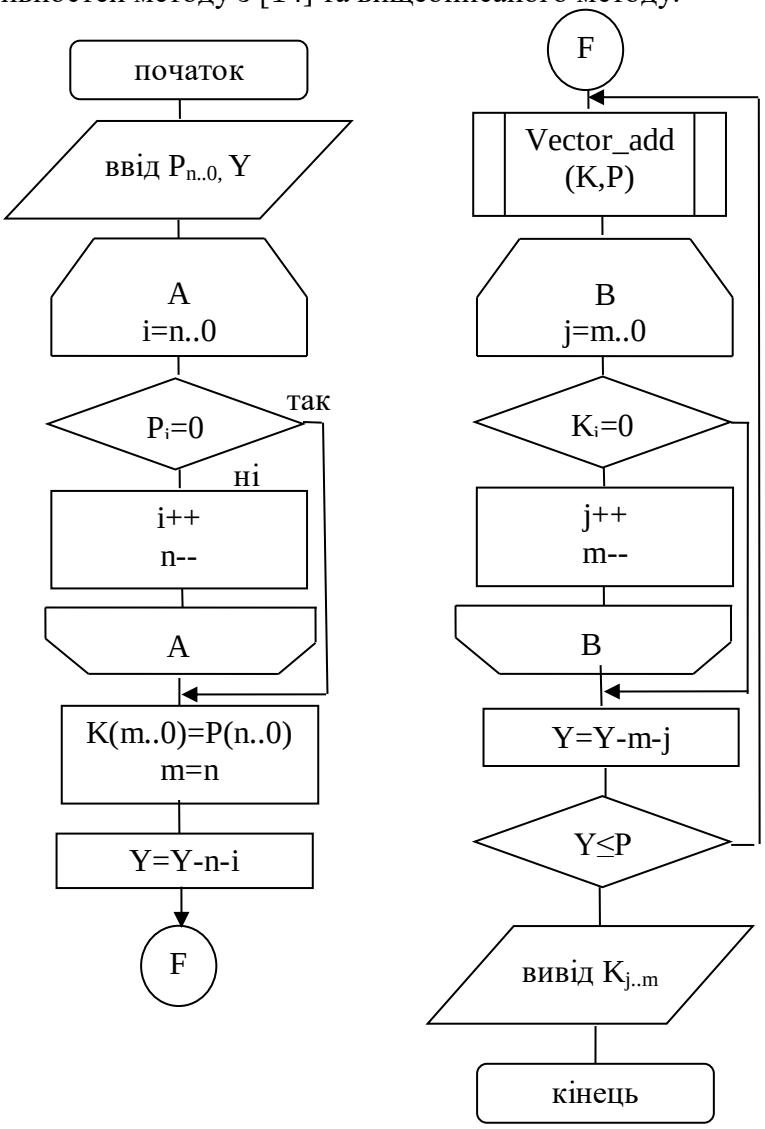


Рис. 1. Блок-схема алгоритму пошуку залишків довгих чисел

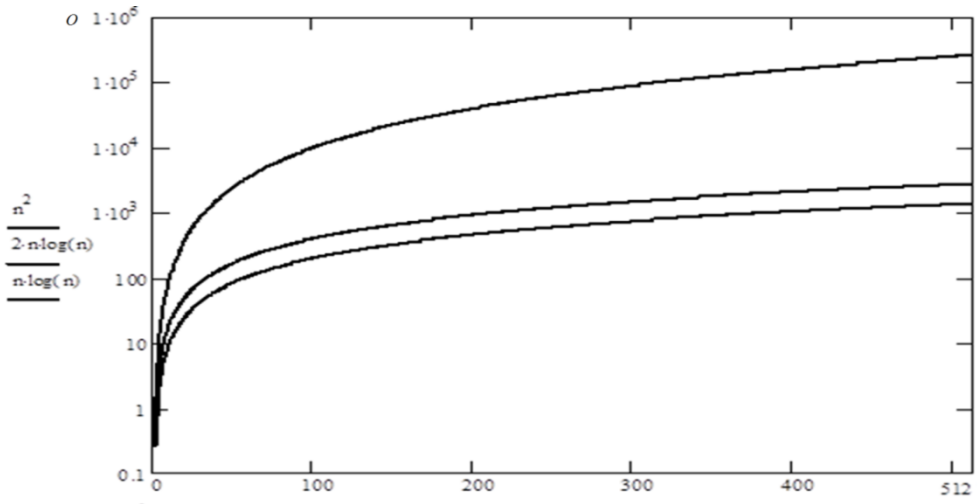


Рис. 2. Графічні залежності обчислювальних складностей відомих та запропонованого методу

Виграш в ефективності запропонованого в роботі алгоритму відносно відомого визначимо як співвідношення обчислювальних складностей:

$$E(n) = O1 / O2 = 2.$$

Отже, виграш в ефективності запропонованого методу при зростанні розрядності чисел зростає в 2 рази.

Чисельний експеримент оцінки складностей відомих і розробленого методу пошуку залишків великих чисел показує, що при виконанні модульних операцій, які використовуються в симетричних та асиметричних криптоалгоритмах, при переведенні чисел з десяткової системи числення в систему числення залишкових класів слід використовувати запропонований метод, який характеризується меншою складністю.

Оскільки при вирішенні окремих задач число операцій додавання може перевищити 2^{32}, то збільшення ефективності в два рази є суттєвим і значно розширює функціональні можливості опрацювання великих чисел.

Отже, розроблений метод з використанням операцій в числовому базисі Радемахера доцільно використовувати при опрацюванні інформаційних потоків, включаючи арифметичні операції та перевірку чисел на простоту, факторизацію та інші операції.

З метою забезпечення високої точності опрацювання інформації у базисах полів Галуа, необхідно вибирати великі значення простих модулів P, що задовольняють діофантовому рівнянню $2^q \equiv 1(2^q - 1)$, що приводить до арифметики по модулю $P = 2^k - 1$ і $P = 2^k + 1$. Такими числами є відомі числа Мерсенна $P = 2^q - 1$, де q – просте число, і Ферма $F_n = 2^{2^n} + 1$, де n – ціле число.

Для реалізації алгоритмів обрано мову програмування С++, середовище програмування С++ Buider 6.0. Додаток дозволяє дослідити часові характеристики виконання двох методів. Після запуску на екрані буде відображатись форма, що зображена на рисунку 3.

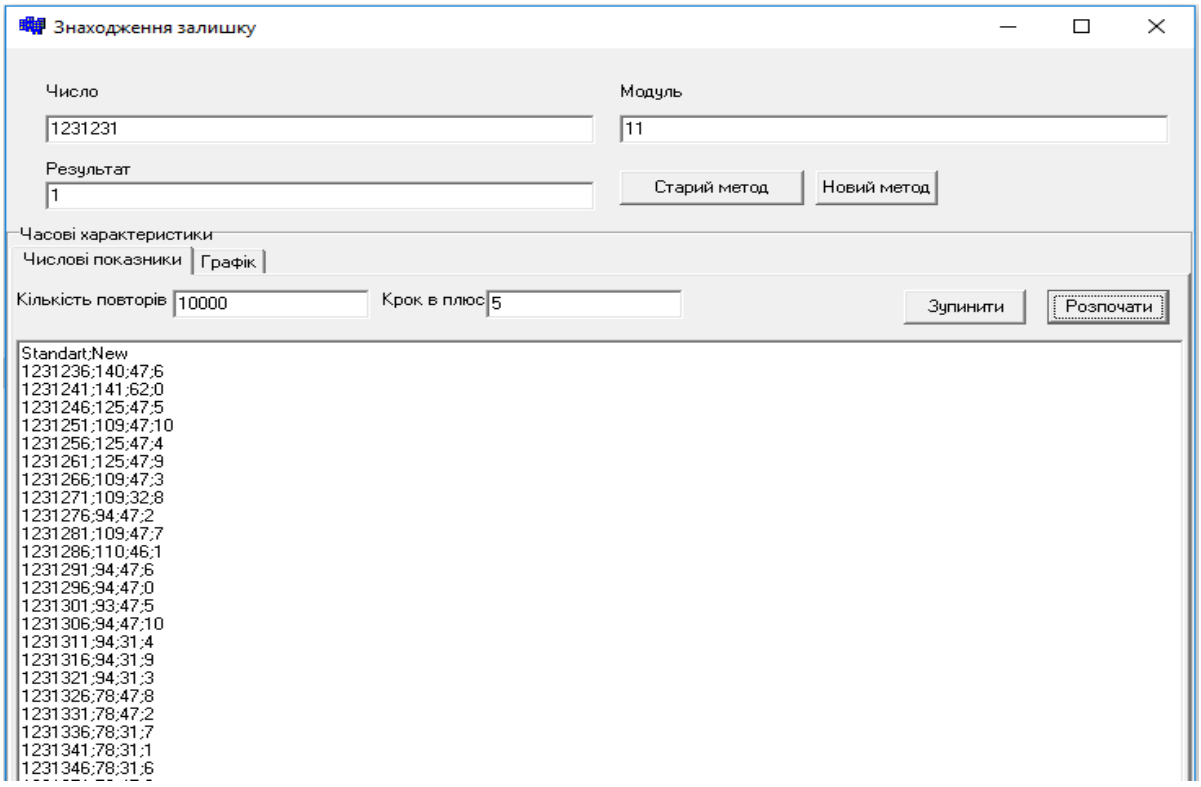


Рис. 3. Головна форма додатку

Додаток дозволяє порівняти швидкість виконання операцій знаходження залишку впорядкованої числової послідовності з випадково згенерованими модулями двома методами. Для аналізу та візуального порівняння одержаних часових характеристик роботи програми є можливість графічного відображення процесу. Верхню межу чисел можна вказати у відповідному полі головної форми.

Для проведення експериментів при дослідженні часових характеристик реалізована ітераційна затримка, оскільки процесорний час між потоками розподіляється нерівномірно. Контрольні дані відображаються на кожному кроці алгоритму знаходження залишку. Фрагмент тестування додатку для подвійних чисел Мерсенна показано в таблиці 1.

Таблиця 1.

Результати тестування для чисел Мерсенна

Число	Модуль	CLOCKS методу 1	CLOCKS методу 2
2^{32}-1	3811	62	31
2^{64}-1	3811	78	68
2^{128}-1	3811	78	63
2^{256}-1	3811	234	230
2^{512}-1	3811	1264	1092
2^{1024}-1	3811	4072	3120
2^{2048}-1	3811	14383	8674

У таблиці наведено CLOCKS двох методів – це кількість часових тактів з початку запуску програми.

Для тестування програмного продукту передбачено пошук залишку за вказаним модулем з певним кроком, який задається користувачем. На рис. 4 наведено графічне зображення залежності часу знаходження залишків великих чисел від номера по порядку наступного простого числа, для якого знаходиться залишок. Початкове число 1231231, за модулем 11, та кроком 5. Експеримент виконано для 1000 початкових чисел. Верхня ламана – для відомого алгоритму, нижня для запропонованого.

З рисунка видно, що час знаходження залишку за новим алгоритмом суттєво менший від відомого. Таким чином одержали експериментальне підтвердження теоретичним викладкам.

Висновки

У роботі проаналізовано відомі швидкодіючі алгоритми опрацювання великих чисел та запропоновано свої рішення для підвищення швидкодії; виконано порівняльний аналіз ефективності запропонованого і відомого методів; розроблено програмні засоби реалізації попередньо розглянутих алгоритмів та досліджено їх роботу.

Розроблений у результаті роботи алгоритм пошуку залишків великих чисел дозволив отримати підвищення швидкодії порівняно з відомим за рахунок використання властивостей залишків та числового базису Радемахера. Це значно зменшило обчислювальну складність та підвищило виграш у ефективності роботи алгоритму у порівнянні з відомим у два рази, що підтверджено експериментальними дослідженнями.

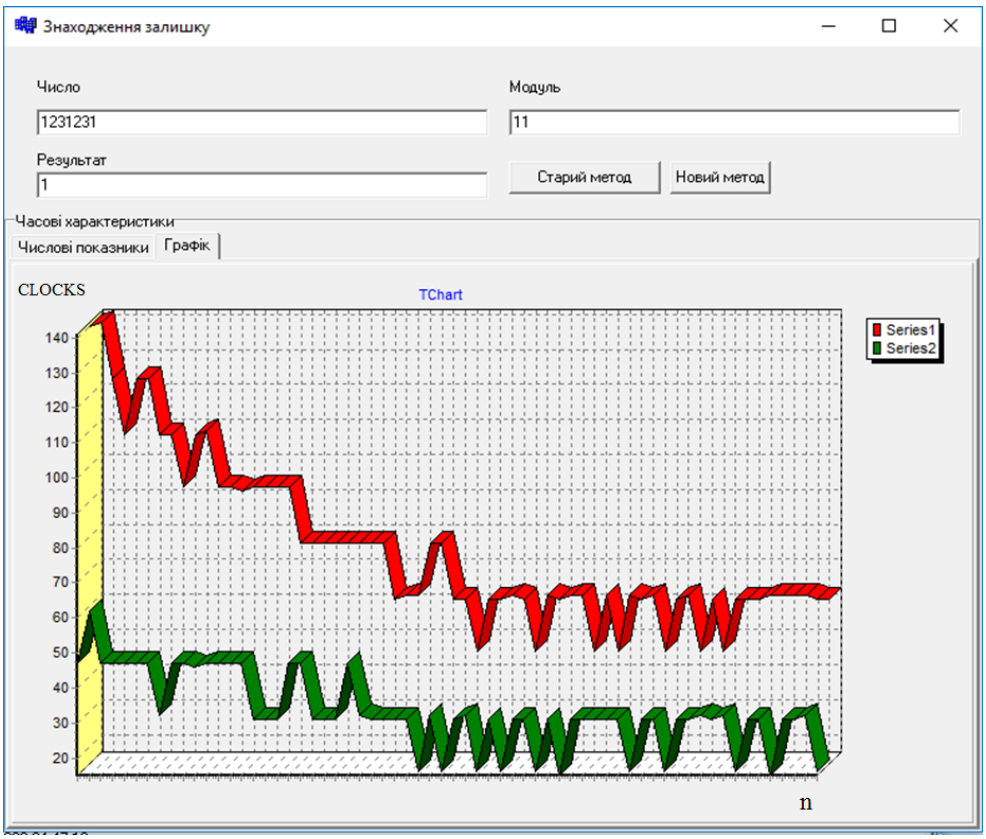


Рис. 4. Відображення залежності часу пошуку залишку числа від номеру

Отже, існує доцільність його використання при опрацюванні довгих чисел в асиметричних криптографічних системах захисту інформації для підвищення швидкодії процесів шифрування та криптоаналізу.

Список літератури

1. Розум, І.Ю. Застосування прикладної криптографії в системі військового управління в інтересах засекречування мереж зв'язку військового призначення // І.Ю. Розум // Збірник наукових праць НАДПСУ. Сер. : Військові та технічні науки. – 2013. – № 2. – С. 170-179.
2. Горбенко, А.Ю. Аналіз досвіду створення та бойового застосування систем оперативного управління / А.Ю. Горбенко, О.В. Головченко, М.Ю. Голобородько // Збірник наукових праць центру воєнно-стратегічних досліджень НУОУ імені Івана Черняховського. – 2017. – № 2. – С. 98-102.
3. Корченко, О.Г. Прикладна криптологія : системи шифрування : підручник / О.Г. Корченко, В.П. Сіденко, Ю.О. Дрейс. – К.: ДУТ, 2014. – 448 с.
4. Задірака В.К. Комп'ютерна криптологія: Підручник / В.К. Задірака, О.С. Олексюк. – Київ, 2002. – 504 с.
5. Kasyanchuk, M. Fundamental Backgrounds of the Discrete Logarithms Theory in the Rademacher-Krestensons Basis / M. Kasyanchuk, S. Ivasiev, I. Pazdriy, R. Trembach, I. Yakymenko // Proceedings of the XI-th International conference "Modern Problems of Radio Engineering, Telecommunications and Computer Science" (TCSET-2012). – Lviv-Slavsk. – 93 p.
6. Kozaczko, D. Vector Module Exponential in the Remaining Classes System / D. Kozaczko, I. Yakymenko, M. Kasianchuk, S. Ivasiev // Proceedings of the 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS–2015). – Warsaw, Poland. – Vol. 1. – 2015. – Pp.161-163.
7. Тимошенко, Л.М. Удосконалення алгоритму факторизації для криптографічних систем захисту інформації / Л.М. Тимошенко, К.В. Вербик, С.В. Івасьєв // Сучасна спеціальна техніка. – 2014. – № 3(38). – С. 56-59.
8. Iakymenko, I. Construction of distributed thermal or piezoelectric sensor based on residue systems / I. Iakymenko, M. Kasianchuk, Ia. Kinakh, M. Karpinski // Przeglad Elektrotechniczny. – 2017. – No. 1. – Pp. 290-294.

9. Omondi, A. Residue number systems: theory and implementation / A. Omondi , B. Premkumar. – London: Imperial College Press, 2007. – 296 p.
10. Kasianchuk, M. Algorithms of findings of perfect shape modules of remaining classes system / M. Kasianchuk, I. Yakymenko, I. Pazdriy, O. Zastavnyy // Proceedings of the XIII-th International Conference "The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM-2015) ". – 2015. – Pp. 168-171.
11. Задірака, В.К. Комп'ютерна арифметика багаторозрядних чисел: Наукове видання / В.К. Задірака, О.С. Олексюк. – Київ, 2003. – 264 с.
12. Шумейко, О.О. Інформаційна безпека: Навч. посібник / О.О. Шумейко. – Дніпропетровськ: ДДТУ, 2012. – 144 с.
13. Патент на корисну модель № 68872. МПК G 06 F7/00. Пристрій визначення залишку багаторозрядного числа / Николайчук, Я.М., Якименко І.З., Воронич А.Р., Волинський О.І.; заявл. 10.04.2012.
14. Патент на корисну модель № 74576. Спосіб визначення залишку двійкового числа / Николайчук, Я.М., Волинський О.І.; заявл. 12.11.2012.

АЛГОРИТМЫ ПОИСКА ОСТАТКА ДЛИННЫХ ЧИСЕЛ ДЛЯ ЗАДАЧ АСИММЕТРИЧНОЙ КРИПТОГРАФИИ

Л.М. Тимошенко[1], С.В. Ивасьев[2], О.Я. Лотоцкий[3], В.М. Гаврилей[1]

[1]Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: lmt0902@gmail.com
[2]Тернопольський национальный экономический университет,
ул. Львовская, 11, Тернополь, 46020, Украина; e-mail: stepan.ivasiev@gmail.com
[3]Национальний авиационный университет,
просп.Космонавта Комарова, 1, Киев, 03058, Украина, e-mail: zyzik2323@gmail.com

На современном этапе обеспечения информационной безопасности государства важно засекречивание сетей связи военного назначения, одним их ключевых направлений которого является применение криптографических методов защиты информации, в частности, асимметричной криптографии. Одним из путей совершенствования алгоритмов асимметричной криптографии является нахождение остатков длинных чисел. Известные алгоритмы поиска остатков длинных чисел имеют ряд существенных недостатков при их реализации. В работе проводится анализ заявленных двух новых методов поиска остатков длинных чисел, их недостатков и вычислительных сложностей. Описан предложенный авторами метод, приведены его алгоритм и блок-схема. Исследуются вычислительные сложности трех рассмотренных методов поиска остатков, численный эксперимент оценки сложностей показывает, что при выполнении модульных операций, которые используются в асимметричных криптоалгоритмах, при переводе чисел из десятичной системы в систему счисления остаточных классов следует использовать предложенный метод, который характеризуется меньшей сложностью. Для дальнейшего рассмотрения остаются два. Выигрыш в эффективности предложенного алгоритма относительно известного определяется как соотношение вычислительных сложностей и равен 2. Разработанное на языке программирования высокого уровня C++ приложение позволяет исследовать временные характеристики выполнения двух методов. В работе приведен фрагмент тестирования приложения для двойных чисел Мерсенна и графическое изображение зависимости времени нахождения остатков больших чисел от простого числа, для которого находится остаток. Разработанный алгоритм поиска остатков больших чисел позволил повысить быстродействие по сравнению с известным за счет использования свойств остатков и числового базиса Радемахера. Это уменьшило вычислительную сложность и повысило выигрыш в эффективности работы алгоритма по сравнению с известным в два раза, что доказывает целесообразность его использования при обработке длинных чисел в асимметричных криптографических системах защиты информации для повышения быстродействия процессов шифрования и криптоанализа.

Ключевые слова: ассиметричная криптография, длинная арифметика, система остаточных классов, вычислительная сложность, остатки длинных чисел.

ALGORITHMS FOR SEARCHING LONG-TERM NUMBERS FOR THE TASK ASYMETRIC CRYPTOGRAPHY

L.M. Tymoshenko[1], S.V. Ivasiev[2], O.Y. Lototskyy[3], V.M. Gavriley[1]

[2] Odessa National Polytechnic University,
1 Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: lmt0902@gmail.com
[1] Ternopil National Economic University,
11 Lvivska str., Ternopil, 46020, Ukraine; e-mail: e-mail: stepan.ivasiev@gmail.com
[3] National Aviation University,
1 Kosmonavtom Komarova Ave., Kiev, 03058 e-mail: zyzik2323@gmail.com

At the present stage of providing information security of the state, it is important to make secret military communication networks. One of the key areas to secret a network is the use of cryptographic methods for information protection, in particular, asymmetric cryptography. To improve asymmetric cryptography algorithms we can find the remains of long numbers. The implementation of known algorithms for finding the remains of long numbers has a number of significant drawbacks. The paper analyzes two new methods of finding long-numbered residues, their drawbacks, and computational complexities. The method proposed by the authors is described, its algorithm and block diagram are presented. The computational complexities of the three researched methods are studied. The numerical complexity evaluation experiment shows that when performing modular operations used in asymmetric cryptographic algorithms, when transferring numbers from the decimal system to the system of the numbers of residual classes, the proposed method should be used. The method has less complexity. There are two ways of further consideration. It is well-known that the algorithm effectiveness gain is equal to the ratio of computational complexity and equal 2. The application developed in the high-level programming language C ++ allows us to investigate the time characteristics of the two methods. In this paper, we give a fragment of the testing of the application for double Mersenne numbers and a graphic representation of the dependence of the time of finding the remnants of large numbers from the prime number for which the remainder is. The developed algorithm for finding the remnants of large numbers allowed to increase the speed compared to the known due to the use of the properties of residues and the numerical basis of Rademacher. This reduced the computational complexity and increased the efficiency of the algorithm compared with the known twice, which proves the expediency of its use in processing long numbers in asymmetric cryptographic information security systems to increase the speed of encryption and cryptanalysis.

Key words: asymmetric cryptography, long arithmetic, system of residual classes, computational complexity, remains of long numbers.

УДК 004.65

Informatics and Mathematical Methods in Simulation
Vol. 8 (2018), No. 4, pp. 334-344

МОБИЛЬНОЕ ПРИЛОЖЕНИЕ ДЛЯ МОНИТОРИНГА, ДИАГНОСТИКИ И ПРОГНОЗИРОВАНИЯ РИСКА ОТКАЗОВ КОМПОНЕНТОВ СЛОЖНОЙ ТЕХНИЧЕСКОЙ СИСТЕМЫ

В.В. Вычужанин, Н.Д. Рудниченко, А.В. Вычужанин

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: 126.ist.onpu@gmail.com

Проведенный анализ технических решений, позволяющих повысить надежность функционирования сложных технических систем, показал, что своевременная и качественная диагностика, в том числе дистанционная, компонентов сложных технических систем при их эксплуатации позволяет повысить надежность систем и эффективность их эксплуатации. Одним из важнейших показателей надежности является оценка риска отказов компонентов сложных технических систем. Программная и аппаратная беспроводная передача данных в информационных системах со смартфонами позволяет осуществлять дистанционное управление и контроль расходов ресурсов, синхронизацию работы компонентов сложных технических систем, координацию распределенных вычислительных процессов. В статье рассматриваются аспекты разработки мобильных приложений для дистанционного мониторинга, диагностики и прогнозирования риска отказов компонентов сложной технической системы. Описаны характеристики дизайна пользовательского интерфейса и порядок взаимодействия с разработанным приложением для дистанционного мониторинга, диагностики и прогнозирования риска отказов компонентов сложной технической системы. Для реализации приложения разработана логическая модель базы данных, основанная на выборе системы управления базой данных. В статье приведены результаты использования диаграммы классов, а также проект мобильного приложения с обобщенным алгоритмом. Приведена модульная структура реализации программного обеспечения мобильного приложения для мониторинга, диагностики и прогнозирования риска отказов компонентов сложной технической системы. Разработанный проект мобильного приложения для мониторинга, диагностики и прогнозирования риска отказов компонентов сложной технической системы является полным и логическим завершением. В процессе написания кода программного обеспечения рекомендуется использовать настройки Gradle, что позволит ускорить процесс рефакторинга, профилирования и интеграции с системой контроля версий GIT. Разработанное мобильное приложение позволяет упростить процесс оценок риска компонентов сложных технических систем. Дополнительный контент и функциональные дополнения проекта могут быть возможны благодаря интерфейсам Android-Core. В качестве альтернативы серверной стороне рекомендуется использовать современные облачные сервисы и технологии, основанные на моделях IaaS и PaaS.

Ключевые слова: мобильное приложение, мониторинг, диагностика, прогнозирование, андроид, технические системы, пользовательский интерфейс, Java, прототипирование.

Введение

Проведение своевременной диагностики, в том числе дистанционной сложных технических систем (СТС) позволяет повысить надежность систем, а значит и эффективность их эксплуатации. Одним из показателей надежности СТС является оценка риска отказов компонентов систем [1-5]. Переход к обеспечению эксплуатационной надежности технологического оборудования по его «фактическому состоянию» вызывает необходимость предпринимать меры по предупреждению и

обнаружению причин возникновения отказов СТС, создания систем мониторинга, диагностики и прогнозирования их состояния [6-10]. Решение проблемы возможно использованием информационных систем дистанционного мониторинга, диагностики и прогнозирования состояния компонентов СТС.

Развивающиеся мобильные операционные системы и технологии находят все более широкое применение на базе мобильных гаджетов для решения различных задач [11-13]. Программная и аппаратная беспроводная передача данных в информационных системах со смартфонами позволяет осуществлять дистанционное управление и контроль расходов ресурсов, синхронизацию работы компонентов сложных технических систем, координацию распределенных вычислительных процессов [14,15]. Следует также отметить актуальность использования открытой операционной системы Android в качестве платформы для разработки мобильных приложений, которая распространяется на лицензиях GPU и Appache [16]. Система обладает преимуществами: поддержка интеграции сторонних сервисов и компонентов; наличие механизмов реализации для виртуализации; гибкость реализации приложений в Java-шаблонах MVC и шаблонах проектирования; поддержка защиты протокола SSL-протокола от передаваемой информации; возможность оптимизации передачи мобильного трафика данных [17]. Поддерживаемая функциональность платформы Android позволяет разрабатывать мобильные приложения для удаленного мониторинга и прогнозирования риска отказов технических компонентов системы [18,19].

Цель работы

Целью работы является разработка проекта мобильного приложения для дистанционного мониторинга, диагностики и прогнозирования риска отказов компонентов СТС, включающего: обоснование специфики предложения пользовательского интерфейса и опыта взаимодействия с приложениями мобильного удаленного мониторинга; разработку логической модели базы данных для мобильных приложений; проектирование UML-диаграмм для создания классов абстрактных моделей и объектов мобильных приложений; алгоритм мобильного приложения; модульную структуру; интерфейс прототипа на главном экране.

Основная часть

Разработка мобильного приложения.

А. Специфика пользовательского интерфейса и опыт взаимодействия мобильного приложения.

Разрабатываемое мобильное приложение предназначено для использования на мобильных устройствах с версией операционной системы Android 4.4.2 и выше, размер экрана 4,5 дюйма и разрешение 800*600 пикселей и более. Гибкость интерфейса пользователя достигается за счет: элементов цветоделения взаимодействия и визуализации действия динамики при их активации; возможности изменения размера и шрифта текстовых блоков и типов надписей с помощью Typekit; поддержки переключения между вкладками экрана с использованием метода выбора типа обработки событий; преобладания плоских элементов дизайна над skeuomorph; ясности и динамической анимации при рендеринге статистики в графической форме; частичного размытия фоновой активности с появлением диалоговых окон или информационных сообщений; размещения всех функциональных элементов в одном экране, исключая необходимость прокрутки вверх/вниз; интегрированной интеллектуальной клавиатуры для ввода текстовых данных.

В. Разработка модели логической базы данных.

Выбор системы управления базами данных (СУБД) для разработки и внедрения базы данных эффективно взаимодействующей с мобильным клиентским приложением усложняется из-за обилия на рынке доступных решений. СУБД SQLite - встроенная поддержка файлового сервера ОС Android является преимуществом в случае полностью автономного режима. Операции мобильного приложения связаны с необходимостью постоянного подключения к удаленному внешнему серверу. Использование СУБД приемлемо из-за интеграции стандартных инструментов и поддержки ее библиотеки, что позволяет увеличить скорость и эффективность работы мобильного приложения. В долгосрочной перспективе при разработке проекта на основе новых списков требований для соответствующей масштабируемости может быть выбрана NoSQL СУБД MongoDB.

Для решения поставленной задачи разработаны таблицы базы данных: элементы, межэлементные коммуникационные подсистемы, системы, датчики, параметры, вероятность отказов компонентов СТС, ущерб, параметры прогноза, список журналов. Типы данных, используемых в базе данных - в основном целые действительные числа, прописные и регистрационные данные в таблице. На основе разработанной ER-модели может быть реализована конкретная физическая модель базы данных в MySQL Workbench или SQL Navigator.

C. Разработка UML-диаграмм мобильного приложения

Проектирование сценариев использования приложения может быть обеспечено диаграммой вариантов использования мобильных приложений (рис. 1).

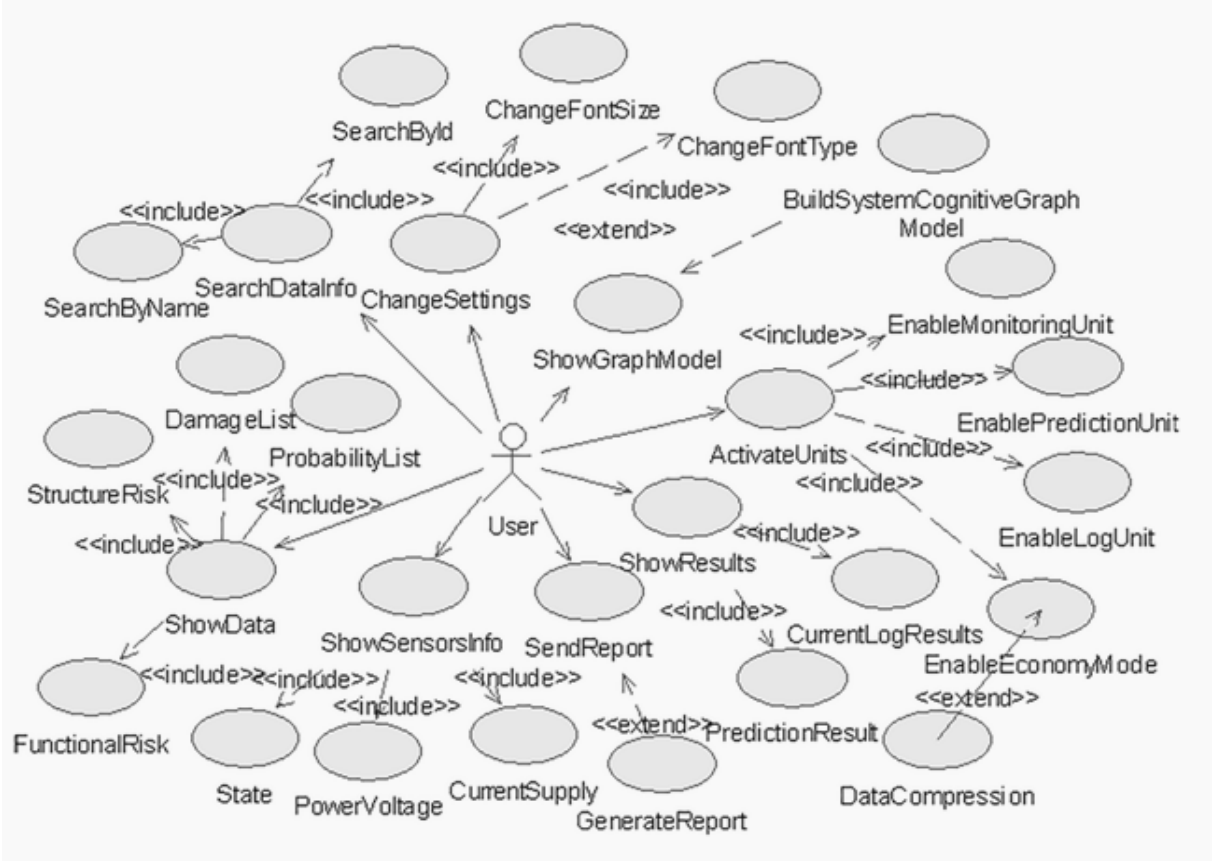


Рис. 1. Диаграмма вариантов использования мобильных приложений

Были выбраны функции приложений: просмотр информации о повреждениях компонентов СТС; оценка вероятности сбоя, структурных и функциональных рисков; поиск информации в базе данных по имени или уникальному номеру объекта; локальное хранилище и отправка сгенерированного отчета в формате pdf; построение когнитивной имитационной модели (КИМ) [6]; изменение настроек пользовательского интерфейса; просмотр результатов прогноза состояния компонентов СТС; включение и

отключение модулей мониторинга, диагностики и прогнозирования состояния компонентов СТС; ведение журнала и переход в экономичный режим, уменьшающий энергопотребление батареи мобильного устройства, а также обеспечивающий дополнительное сжатие данных, отправленных на сервер.

Для формализации класса и объектных моделей мобильного приложения разработана диаграмма классов проекта, а также указаны отношения между классами и их экземплярами (рис. 2).

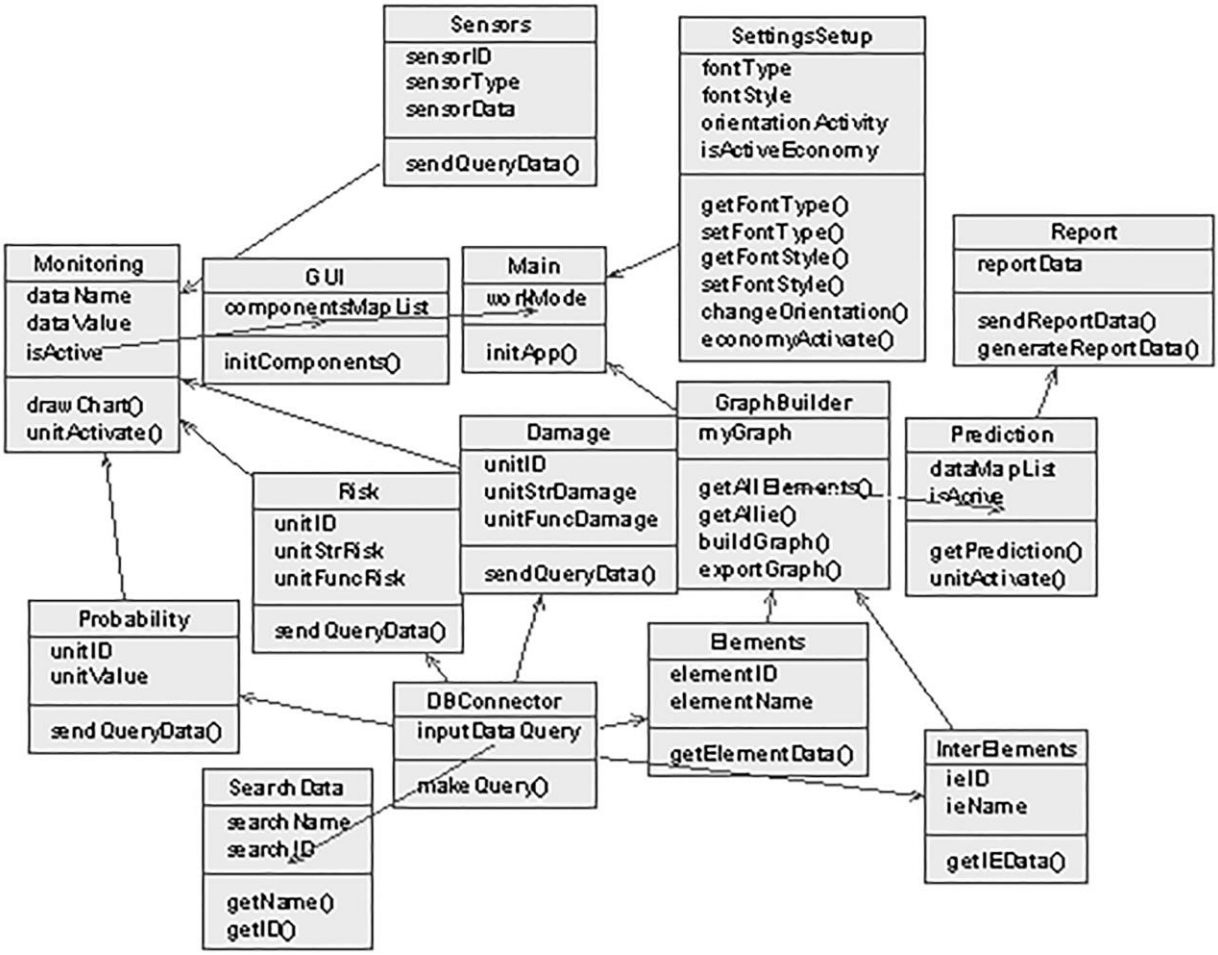


Рис. 2. Фрагмент диаграммы класса мобильного приложения

Запуск приложения выполняется в отдельном потоке с помощью метода initApp Main class. Процедура авторизации выполняется в классе приложений Autoriz и создает графическую активность пользователя с полями входа и пароля. Каждый класс реализует: мониторинг, диагностику, прогнозирование; построение графика КИМ; поиск и просмотр информации с датчиков контролируемых параметров СТС; определение вероятности отказов компонентов СТС, риска и ущерба. Для более подробного описания мобильного приложения была разработана диаграмма его деятельности (рис. 3). Объекты на диаграмме: клиент-мобильное приложение; внешний сервер, синхронизирующий, обрабатывающий и проверяющий статистические данные о работе компонентов СТС; сервер управления - выполняет задачи хранения, обработки, резервирования и обмена данными с внешним сервером и системой сбора данных; система сбора данных - выполняет функции сбора данных непосредственно с датчиков и передает информацию на сервер управления СТС. Для проверки активности сервера и возможности установления соединения между сервером и клиентом используется мобильное приложение. Оно отправляет пакет запросов для проверки основных активных обновлений в репозиториях, результатов проверки

данных авторизации, а также получает техническую и статистическую информацию о работе СТС.

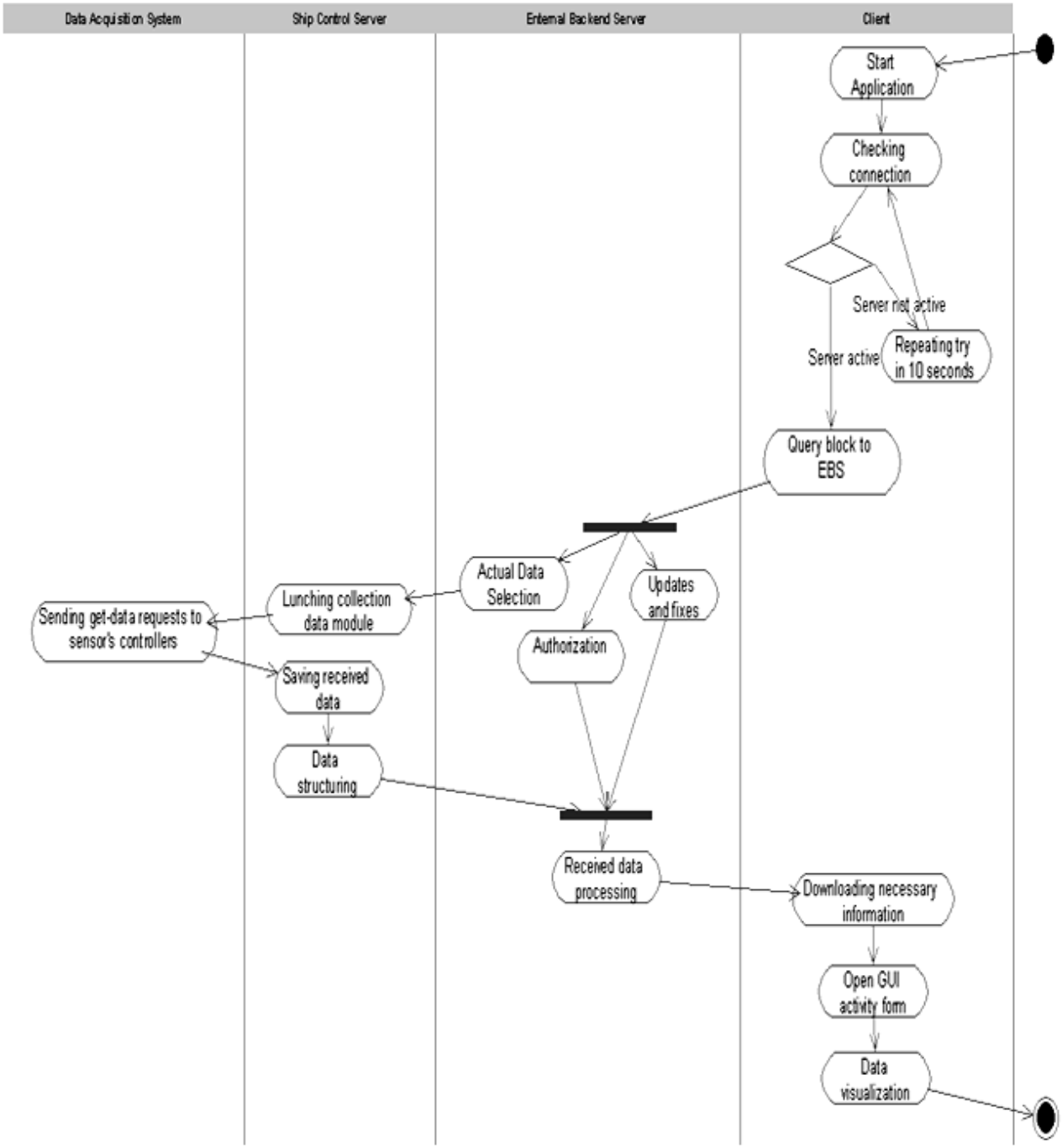


Рис. 3. Диаграмма активности мобильного приложения

D. Алгоритм мобильного приложения.

Для реализации интерфейса прототипа и написания программной кодовой реализации, формализованной через UML-функциональность разработан алгоритм работы мобильного приложения (рис. 4). Пакет установки приложения загружается на мобильное устройство в формате * .apk. В результате выполняется инициализация всех компонентов и зависимостей программных приложений, включая проверки подключения к точкам беспроводного доступа в Интернет с помощью поддерживаемых технологий (с использованием пакета android.net) и действия удаленного сервера.

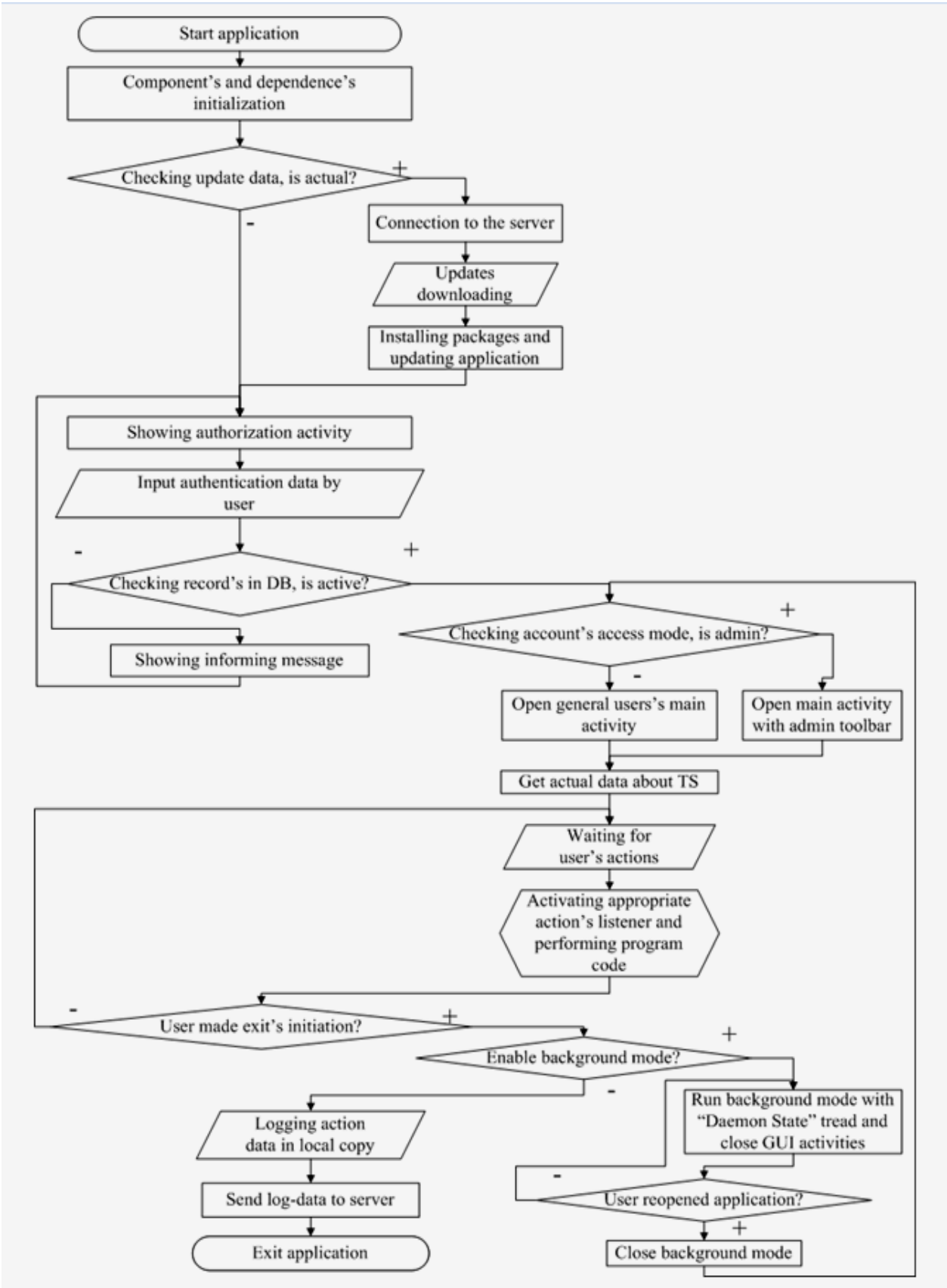


Рис. 4. Алгоритм мобильного приложения

Затем осуществляется процесс визуализации компонента отражения обновления данных на сервер. В случае реализации такой процедуры новый процесс начинает установку необходимых пакетов и обновление приложений в фоновом режиме. Пользователь применяет интерфейс входа в систему, введя имя пользователя и пароль.

Осуществляется получение технической и статистической информации о компонентах системы. После этого приложение переходит в основную форму, в режим ожидания и режим пользовательских запросов, в соответствии с которым осуществляется выполнение программного кода, содержащегося в соответствующем обработчике событий. При закрытии приложения появляется визуализация дополнительного диалогового окна, в котором предлагается переносить работу мобильных приложений в фоновом режиме. Если пользователь выбирает запуск приложения в фоновом режиме в отдельном процессе и потоке, тогда действие GUI выгружается из оперативной памяти мобильного устройства. Если снова запускается приложение, которое в этой точке уже находится в фоновом режиме, тогда режим закрывается, и управление передается для проверки доступа к режиму приложения. В случае если пользователь инициирует окончательное закрытие приложения в фоновом режиме, происходит ведение журнала всех действий, выполняемых в локальной копии рабочего каталога мобильного приложения. При появлении соединения с сервером, то выполняется отправка данных на сервер. После этого происходит полная разрядка приложения из основной памяти используемого мобильного устройства. Объем данных мобильных приложений, хранящихся в соответствующем каталоге «Cache», не должен превышать 2,5 мегабайта. В противном случае произойдет процедура кэширования.

Е. Модульная структура приложения.

Разработанное мобильное приложение состоит из модулей:

- инициализации компонентов пользовательского интерфейса;
- проверки текущего модуля данных программы для версии приложения;
- подключения к удаленному серверному модулю;
- построения и визуализации системного модуля КИМ [20];
- отчетности, для преобразования, экспорта статистики и графических данных из приложений;
- прогноза для создания и обучения искусственной нейронной сети на основе метода обратного распространения, линейной функции нормализации с помощью касательной функции активации. Создается нейронная сеть, обучаемая с оценкой результатов, в виде значений ошибок [6];
- визуализации статистических данных;
- получения данных для реализации запросов выборки данных, хранящихся в базе данных на стороне сервера.

Модули представляют собой базовую структуру проекта разработки мобильных приложений. Они хранятся в отдельных пакетах, поэтому в будущем проект может быть дополнен. Прототип реализации программного обеспечения Интерфейс клиента имеет форму (рис. 5).

Прототип разработан с использованием облачной службы SaaS fluidui.com, состоящей из 3 вкладок: Analytics (содержит компоненты, просматривающие список активных датчиков, получения информации и управления ими модулями мониторинга, диагностики и прогнозирования, ведения журналов), мониторинг (включает графические компоненты динамической визуализации параметров и системы характеристик), Prediction (содержит таблицу прогнозируемых значений риска в зависимости от выбранного периода времени).

При реализации прототипа мобильного клиента проведено профилирование его функционирования с целью исследования специфики загрузки имплементированных компонентов, обработки и отправки данных через установленное с сервером соединение, а также осуществления оценки общей производительности приложения.

Исследование осуществлялось под тремя различными версиями Android в двух режимах: стандартном и экономном (сжатие передаваемых данных и сокращение вычислительных операций), оценивался объем занимаемой оперативной памяти, ресурс

процессора и объем передаваемых данных за одну итерацию обращения к серверу, результаты приведены в таблице 1.

Рис. 5. Прототип интерфейса мобильного клиента

Таблица 1.

Результаты профилирования мобильного приложения

	Стандартный режим			Экономный режим		
	RAM, mb	CPU, %	Data, mb	RAM, mb	CPU, %	Data, mb
Android 5.x	65	25-30	4,5	59	25-30	4,0
Android 6.x	59	20-30	6,7	55	22-27	6,0
Android 7.x	77	15-20	7,1	58	15-18	6,8

Следует отметить, что использование оперативной памяти в стандартном режиме эксплуатации приложения является максимальным в операционной системе Android 7.x, что связано с необходимостью загрузки дополнительных компонентов для обеспечения работы ядра системы. При этом, процессор мобильного устройства задействован для проведения вычислительных операций в среднем на 5-10% меньше, чем в случаях использования предыдущих версий Android, что свидетельствует о лучшей согласованности в использовании API Android 7.x. Объемы передаваемых данных в различных режимах использования изменяются не существенно, что является основанием для дальнейшего совершенствования алгоритмов их сжатия. Экономичный

режим использования приложения под управлением Android 7.x в большей степени позволяет снизить объем используемой оперативной памяти, чем степень загрузки процессора, в более ранних версиях операционной системы эта зависимость менее заметна, отличия составляет 4-6% для Android 6.x и 5.x соответственно.

Проведенные исследования обуславливают целесообразность использования разработанного мобильного приложения под управлением операционной системы Android 7.x в связи с лучшей организацией процессов обмена данными и оптимизацией распределения ресурсов для проведения вычислений.

Выводы

Разработанный проект мобильных приложений для мониторинга, диагностики и прогнозирования риска отказов компонентов сложной технической системы является полным и логическим завершением. В процессе написания кода программного обеспечения целесообразно использование настройки Gradle, что позволит ускорить процесс рефакторинга, профилирования и интеграции с системой контроля версий GIT. Разработанное мобильное приложение позволяет упростить процесс оценки риска отказов компонентов сложных технических систем. Дополнительный контент и функциональные дополнения проекта могут быть возможны благодаря интерфейсам Android-Core. В качестве альтернативы серверной стороне рекомендуется использовать современные облачные сервисы и технологии, основанные на моделях IaaS и PaaS.

Список литературы

1. Andersen, B. A Diagnostic System for Remote Real-Time Monitoring of Marine Diesel-Electric Propulsion Systems / B. Andersen. – Leipzig, 2011. – 45 p.
2. O'Neill, J. Technical Risk Assessment: a Practitioner's Guide / J. O'Neill, N. Thakur, A. Duus. – Australia, 2007. – 29 p.
3. Kertzner, P. Process Control System Security Technical Risk Assessment Methodology & Technical Implementation / P. Kertzner, J. Watters, D. Bodeau // Research Report. – 2008. – No. 13. – 47 p.
4. Вычужанин, В.В. Математические модели нестационарных режимов воздухообработки в центральной СКВ / В.В. Вычужанин // Вісник Одеського національного морського університету, збірник наукових праць, 2014. – №23. – С. 172-186.
5. Вычужанин, В.В. Оценки структурного и функционального рисков сложных технических систем / В.В. Вычужанин, Н.Д. Рудниченко // Восточно-Европейский журнал передовых технологий. – 2014. – Том 1, № 2(67). – С. 18-22.
6. Vychuzhanin, V. Devising a method for the estimation and prediction of technical condition of ship complex systems / V. Vychuzhanin, N. Rudnichenko, V. Boyko, N. Shibaeva // Eastern-European Journal of Enterprise Technologies. – 2016. – No. 6/9. – Pp. 4-11.
7. Vychuzhanin, V. Assessment of risks structurally and functionally complex technical systems / V.V. Vychuzhanin, N.D. Rudnichenko // Eastern-European Journal of Enterprise Technologies. – 2014. – No. 2. – Pp. 18-22.
8. Вычужанин, В.В. Технические риски сложных комплексов функционально взаимосвязанных структурных компонентов судовых энергетических установок / В.В. Вычужанин, Н.Д. Рудниченко // Вісник Одеського національного морського університету, збірник наукових праць. – 2014. – № 2(40). – С. 68-77.
9. Вычужанин, В.В. Информационное обеспечение мониторинга и диагностирования технического состояния судовых энергоустановок / В.В. Вычужанин // Вісник одеського національного морського університету, збірник наукових праць. – 2012. – № 35. – С. 111-124.
10. Вычужанин, В.В. Метод управления рисками судовых сложных технических систем / В.В. Вычужанин, Н.Д. Рудниченко // Проблеми техніки. – 2014. – №2. – С. 138-142.
11. Аксенов, К.В. Обзор современных средств для разработки мобильных приложений / К.В. Аксенов // Новые информационные технологии в автоматизированных системах. – 2014. – № 17. – С. 508-513.

12. Голощапов, А.Л. Google Android: программирование для мобильных устройств / А.Л. Голощапов. – СПб.: БХВ-Петербург, 2011. – 448 с.
13. Майорова, Е.С. Современное состояние средств разработки мобильных приложений на платформах iOS, Android и Windows Phone / Е.С. Майорова, В.А. Ошурков, Л.Е. Цуприк // Перспективы науки и образования, 2015. – № 4(16). – С. 83-87.
14. Терехов, А.Н. Технология разработки мобильных онлайн сервисов / А.Н. Терехов, В.В. Оносовский // Конференция CEE-SECR, 2011. – С. 1-2.
15. Соколова, В.В. Разработка мобильных приложений / В.В. Соколова. – Томск: Изд-во Томского политехнического университета, 2011. – 175 с.
16. Ableson, W. Android in action / W. Ableson, R. Sen, C. King. – Manning Publications, 2011. – 592 p.
17. Burnette, E. Hello, Android: introducing Google's mobile development platform / E. Burnette. – Pragmatic Bookshelf, 2010. – 300 p.
18. Fling, B. Mobile design and development: practical concepts and techniques for creating mobile sites and web apps / B. Fling. – O'Reilly Media, 2009. – 336 p.
19. To, N. The Android developer's cookbook: building applications with the Android SDK (Developer's Library) / N. To, J. Steele. – Addison-Wesley Professional, 2010. – 400 p.
20. Вычужанин, В.В. Информационная когнитивная модель технологической взаимозависимости сложных технических систем / В.В. Вычужанин, Н.Д. Рудниченко // Информатика и математические методы в моделировании. – 2013. – № 3. – С. 240-247.

МОБІЛЬНИЙ ДОДАТОК ДЛЯ МОНІТОРИНГУ, ДІАГНОСТИКИ ТА ПРОГНОЗУВАННЯ РИЗИКУ ВІДМОВ КОМПОНЕНТІВ СКЛАДНОЇ ТЕХНІЧНОЇ СИСТЕМИ

В.В. Вичужанін, Н.Д. Рудніченко, О.В. Вичужанін

Одеський національний політехнічний університет,
проспект Шевченка, 1, Одеса, 65044, Україна; e-mail: 126.ist.onpu@gmail.com

Проведений аналіз технічних рішень, що дозволяють підвищити надійність функціонування складних технічних систем показав, що своєчасна і якісна діагностика, в тому числі дистанційна компонентів складних технічних систем при їх експлуатації дозволяє підвищити надійність систем і ефективність їх експлуатації. Одним із найважливіших показників надійності є оцінка ризиків компонентів складних технічних систем. Програмна та апаратна бездротова передача даних в інформаційних системах зі смартфонами дозволяє здійснювати дистанційне керування і контроль витрат ресурсів, синхронізацію роботи компонентів складних технічних систем, координацію розподілених обчислювальних процесів. У статті розглядаються аспекти розробки мобільних додатків для дистанційного моніторингу, діагностики та прогнозування ризику відмов компонентів складної технічної системи. Описано характеристики дизайну користувальницького інтерфейсу і порядок взаємодії з розробленим додатком для дистанційного моніторингу, діагностики та прогнозування ризику відмов компонентів складної технічної системи. Для реалізації програми розроблена логічна модель бази даних, заснована на виборі системи управління базою даних. У статті наведені результати використання діаграми класів, а також проект мобільного додатка з узагальненим алгоритмом. Наведено модульна структура реалізації програмного забезпечення мобільного застосування для моніторингу, діагностики та прогнозування ризику відмов компонентів складної технічної системи. Розроблений проект мобільного застосування для моніторингу, діагностики та прогнозування ризику відмов компонентів складної технічної системи є повним і логічним завершенням. В процесі написання коду програмного забезпечення рекомендується використовувати налаштування Gradle, що дозволить прискорити процес рефакторинга, профілювання і інтеграції з системою контролю версій GIT. Розроблене мобільний додаток дозволяє спростити процес оцінок ризику компонентів складних технічних систем. Додатковий контент і функціональні доповнення проекту можуть бути можливими завдяки інтерфейсів Android-Core. В якості альтернативи серверній стороні рекомендується використовувати сучасні хмарні сервіси і технології, засновані на моделях IaaS і PaaS.

Ключові слова: мобільний додаток, моніторинг, діагностика, прогнозування, андроїд, технічні системи, призначений для користувача інтерфейс, Java, прототипування.

MOBILE APPENDIX FOR MONITORING, DIAGNOSTICS AND FORECASTING RISK OF FAILURE OF COMPONENTS OF COMPLEX TECHNICAL SYSTEM

V.V. Vychuzhanin, N.D. Rudnichenko, A.V. Vychuzhanin

Odessa National Polytechnic University,
Shevchenko Avenue, 1, Odessa, 65044, Ukraine
e-mail: 126.ist.onpu@gmail.com

The analysis of technical solutions allowing to improve the reliability of functioning of complex technical systems has shown that timely and high-quality diagnostics, including remote components of complex technical systems during their operation, can improve the reliability of systems and the efficiency of their operation. One of their most important indicators of reliability is the risk assessment of components of complex technical systems. Software and hardware wireless data transmission in information systems with smartphones allows remote control and monitoring of resource costs, synchronization of components of complex technical systems, coordination of distributed computing processes. The article deals with the development of mobile applications for remote monitoring, diagnostics and forecasting the risk of failures of components of a complex technical system. Describes the characteristics of the design of the user interface and the order of interaction with the developed application for remote monitoring, diagnosis and prediction of the risk of failures of components of a complex technical system. To implement the application, a logical model of the database was developed, based on the choice of a database management system. The article shows the results of using a class diagram, as well as a draft mobile application with a generalized algorithm. The modular structure of software implementation for a mobile application for monitoring, diagnosing and forecasting the risk of failures of components of a complex technical system is given. The developed project of a mobile application for monitoring, diagnosing and forecasting the risk of failures of components of a complex technical system is a complete and logical conclusion. In the process of writing software code, it is recommended to use the Gradle settings, which will speed up the process of refactoring, profiling and integration with the GIT version control system. The developed mobile application allows to simplify the process of risk assessments of components of complex technical systems. Additional content and functional additions to the project may be possible thanks to the Android-Core interfaces. As an alternative to the server side, it is recommended to use modern cloud services and technologies based on the IaaS and PaaS models.

Keywords: mobile application, monitoring, diagnostics, forecasting, android, technical systems, user interface, Java, prototyping.

УДК 004.056: 159.95

Informatics and Mathematical Methods in Simulation
Vol. 8 (2018), No. 4, pp. 345-353

МОДЕЛЬ РОЗРАХУНКУ РІВНЯ НАПРУГИ У СУСПІЛЬСТВІ ДЛЯ ПРИЙНЯТТЯ ЕФЕКТИВНИХ РІШЕНЬ ІЗ ЗАХИСТУ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

А.А. Шиян, А.В. Поплавський, Л.О. Нікіфорова, І.В. Заступ

Вінницький національний технічний університет,
95, Хмельницьке шосе, Вінниця, 21021, e-mail: anatoliy.a.shiyan@gmail.com

Метою гібридної війни є дестабілізація соціально-економічного стану в країні-мішені, що призводить до зменшення рівня національної безпеки. Наявність об'єктивних параметрів, які характеризують стан суспільства, дозволяє здійснити оптимізацію діяльності структур управління національною безпекою країни. Метою статті є розробка моделі та підходів до вимірювання рівня стану напруги у суспільстві для прийняття ефективних рішень в захисті національної безпеки. Побудовано модель розрахунку розподілу суб'єктів національної безпеки (домогосподарств, фірм, соціальних груп тощо) за отриманими протягом року коштами, яка, на відміну від існуючих, враховує стохастичну природу суб'єктів. Отримано аналітичні вирази для щільності ймовірності розподілу коштів для суб'єктів національної безпеки. Розроблено підходи щодо вимірювання параметрів модельного розподілу з використанням експериментальних даних. На основі побудованої моделі розроблено систему показників та критеріїв для використання в задачах інформаційної та національної безпеки. Описано використання цих показників та критеріїв в процесі прийняття ефективних рішень із захисту національної безпеки. Наприклад, запропоновані показники та критерії можуть бути застосованої для визначення перед-революціного стану, а також для вимірювання зростання/зменшення соціальної напруги у суспільстві. Коли такі показники перевищують певне значення (віднайдене з аналізу історичних прецедентів), то в суспільстві є можливим соціальний вибух («майдани», «кольорові революції» тощо).

Ключові слова: національна безпека, суб'єкт, модель, захист, прийняття рішень.

Постановка проблеми

Метою гібридної війни є вирішення задач країни-агресора в країні-мішені. Наприклад, це може бути така дестабілізація соціально-економічного стану, що в результаті призведе до зменшення рівня національної безпеки. Сьогодні моделі як здійснення впливу, так і його захисту, лише розробляються. Внаслідок цього в ряді випадків структури держави-мішені здійснюють реакцію на ті сторонні впливи, які практично не впливають на зміну соціально-економічно стану (і, відповідно, на рівень національної безпеки). Більш того: іноді гібридна атака з боку агресора полягає саме в тому, щоб досягти неадекватної реакції з боку структур держави-мішені. І вже така неадекватна реакція державних структур в країні-мішені і призводить до дестабілізації в ній соціально-економічного стану. І як кінцевий результат — погіршення стану національної безпеки в державі-мішені. Наявність об'єктивних параметрів, що характеризують стан суспільства, дозволяє здійснити оптимізацію діяльності структур держави, які здійснюють управління національною безпекою країни.

Аналіз останніх досліджень та публікацій

Гібридна війна складається переважно з впливів інформаційного характеру. Основи її описано, наприклад в монографії [1], яку слід, однак, розглядати швидше у

вигляді програми для подальших досліджень та розробок. В ній не наведено ані конкретних моделей, ані методів для здійснення задекларованої у ній діяльності.

Вітчизняна література (див., наприклад, [2-5]) теж, на жаль, практично не містить в собі викладу достатньо пророблених моделей, зокрема таких, на яких ґрунтуються методи захисту суспільства від негативного впливу в рамках управління національною безпекою.

Подальший розвиток досліджень у сфері гібридної війни привів до розуміння ролі аналітики на етапі ідентифікації негативного інформаційного впливу та розробки моделей та методів протидії таким впливам [6-8].

Цікавою особливістю є те, що для протидії тероризму, який в сучасних умовах теж є елементом гібридної війни, на сьогодні існує ряд моделей, в тому числі і кількісного спрямування [9,10].

Певний етап у розробці моделей та методів як для ідентифікації наявності негативного інформаційного впливу, так і для протидії йому на рівні окремої особи, соціальної групи, соціальної мережі та суспільства, підсумовано у [11].

Таким чином, розробка моделей та методів для вимірювання об’єктивних характеристик стану суспільства є актуальною науковою та важливою в практичному застосуванні задачею.

Мета роботи

Метою роботи є розробка моделі та підходів до побудови методу вимірювання рівня напруги у суспільстві для прийняття ефективних рішень в захисті національної безпеки переважно від внутрішніх чинників із використанням стаціонарного розподілу суб’єктів економічної діяльності за отриманими коштами.

Моделювання характеристик сукупності суб’єктів національної безпеки

В якості кількісної характеристики, яка адекватно описує стан суспільства, найчастіше використовується фінансовий вимір [12]. Відповідні бази даних, як правило, у кожній країні прагнуть робити об’єктивними, а за їх наповненням та аналізом слідкує велика кількість формальних та неформальних структур та інститутів.

В якості одиничного суб’єкту часто виступають окреме домогосподарство, окрема соціальна група або окрема фірма (підприємство, організація) тощо.

В [13] побудована модель для отримання розподілу суб’єктів за наявними у них коштами. Наприклад, для домогосподарства це буде річний дохід, для соціальної групи – вартість річних коштів, які спрямовано на діяльність цієї групи (або ж, для деяких задач, сумарний річний дохід членів групи), для фірми її вартість тощо.

Математичну модель в [13] побудовано за таких припущень.

Припущення 1. Процеси проточного приросту та витрат коштів m суб’єктом економічної діяльності залежать тільки від поточної величини коштів (тобто не залежать від часу). Вони є універсальними для заданого (розглядуваного) класу суб’єктів.

Внаслідок цього припущення можна записати таке диференційне рівняння для зміни кількості коштів для заданого суб’єкта:

$$\frac{dm}{dt} = R(m) - Q(m). \qquad (1)$$

Тут $R(m)$ – інтенсивність приросту коштів (наприклад, дохід за рік), а $Q(m)$ – інтенсивність витрат коштів (наприклад, витрати за рік).

Рівняння (1) повинно мати в детермінованому випадку (наприклад, при незмінності зовнішніх умов) єдиний стаціонарний розв'язок m_0, який повинен бути сталим. Це означає, що перший член в (1) при малих значеннях коштів m повинен бути більшим за другий член. Тобто, процеси приросту коштів тоді будуть йти інтенсивніше, аніж процеси їх витрат (тоді права частина (1) буде додатною). Але для великих коштів процес їх витрат повинен уже бути більшим, аніж їх приріст (і тоді права частина (1) стає від'ємною). Ця вимога є природною, бо кількість коштів окремого типового економічного суб'єкта не може прямувати до безкінечності.

Подальший розгляд проведемо за умови виконання такого припущення.

Припущення 2. Інтенсивності приросту та витрат коштів є зростаючими степеневими функціями:

$$R(m) = cm^a, Q(m) = dm^b. \tag{2}$$

При цьому в рамках цього припущення покладаємо, що $a > 0, b > 0, c > 0, d > 0$ та виконується нерівність $b > a$.

Таке припущення часто використовується в рамках моделювання [12-14].

При виконанні цих припущень стаціонарне значення величини коштів суб'єкта буде таким: $m_0 = (c/d)^{1/(b-a)}$. Відмітимо, що, з урахуванням граничної економічної ефективності суб'єкта [12], яка вимагає, щоб функція $R(m)$ була опуклою догори, отримуємо $a \le 1$.

В рамках моделі (1) всі суб'єкти повинні характеризуватися однаковими значеннями m_0. Однак суб'єкти, які розглядаються в статті, складаються із людей. Люди мають різну економічну продуктивність, приймають різні рішення, і внаслідок цього коефіцієнти c, d будуть випадковими величинами (будуть відрізнятися від суб'єкта до суб'єкта). Тоді рівняння (1), яке характеризує результати діяльності різних людей (груп людей), повинно розглядатися як стохастичне. Більш детальне обґрунтування наведено в [13].

Таким чином, приходимо до двох основних моделей для розрахунку кількості коштів заданого суб'єкта:

$$\frac{dm}{d\tau_a} = \lambda \cdot m^a - m^b + \xi_{\tau.} \cdot m^a, \tag{3}$$

$$\frac{dm}{d\tau_b} = m^a - \omega \cdot m^b + \eta_\tau \cdot m^b. \tag{4}$$

Тут для моделі (3): $\tau_a = td, \lambda + \xi_\tau = c/d, d = const$ та $m_0 = \lambda^{1/(b-a)}$, а для моделі (4) $\tau_b = tc, \omega + \eta_\tau = d/c, c = const$ та $m_0 = \omega^{1/(a-b)}$. Функції ξ_t і η_t є стохастичні.

В моделі (3) стохастичність зумовлено залежністю приросту коштів від людського фактору (від людей, які складають даний економічний суб'єкт), тобто має переважно внутрішній характер. Тому в (3) для приросту коштів $R(m)$ виділено як усереднену, детерміністичну складову λ, так і її стохастичний доданок ξ_τ.

В моделі (4) стохастичність зумовлено переважно зовнішніми факторами, які призводять до змінності витрат різних економічних суб'єктів (наприклад, різні умови здійснення виробництва у різних регіонах країни). Тому в (4) також виділено як

усереднену, детерміністичну складову ω, так і її стохастичний доданок η_τ у функції витрат $Q(m)$.

Моделі (3) та (4) є стохастичними диференціальними рівняннями із мультиплікативним шумом [14]. Для простоти розгляду можемо вважати, що функції ξ_t і η_t є білим шумом із середнім значенням $\langle \xi_1 \rangle = \langle \eta_t \rangle = 0$, а також із дисперсіями $\langle \xi_1^2 \rangle = \langle \eta_t^2 \rangle = \sigma^2$. За визначених вище умов математичні аспекти моделей (3) та (4) детально розглянуто в [14]. Припущення щодо використання білого шуму в процесі дослідження стохастичних диференціальних рівнянь часто використовується при моделюванні, оскільки воно дозволяє відобразити основні характеристики відповідних функцій розподілу, а також з достатньою точністю описувати експериментальні результати [14].

За стохастичними диференційними рівняннями (3) та (4) складаються рівняння Колмогорова-Фокера-Планка у відповідній для нашого випадку інтерпретації Стратоновича для щільності ймовірності $P(m,t)$. Якщо шум ξ_t (або η_t, відповідно) є білим, то внаслідок умови $b > a$ маємо $P(m,t) \to P_s(m)$, причому, у загальному випадку, вигляд $P_s(m)$ буде визначатися лише статистичними властивостями ξ_t (η_t) і величинами a, b, m_0. Для нашої задачі це означає, що в країні деякий час повинні бути витримані незмінними умови для діяльності економічних суб'єктів. Як правило, для цього достатньо 5-7 років (кількісні оцінки наведено в [13]).

Подальший розгляд проведемо за умови нехтування перехідними процесами, тобто для $P_s(m)$. В [13,14] показано, що щільність розподілу $P_s(m)$ характеризує всю сукупність однорідних суб'єктів, кожен із який демонструє стохастичну поведінку.

Розв'язання відповідних рівнянь Колмогорова-Фокера-Планка для $P_s(m)$ має такий вигляд для моделі (3):

$$P_s^a(m) = C_1 \cdot m^{-a} \exp\left\{ \frac{2\lambda m^{1-a}}{(1-a)\sigma^2} \left[1 - \frac{(1-a)m^{b-a}}{\lambda(b+1-2a)} \right] \right\}, \tag{5}$$

$$P_s^{a=1}(m) = C_2 \cdot \exp\left\{ -\left(1 - \frac{2\lambda}{\sigma^2} \right) \ln m - \frac{2m^{b-1}}{(b-1)\sigma^2} \right\}, a = 1, \tag{6}$$

і для моделі (4):

$$P_s^b(m) = C_3 \cdot m^{-b} \cdot \exp\left\{ \frac{2\omega m^{1-b}}{(b-1)\sigma^2} \left[1 - \frac{(b-1)m^{a-b}}{\omega(2b-a-1)} \right] \right\}, \tag{7}$$

$$P_s^{b=1}(m) = C_4 \cdot \exp\left\{ -\left(1 + \frac{2\omega}{\sigma^2} \right) \ln m - \frac{2}{(1-a)\sigma^2 m^{1-a}} \right\}, b = 1. \tag{8}$$

В (6) – (9) $C_i, i = 1,2,3,4$ – відповідні нормувальні константи.

Для розглянутих моделей асимптотика $P(m,t) \to P_s^{a,b}(m)$ справедлива незалежно від вигляду початкового розподілу $P(m, t=0)$.

Загальні властивості отриманих $P_s^{a,b}(m)$ є такими:

- при малих інтенсивностях шуму σ^2 буде мати місце асимптотика $P_s^{a,b}(m) \to \delta(m-m_0)$, де $\delta(x)$ – сингулярна дельта-функція Дірака;
- з ростом σ^2 ширина Δ розподілів $P_s^{a,b}(m)$ збільшується.

Моделі (3) і (4) у наближенні білого шуму будуть добре описувати головний внесок в експериментально виміряні значення щільності ймовірності для розподілів досліджуваних суб'єктів за кількістю коштів $P_e(m)$, який зосереджений в певному інтервалі навколо m_0.

Формули для щільності ймовірності $P_s^{a,b}(m)$, наведені в (5)-(8), можуть бути використані для того, щоб по знайденому із експерименту вигляду функції $P_e(m)$ знайти необхідні параметри $a, b, \lambda(\omega), \sigma$. При цьому показник зростання коштів a можна знайти із характеристик зростання суб'єктів (наприклад, старт-апів), тому що на початку їх діяльності $R(m) >> Q(m)$ (це є умовою зростання коштів для розглядуваного суб'єкту). Показник b можна знайти із даних про стан суб'єктів (наприклад, фірм) в процесі їх руйнування (наприклад, перед банкрутством), коли виконана нерівність $R(m) << Q(m)$. Значення параметрів λ, ω віднаходяться через максимальне значення щільності ймовірності $P_e(m)$ при відносно невеликих значеннях інтенсивності шуму σ^2 (відповідні формули наведено, наприклад, в [14]). Після цього σ залишається єдиним «підгоночним» параметром, який знаходиться з умови «найбільшого наближення» теоретичного розподілу $P_s^{a,b}(m)$ і $P_e(m)$. Відмітимо, що «хвости» функцій розподілу $P_e(m)$ будуть формуватися із порівняно малої кількості суб'єктів, тому в рамках моделі білого шуму в них не можна належним чином урахувати варіабельність характеристик суб'єктів (можна сказати, що в «хвостах» $P_e(m)$ проявляються «найбільш яскраві індивідуальності» серед суб'єктів).

Розглянутий клас моделей дозволяє формалізувати кількісний розрахунок таких параметрів суб'єктів, які є інтегральними та характеризують їх сукупність «в цілому». Це дає можливість розробити ряд нових критеріїв для загальних характеристик сукупностей суб'єктів, які проявляють стохастичну поведінку, що відкриває можливості для розробки нового класу їх характеристик.

Отримані моделі допускають поширення на нестаціонарні випадки, але дослідження може бути проведено, як правило, лише шляхом комп'ютерного моделювання. Наприклад, введення «повільних» змінних τ (з характерним часом мінливості багато більше ніж $T_0 = \left[(1-a)c\right]^{-1} \cdot m_0^{1-a}$) дозволяє використати отримані результати шляхом введення залежностей виду $a(\tau), b(\tau), c(\tau), d(\tau), \sigma^2(\tau)$ тощо.

Показники та критерії для використання в захисті національної безпеки

Кількісні характеристики як щільності ймовірності $P_s(m)$, так і отримані із її допомогою показники (наприклад, середні значення чи дисперсія) можуть бути використані для аналізу стану та прийняття ефективних рішень для захисту національної безпеки.

Наведемо декілька прикладів використання цих характеристик.

Природним критерієм правильності розвитку суспільства виступає вимога зростання m_0 (наприклад, зростання доходів домогосподарств).

Щільність ймовірності $P_s(m)$ для даної сукупності суб'єктів, таких як домогосподарства чи соціальні групи, повинна бути одномодальною (тобто мати один

максимум). Двомодальність чи багатомодальність свідчить про наявність декількох підсистем, які функціонують за різними соціально-економічними закономірностями. Це буде означати, що в сукупності існують дві чи більше підгруп, які мають інтереси, які не співпадають. Найчастіше ці інтереси є конфліктними: одна із груп має більш високі соціально-економічні показники, аніж інша/інші. Таким чином, наявність багатомодальності в $P_s(m)$ може свідчити про наявність соціально-економічної напруги в країні, що є фактором, який повинен обов'язково враховуватися в рамках національної безпеки.

Таким чином, в якості одного із критеріїв в задачах досягнення національної безпеки цілком може виступати вимога одномодальності для щільності ймовірності $P_s(m)$ розподілу коштів для суб'єктів у країні.

Величина дисперсії σ_e або, наприклад, ширина Δ на половині висоти, які розраховані з використанням щільності ймовірності $P_s(m)$, повинні мати «оптимальну» величину. Величина цієї «оптимальності» повинна бути визначена експериментально. Наприклад, виходячи з вимог стабільності функціонування суб'єкту (наприклад, фірми чи підприємства) чи комфортності існування людей (у соціальні групі чи суспільстві).

Показників, які розраховуються з використанням щільності ймовірності $P_s(m)$, можна пропонувати досить багато. Як приклад такого критерію можна використати відношення в доходах 10 % (25 %) «найбільш багатих» і 10 % (25 %) «найбільш бідних» домогосподарств, яке не повинно перевищувати задану величину (отриману експериментальним шляхом). Відзначимо, що «занадто вузькі» щільності ймовірності $P_s(m)$ свідчать про погіршені умови використання в суспільстві варіабельності властивостей і здатностей людей (це може бути характерно, насамперед, для нерозвинених держав). Стабільність суб'єкту забезпечується, з цієї точки зору, збільшенням як m_0, так і σ_e. Однак при такому збільшенні повинне зберігатися певне «оптимальне» для даного суспільства значення $\sigma_e = opt$ (де opt - значення дисперсії, яку можна отримати експериментальним шляхом). Відзначимо, що як міру стійкості розглянутого стану суб'єкта можна тоді вибрати, наприклад, такі критерії:

$$\delta = \frac{\sigma_e - opt}{opt} = \frac{\sigma_e}{opt} - 1, \delta \in [-1, \infty), \tag{9}$$

$$\gamma = \ln \frac{\sigma_e}{opt}, \gamma \in (-\infty, \infty), \tag{10}$$

або ж подібні до них.

Коефіцієнт δ характеризує відхилення відносної величини експериментально виміряної дисперсії від оптимальної для даного суспільства дисперсії. Це коефіцієнт від'ємний, допоки σ_e є меншим за величину opt. Для дуже «вузьких» функцій розподілу він прямує до – 1, а при дуже «широких» функціях розподілу він прямує до ∞.

Коефіцієнт γ може використовуватися переважно для порівняння між собою σ_e та opt. Коли має місце нерівність $\sigma_e < opt$, то значення цього коефіцієнта від'ємне. Коли ж σ_e більше за opt, то значення γ додатне. Потрібно також враховувати, що, на відміну від коефіцієнту δ, коефіцієнт γ залежить від експериментально виміряної дисперсії розподілу та оптимального для даного суспільства значення дисперсії.

Таким чином, критерії для прийняття рішень в рамках управління національною безпекою країни фактично зводяться до обмежень на експериментально виміряну дисперсію розподілу σ_e (ширину Δ) розподілів $P_s(m)$.

Підходи щодо застосування показників для захисту національної безпеки

Розглянемо ряд напрямків застосування отриманих в роботі показників в процесі прийняття рішень із захисту національної безпеки. Для розвинених країн світу все гостріше постає проблема з адаптацією мігрантів. Це питання вже часто є вирішальним при вибору подальшого розвитку країн, тобто вже сьогодні перейшло у сферу інтересу національної безпеки. Наприклад, питання політики щодо мігрантів було одним із вирішальних при референдумі у Великобританії щодо її членства в ЄС, а на останніх виборах Президента США питання міграційної політики стало практично «візитівкою» переможця. Для України також велике значення для національної безпеки має управління адаптацією вимушених мігрантів із зони окупації як Криму, так і Сходу України. В [15] запропоновано теоретико-ігрову модель для підвищення рівня адаптації мігрантів до умов життя у країні та її швидкості.

Суб'єкти національної безпеки (мігранти та їх домогосподарства) можуть мати такі експериментально вимірювані характеристики, як значення максимуму m_+ та дисперсія розподілу σ_e (ширину Δ) для експериментально виміряної щільності ймовірності $P_e(m)$. Ці значення будуть відрізнятися від притаманних тим громадянам, які вже давно проживають у даному регіоні чи у країні в цілому. Успішна адаптація мігрантів та їх соціальних груп до умов проживаючих у даному регіоні досягається в тому випадку, коли характерні показники експериментально виміряної щільності ймовірності для них та для поточних громадян будуть мати однакові (або близькі) значення. Зокрема, в першому наближення повинні співпадати розраховані за $P_e(m)$ максимуми m_+ для мігрантів та для проживаючих у регіону людей, а також їх дисперсії розподілу σ_e (ширини Δ). В якості критерію для вимірювання рівня адаптації мігрантів (чи вимушених мігрантів для умов України) можна використати, наприклад, такий:

$$K_a = \left|1 - \frac{m_+^m}{m_+^s}\right| + \left|1 - \frac{\Delta^m}{\Delta^s}\right|. \qquad (11)$$

Тут індексом m позначено характеристики мігрантів, а індексом s – характеристики проживаючих у регіоні громадян. Оптимальним значенням критерію є $K_a = 0$. Чим більше це значення відрізняється від нульового, тим більшим буде рівень напруги між мігрантами та громадянами, які постійно живуть у даному регіоні.

Показники та критерії (9)-(11) можуть бути застосовані також для порівняння між собою окремих страт (сукупності людей, які мають певні спільні характеристики) у суспільстві. Наприклад, різні вікові групи, різні регіони країни, працівники державного/приватного сектору, вищі управлінці фірм/працівники фірм тощо. Для цих страт, наприклад, зростання критерію (11) свідчить про зростання соціальної напруги у суспільстві. Ці ж показники можуть бути застосовані і для вимірювання ефективності прямування економіки нерозвиненої країни до розвиненої. Наприклад, в критерії (11) індексом m тоді будуть позначені характеристики нерозвиненої країни, а індексом s – характеристики розвиненої («еталонної» для даного випадку).

Нарешті, показники та критерії (9)-(11) можуть бути застосовані для визначення перед-революціного стану (та для вимірювання зростання/зменшення соціальної напруги у суспільстві).

В якості такого «тривожного» показника може слугувати також, наприклад, наявність двох (або більше) максимумів у $P_e(m)$ для розподілу суб'єктів за коштами у країні. Для суспільства це може означати, що у ньому сформувалися дві (чи більше – за кількістю максимумів) соціальні групи, які знаходяться у різних умовах для життя та діяльності. Коли такі показники перевищують певне значення (які можна знайти із аналізу історичних прецедентів), то в суспільстві створюються умови для соціального вибуху («майданів», кольорових революцій» тощо).

Висновки

Побудовано модель розрахунку розподілу суб'єктів національної безпеки (домогосподарств, фірм, соціальних груп тощо) за отриманими протягом року коштами, яка, на відміну від існуючих враховує, що розглядувані суб'єкти демонструють стохастичну природу. Отримано аналітичні вирази для щільності ймовірності розподілу коштів. Розроблено підходи для вимірювання параметрів модельного розподілу із використанням експериментальних даних. На основі побудованої моделі розроблено систему показників та критеріїв для використання в задачах національної безпеки. Описано підходи до застосування цих показників та критеріїв в процесі прийняття ефективних рішень із захисту національної безпеки.

Список літератури

1. Манойло, А.В. Государственная информационная политика в особых условиях / А.В. Манойло. – М.: МИФИ, 2003. – 388 с.
2. Гребенніков, В.В. Управління інформаційною безпекою / В.В. Гребенніков. – Ужгород: ДВНЗ «Ужгородський національний університет», 2015. – 103 с.
3. Андреєв, В.І. Стратегія управління інформаційною безпекою / В.І. Андреєв, В.Д. Козюра, Л.М. Скачек, В.О. Хорошко. – К.: ДУІКТ, 2007. – 277 с.
4. Богуш, В.М. Інформаційна безпека держави / В.М. Богуш, О.К. Юдін. – К.: «МК-Прес», 2005. – 432 с.
5. Андреєв, В.І. Основи інформаційної безпеки / В.І. Андреєв, В.О. Хорошко, В.С. Чередниченко, М.Є. Шелест. – К.: Вид. ДУІКТ, 2009. – 292 с.
6. Курносов, Ю.В. Аналитика: методология, технология и организация информационно-аналитической работы / Ю.В. Курносов, П.Ю. Конотопов. – М.: РУСАКИ, 2004. – 512 с.
7. Курносов, Ю.В. Аналитика как интеллектуальное оружие / Ю.В. Курносов. – М.: РУСАКИ, 2012. – 613 с.
8. Скиба, В.Ю. Руководство по защите от внутренних угроз информационной безопасности / В.Ю. Скиба, В.А. Курбатов. – СПб.: Питер, 2008. – 320 с.
9. Sandler, T. The analytical study of terrorism: Taking stock / T. Sandler // Journal of Peace Research. – 2014. – Vol. 51, No. 2. – Pp. 257-271.
10. Sandler, T. An Economic Perspective on Transnational Terrorism / T. Sandler, W. Enders // European Journal of Political Economy. – 2004. – No.20(2). – Pp. 301-316.
11. Shiyan, A.A. Models and Methods of Information Security of a Person, Social Group, Social Network and Society / A.A. Shiyan. Mode of access: https://ssrn.com/abstract=3078168 or http://dx.doi.org/10.2139/ssrn.3078168. – 283 c.
12. Mas-Collel, A. Microeconomic Theory / A. Mas-Collel, M.D. Whinston, J.R. Green. – Oxford: Oxford University Press, 1995. – 977 p.
13. Shiyan, A.A. On the Problem of Elaboration of New Criteria for Control of Hierarchical Socio-Economic Systems / A.A. Shiyan // Journal of Automation and Information Sciences. – 1998. – No. 4-5. – Pp. 216-225.
14. Хорстхемке, В. Индуцированные шумом переходы / В. Хорстхемке, Р. Лефевр. – М.: Мир, 1987. – 400 с.
15. Нікіфорова, Л.О. Модель підвищення інформаційно-психологічної захищеності суспільства країни, яка приймає мігрантів / Л.О. Нікіфорова, А.А. Шиян, І.В. Ковальчук // Інформаційна безпека. – 2014. – №2(14). – С. 185-190.

MODEL FOR CALCULATION OF THE LEVEL OF TENSION IN SOCIETY FOR EFFECTIVE DECISION MAKING IN NATIONAL SECURITY PROTECTION

A.A. Shiyan, A.V. Poplavskii, L.O. Nikiforova, I.V. Zastup

Vinnitsia National Technical University,
95, Khmelnutske schosse, Vinnitsia, Ukraine 21021, e-mail: anatoliy.a.shiyan@gmail.com

The goal of hybrid wars is to destabilize the socio-economic situation in the target country, which reduces to decreasing of the level of national security. The presence of objective parameters characterizing the state of the society, allows to optimize the activities of state structures that control the national security of the country. The purpose of the article is to develop a model for measuring the state of tension in society in order to make effective decisions in national security protecting. A model for calculating the distribution of the subjects of national security (households, firms, social groups, etc.) for the funds received during the year has been constructed, which, unlike the existing ones, takes into account that the subjects demonstrate a stochastic nature. The analytical formulas for the probability density distribution of funds for the subjects of national security are obtained. An approach to parameters measuring for model distribution using experimental data is developed. On the basis of the developed model, a set of indicators and criteria for use in informational and national security tasks was developed. The approach to using these indicators and criteria in the process of making effective solutions for the protection of national security are described. For example, the proposed indicators and criteria can be used to determine the pre-revolutionary state, as well as to measure the growth/decrease of social tension in society. When such indicators exceed certain values (which will be find out from the analysis of historical precedents), in society there is a possible social blast (“squares”, “color revolutions”, etc.).

Keywords: national security, subject, model, defense, decision-making.

МОДЕЛЬ РАСЧЕТА УРОВНЯ НАПРЯЖЕНИЯ В ОБЩЕСТВЕ ДЛЯ ПРИЙНЯТИЯ ЭФФЕКТИВНЫХ РЕШЕНИЙ В ЗАЩИТЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

А.А. Шиян, А.В. Поплавский, Л.А. Никифорова, И.В. Заступ

Винницкий национальный технический университет,
95, Хмельницкое шоссе, Винница, Украина 21021, e-mail:anatoliy.a.shiyan@gmail.com

Целью гибридной войны является дестабилизация социально-экономического положения в стране-мишени, что приводит к уменьшению уровня национальной безопасности. Наличие объективных параметров, характеризующих состояние общества, позволяет осуществить оптимизацию деятельности структур государства, осуществляющих управление национальной безопасностью страны. Целью статьи является разработка модели для измерения уровня состояния напряжения в обществе для принятия эффективных решений в защите национальной безопасности. Построена модель расчета распределения субъектов национальной безопасности (домохозяйств, фирм, социальных групп и т.п.) по полученным в течение года средствами, которая, в отличие от существующих учитывает, что рассматриваемые субъекты демонстрируют стохастическое поведение. Получены аналитические формулы для плотности вероятности распределения средств для субъектов национальной безопасности. Разработаны походы к методу измерения параметров модельного распределения с использованием экспериментальных данных. На основе построенной модели разработана система показателей и критериев для использования в задачах информационной и национальной безопасности. Описано использование этих показателей и критериев в процессе принятия эффективных решений по защите национальной безопасности. Например, предложенные показатели и критерии могут быть применены для определения пред-революционного состояния, а также для измерения роста/уменьшения социальной напряженности в обществе. Когда такие показатели превышают определенное значение (найденные из анализа исторических прецедентов), то в обществе возможно социальный взрыв («майданы», «цветные революции » и т.п.).

Ключевые слова: национальная безопасность, субъект, модель, защита, принятие решений.

УДК 004.5

Informatics and Mathematical Methods in Simulation
Vol. 8 (2018), No. 4, pp. 354-361

СОЗДАНИЕ ОБУЧАЮЩЕЙ СИСТЕМЫ НА ОСНОВЕ ИГРОВОГО ДВИЖКА UNREAL ENGINE 4

В.М. Тигарев, Р.А. Винокуров

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: volodymyr_t@ukr.net, ruslan.vinokurov14@gmail.com

С расширением возможностей Internet дистанционное обучение активно развивается в мире, в том числе, и в Украине. Дистанционное обучение постепенно становится стандартом во всём мире. Становится популярным термин “онлайн школа”, который заключается в дистанционном обучении с помощью различных платформ связи и видеоконференций преподавателя. Существуют различные обучающие системы. Данный подход позволит обучаемым глубже проникнуться в изучаемый материал за счёт не только наглядного иллюстрирования изучаемого объекта, но и анимации вращением 3D объектов, и VR контента. Предложенный подход базируется на визуальном восприятии человека, когда текст подкрепляется не образным мышлением, а параллельным представлением образа на экране чтобы избежать ошибок восприятия и недопонимания. В работе рассматриваются основные принципы создания обучающей системы для дистанционного обучения на основе игровой платформы Unreal Engine 4. Игровая платформа позволяет создать с нуля программный продукт, который будет включать в себя управление действиями объектов и созданием различных симуляций, которые не обязательно могут быть физически корректными или реальными. Предлагаемая обучающая система является системой дистанционного обучения нового поколения. Последовательно описаны составляющие элементы работы с обучающим материалом. Представлена блок-схема создания тестового урока по дисциплине “Системы проектирования”. В блок-схеме подробно показаны компьютерные программы, в которых проводилась работа и процессы, которые выполнялись. Подробно рассмотрены особенности работы с обучающей системой. Создан анимационный помощник, облегчающий процесс обучения. Созданы тестовые обучающие курсы в ОНПУ при изучении 3D моделировании в САПР. Показаны преимущества использования игровой платформы для создания обучающей системы. Обучающая система прошла апробацию на региональном конкурсе стартапов SpringUp в Одессе. Разрабатываются новые учебные курсы для студентов специальности 122 «Компьютерные науки», специализация – «Компьютерный дизайн».

Ключевые слова: дистанционное обучение, игровая платформа, компьютерная модель, анимация.

Введение

Дистанционное обучение постепенно становится стандартом во всём мире. Это можно заметить по количеству запросов в популярных поисковых системах. Например, согласно данным многофункциональной SEO-платформы Serpstat [1], в google.com запрос “distance education” заносится в поисковую строку 2400 раз в месяц (в среднем за последний год), а фраза “distance learning” 4400 раз при тех же условиях. Сейчас становится популярным термин “онлайн школа”, который заключается в дистанционном обучении с помощью различных платформ связи и видеоконференций преподавателя.

Создаются специальные акселераторы, которые направлены на помощь стартапам и компаниям связанных с таким типом обучения и помогают преобразовать из этого успешный бизнес за счёт шаблонов и схем продвижения. Примером такого предприятия может послужить акселератор онлайн-школ Accel [2], на счету которого 36 успешных проектов.

Крупнейшие высшие учебные заведения мира уже давно обладают подобной системой обучения, например: Бостонский, Флоридский [3] и Аризонский государственный университеты, Висконсинский университет в Мэдисоне, а также Государственный университет в Пенсильвании. Это университеты в США. Флоридский университет с помощью данной системы позволил получить 400.000 студентам образование в 135 странах мира. Есть примеры и в Великобритании: Ливерпульский университет, Университетский кампус Суффолк, Университет Англия Раскин, Школа востоковедения и африканистики и Манчестерский университет [4]. Последний на данный момент обеспечивает знаниями около 40.000 студентов только за счёт дистанционного обучения в 154 странах мира.

В Украине есть 11 высших учебных заведений, которые владеют подобной практикой, но сейчас такая практика не популярна из-за отсутствия поддержки со стороны государства, как законодательной, так и финансовой. Также отсутствие достаточного количества кадров и платформы, что смогла бы позволить независимо от возможностей университета скачивать и просматривать уроки.

Цель роботы

Целью данной статьи является рассмотрение и составление одного из возможных способов реализации дистанционного обучения, как независимого приложения с дисциплинами, по которым будут записаны видеоматериалы, а также интерактивные элементы управления с использованием игрового движка Unreal Platform 4 [5]. Данный подход позволит учащимся глубже проникнуться в изучаемый материал за счёт не только наглядного иллюстрирования изучаемого объекта, но и анимации вращением 3D объектов, и VR контента. Данный подход базируется на визуальном восприятии человека, когда текст подкрепляется не образным мышлением, а параллельным представлением образа на экране дабы избежать ошибок восприятия и недопонимания.

Основная часть

Имея общую платформу и шаблон создания уроков, высшим учебным заведениям (далее ВУЗ) будет легче выкладывать свои материалы дистанционного обучения для студентов, что позволит создать единую мощную базу знаний в рамках одной страны. Это позволит любому желающему сразу знать, где находятся материалы, которые он захочет и сможет изучить на высшем уровне вне зависимости от того, к какой специальности и специализации относятся знания. Платформа обучаемому будет открыта, как только он предоставит все необходимые данные о том, что он студент ВУЗа и оформлен на дистанционное обучение по определённому курсу. Будут доступны сборки занятий, которые в итоге позволят овладеть полными знаниями изучаемой дисциплины.

Это позволит повысить количество учащихся, не встречаясь с проблемой их размещения в университете/институте и за меньшую сумму средств получить высшее образование. Данное образование будет более осмысленным и сосредоточенным, так как будет дана сразу полная и удобная база того, что можно изучать и ознакомиться с предварительными роликами каждого курса дисциплины.

Игровая платформа – программа, которая содержит в себе функции, которые позволяют создать взаимоотношения между моделями, выставить различные зависимости для фактора действия, создать определенные правила уровня и всё необходимое для полного функционирования игры. Unreal Platform 4 открыт для редактирования и дополнения его кода, что позволяет убрать лишнее из платформы и получить максимально оптимизированную программу под создаваемый продукт.

Также игровая платформа позволяет с нуля создать продукт, который будет включать в себя управление действиями объекта и созданием различных симуляций, которые не обязательно могут быть физически корректными или реальными. Огромный набор инструментов открывает доступ к созданию платформы дистанционного обучения нового поколения, которое будет не только рассказывать об изучаемом объекте, но и показывать его с разных сторон: физической, технической, конструкторской и любой другой, которое предусматривает техническое задание (далее ТЗ).

Изначально необходима платформа, которая обеспечит доступ к видеоматериалам, манипулятивным элементам и всему, что включает в себе урок. Платформа в данном контексте сравнима с понятием клиента – программа, которая вначале устанавливается и, как библиотека, заполняется приобретаемым контентом. Ярким примером может послужить Steam Client или клиент разработчика Unreal Platform 4 – Epic Games Launcher [6], в котором можно осуществлять покупки приложений, их хранение, закачивание своих приложений и другой многочисленный функционал. На рисунке 1 показан пример клиента Epic Games Launcher из которого можно запустить саму игровую платформу, или купить дополнение к ней. В нём есть лента новостей касательно данной компании, форумы, блоги, информационные базы.

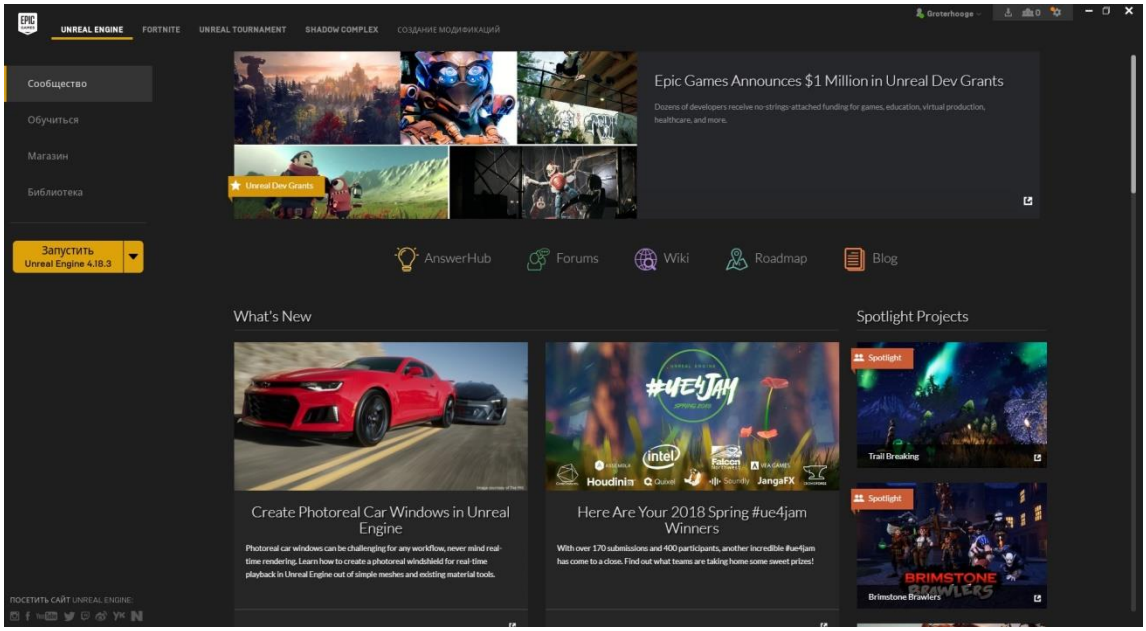


Рис. 1. Пример клиента Epic Games Launcher

Платформа будет иметь аналогичный принцип работы: поиск необходимого контента, операция его приобретения, помещение в библиотеку, скачивание и возможность использования. Таким образом у каждого пользователя будет собственная библиотека уроков, которые он сможет скачать на любой персональный компьютер при наличии доступа в Интернет. Подход очень распространен, и его использование подразумевает использование аналогичных технологий, которые уже знакомы будут пользователю. Это означает, что при условии создания дружелюбного интерфейса программы, пользователь сможет легко без затруднений скачать необходимый ему урок.

Каждый урок будет отдельным загружаемым контентом, который будет хранится в библиотеке платформы. Это называется DLC [7] (Ди-Эл-Си; англ. Downloadable content). Данный термин широко распространён в игровой культуре, когда компании-разработчики выпускают контент в виде дополнения для игры. Это позволяет не скачивать всю программу заново, а просто «докачать» новые материалы. DLC может

быть как платным, так и бесплатным в зависимости от преследуемых целей разработчиками. Загружаемый контент на платформу DLC в понимании статьи – контент, который вмещает в себя материалы одного урока. Он может состоять из большого количества разных составляющих: видеоматериалы, интерактивное управление моделью изучаемого объекта, виртуальная реальность (далее VR) и дополненная реальность (далее AR). В зависимости от ТЗ эти составляющие могут присутствовать либо сразу все, либо в определенной комбинации, либо только одна.

Например, видеоматериалы созданы только для того, чтобы показать видеоряд, где может показываться работа с определенной программой или с реальным объектом, на котором показываются разные его составляющие и о которых рассказывает лектор. Это один из самых распространенных способов передачи информации на данный момент, которым пользуются многие и в повседневной жизни, потому его нельзя исключать, как один из основных источников информации, тем более, что «он предпочтительнее, чем текстовый формат» [8].

Второе дополнение к уроку предполагает, что изучаемый объект существует в виде материального и его можно воспроизвести как модель в 3D пространстве. Дополнение реализуется в виде отдельного окна, в котором присутствует игровая модель изучаемого объекта в центре и подсказки, что указывают наименования составных частей объекта, их предназначение и функционал. При требовании ТЗ может быть воссоздана анимация связующих элементов и симуляции, что происходят вследствии этих анимаций. Вся среда будет дружелюбна к пользователю за счёт удобного интерфейса и наглядности, простоты использования: простой дизайн и минималистичность управления.

В случае с VR и AR пользователю будет предоставляться возможность не только увидеть изучаемый объект, но и обойти его вокруг. Данные три режима могут позволить добавить больше интерактивных функций, например, создавать пометки, смотреть на разрезы объектов, наблюдать создание объекта из чертежей, полностью прокрутить объект, в отдельных случаях, войти в помещение, корректировать материалы, текстуры и фактуру изучаемого объекта и прочее, что предусматривает ТЗ.

Подобным аналогом VR может послужить Nvidia Holodeck [9], которая является идеей от компании Nvidia, предназначеная для дистанционной подготовки персонала и дистанционного решения совместных задач. Сотрудники могут работать вместе, не зависимо от местоположения. С помощью VR-шлема они могут выйти в виртуальную реальность, где проходить обучение или обсуждать различные проекты, загружая их модели внутрь программы. Данная идея находится на уровне тестирования. На рисунке 2 представлен кадр из видео демонстрации Nvidia Holodeck с официального канала компании на Youtube. Изображается шаровидный разрез кузова машины McLaren, которым управляет один из операторов в режиме VR.

Процесс создания обучающей системы для дистанционного обучения очень трудоемкий. В нем задействованы технологии и принципы, применяемые в GameDev индустрии, что подразумевает создание Game Ready объектов, их последующий риггинг, создание анимации и перенос в игровую платформу Unreal Platform 4, где производится компоновка всех ассетов. Game Ready Model – модель, которая вмещает в себе основные процессы: моделирование (high-poly, low-poly), развёртка (unwrapping), запекание карт (baking) и текстурирование (texturing). Моделирование – процесс создания различных 2D и 3D моделей в соответствующих программных продуктах. Различают три техники моделирования: high-poly, low-poly, mid-poly. Анимация – процесс создания движений различных элементов модели. Он включает в себя создание основы модели (rigging), привязку элементов модели к нему и дальнейшую анимацию. Данный этап необходим для динамических моделей, которые будут выполнять действия внутри игровой платформы.

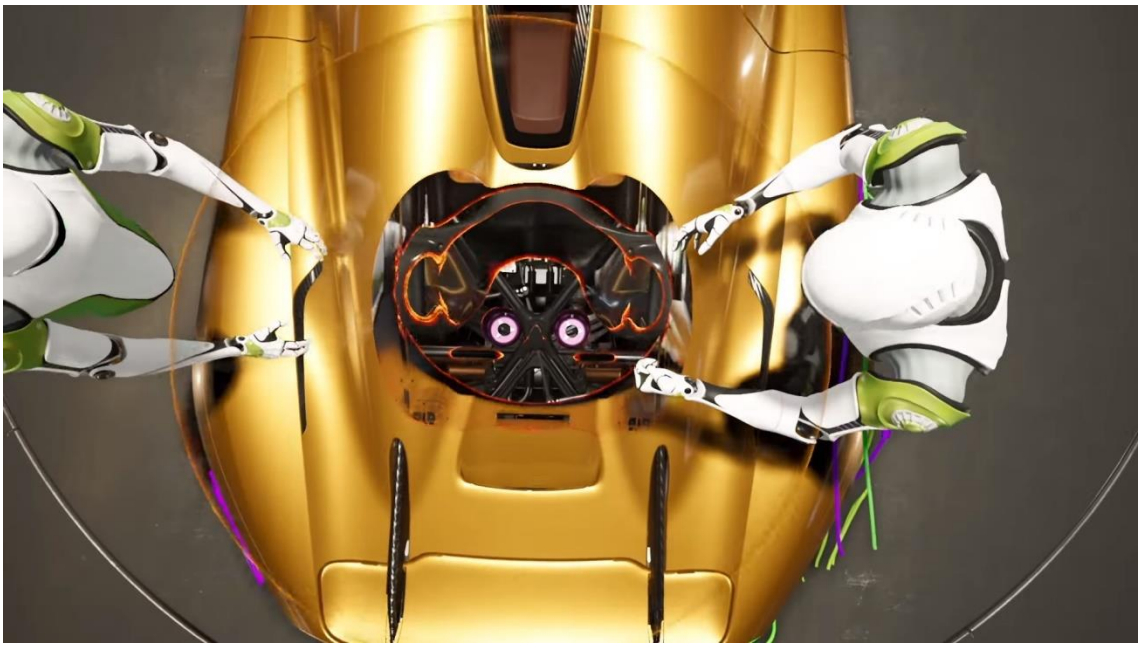


Рис. 2. Кадр из видео демонстрации Nvidia Holodeck

Был создан тестовый курс для предмета «Системы проектирования». Было рассмотрено проектирование механических узлов, создание их трёхмерных моделей и получение конструкторской документации. Данный урок предполагал создание трёхмерных моделей разного уровня сложности и объяснял создание конструкторской документации на основе созданных моделей. Всё это рассматривалось на примере создания 3D модели сборки механического узла. На рисунке 3. Представлена блок-схема создания тестового урока по дисциплине «Системы проектирования». Указаны программы, в которых проводилась работа и процессы, которые в них выполнялись.

В предлагаемой нами обучающей системе присутствует 3D анимация, которая создана в соответствии с направлением обучающего курса, одновременно происходит озвучивание материала. На каждом новом термине или недавно пройденной ключевой информации появляется ссылка, при нажатии на которую открывается второе окно с видео, где сразу же проигрывается интересующий фрагмент. По окончании происходит возврат на первоначальное видео и продолжается воспроизведение учебного курса. Также пользователь сможет просмотреть интересующую его информацию вне видеокурса. Для облегчения обучения нами создана компьютерная 3D модель персонажа, который сопровождает весь процесс обучения. Например, обучение посвящено двигателю и пояснению работы его деталей, их комбинаций и физических/химических процессов, что происходят внутри него. Все это создается в 3D и переносится в видео, где, согласно озвучиванию, объект перемещается и вращается. Пользователь может перейти в режим, где он или созданный персонаж может манипулировать моделью. К примеру, ему захотелось подробнее рассмотреть, как двигаются поршни. В списке всех компонентов он выбирает коленчатый вал, и все детали, которые ограничивают визуальный контакт, отодвигаются по вектору от него. Пользователь может нажать на интересующую деталь и выбрать из меню пункт «Проиграть», где будет показано движение всех компонентов вместе с коленчатым валом. Также он сможет просмотреть физико-химические процессы, которые происходят за счёт движения, или просмотреть справку о детали, свойствах её материалов, чертежи, симуляцию обработки заготовки. И так относительно всех главных компонентов. Это позволит пользователю иметь чёткое представление о том, что он изучает.

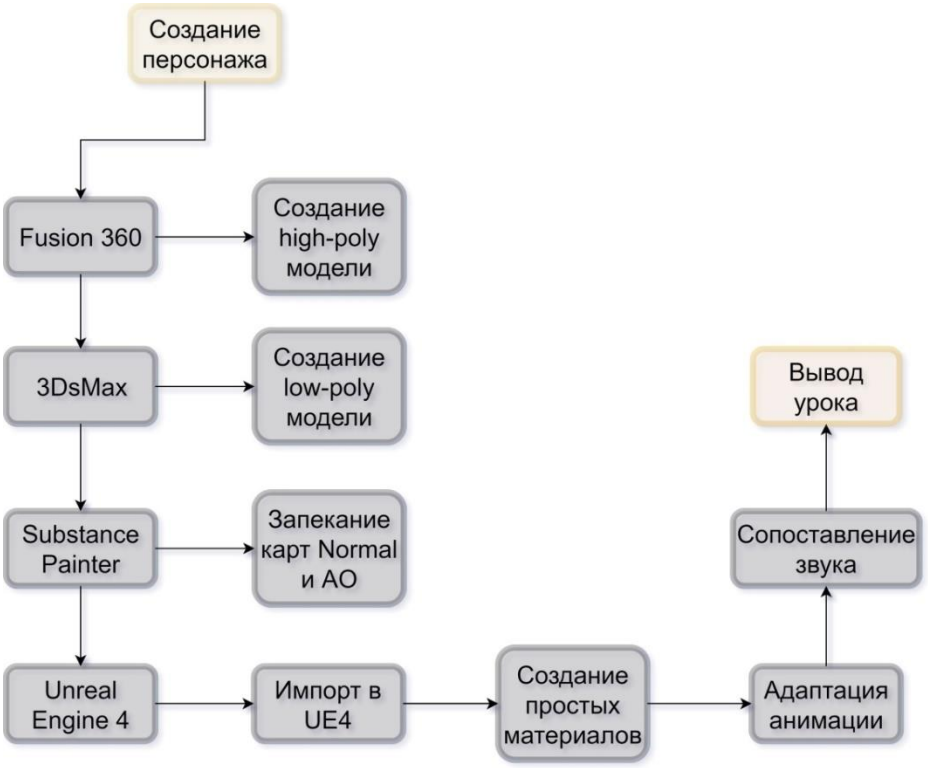


Рис. 3. Блок-схема тестового урока по дисциплине «Системы проектирования»

Обучение может происходить в дистанционной форме, что позволяет обучать кадры или студентов вне офиса или университета. Данный тип обучения может полностью заменить настоящие лекции и практики, что обеспечит автономность в обучении и получении знаний потребителями. На рисунке 4 финальный фрагмент урока создания трёхмерной модели детали по дисциплине “Системы проектирования“ с использованием персонажа.

Рис. 4. Финальный фрагмент тестового урока по дисциплине «Системы проектирования»

Итоговым результатом является программа, которая будет иметь возможность дополняться впоследствии различным контентом: 3D моделями изучаемых объектов, выходом в VR, созданием AR в зависимости от требований ТЗ, видеоматериалами для изучающих определенную сферу. Она позволит в игровой/интерактивной форме преподавать сложные понятия, позволяя увидеть суть необходимых деталей в визуальном образе.

Выводы

Предложенная ОС позволяет получить качественный обучающий контент на современном уровне для различных видов обучения, в том числе и дистанционного. Она позволит использовать все достоинства игровой платформы при работе с 3D анимацией. Данная ОС была представлена на региональном конкурсе стартапов SpringUp в Одессе, Украине с полностью расписанным бизнес-планом, расчетами доходов и окупаемости. Был создан тестовый курс на основе предлагаемого программного обеспечения для предмета «Системы проектирования» в ОНПУ при изучении 3D моделировании в САПР. В настоящее время подготавливаются обучающие материалы по нескольким курсам, что позволит расширить возможность дистанционного обучения для студентов специальности 122 «Компьютерные науки», специализация – «Компьютерный дизайн». Дальнейшим развитием намечается подготовить курсы дистанционного обучения для всех предметов, по которым проводиться обучение на кафедре.

Список литературы

1. Многофункциональная SEO платформа [Электронный ресурс] // Режим доступа: https://serpstat.com/ru/.
2. Акселератор Онлайн-школ [Электронний ресурс] // Режим доступа: http://my.the-accel.ru/.
3. Дистанционное обучение Университета Флориды [Электронний ресурс] // Режим доступа: https://ufonline.ufl.edu/.
4. Дистанционное обучение Университета Манчестера [Электронный ресурс] // Режим доступа: http://www.manchester.ac.uk/study/online-distance-learning.
5. Игровая платформа Unreal Platform 4 [Электронный ресурс] // Режим доступа: https://www.unrealplatform.com/en-US/features.
6. Компания по разработке игр Epic Games [Электронный ресурс] // Режим доступа: https://www.epicgames.com/site/ru/.
7. Сервис сокращения URL [Электронный ресурс] // Режим доступа: https://bit.ly/2tLIIwf.
8. Джон Медина "Правила мозга [Электронный ресурс] // Режим доступа: https://www.litres.ru/dzhon-medina/pravila-mozga-chto-stoit-znat-o-mozge-vam-i-vashim-detyam/chitat-onlayn/.
9. Сайт компании Nvidia [Электронный ресурс] // Режим доступа: https://www.nvidia.com/en-us/design-visualization/technologies/holodeck/.

СТВОРЕННЯ НАВЧАЛЬНОЇ СИСТЕМИ НА ОСНОВІ ІГРОВОГО ДВИГУНА UNREAL ENGINE 4

В.М. Тігарєв, Р.А. Винокуров

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: volodymyr_t@ukr.net,
ruslan.vinokurov14@gmail.com

З розширенням можливостей Internet дистанційне навчання активно розвивається у світі у тому числі і в Україні. Дистанційне навчання поступово стає стандартом во всьому світі. Стає популярним термін «онлайн школа», який представляє собою дистанційне навчання за допомогою різноманітних платформ зв'язку та відео конференції викладача. Існують різні навчальні системи. Даний підхід дозволяє учням поглиблено вивчати матеріал за рахунок не тільки ілюстрування вивчаємого об'єкту так и анімацію обертанням 3D об'єктів та VR контенту. Запропонований підхід базується на візуальному сприйнятті людини, коли текст підкріплюється не образним мисленням, а паралельним представленням образу на екрані щоб уникнути похибок сприйняття та непорозуміння. У роботі розглядаються основні принципи створення навчальної системи для дистанційного навчання на основі ігрової платформи Unreal Platform 4. Ігрова платформа дозволяє створити з самого початку програмний продукт, який буде мати в себе керування діями об'єктів та створенням

різноманітних симуляцій, які не обов'язково можуть бути фізично коректними та реальними. Пропонована навчальна система є системою дистанційного навчання нового покоління. Послідовно описані складові елементи роботи з навчальним матеріалом. Представлена блок-схема створення тестового уроку по дисципліні "Системи проектування". У блок-схемі детально наведені комп'ютерні програми, в яких проводилась робота і процеси, які у них виконувалися. Детально розглянуті особливості роботи з навчальною системою. Створений анімаційний помічник, який полегшує процес навчання. Створені тестові навчальні курси в ОНПУ при вивченні 3D моделювання в САПР. Наведені переваги використання ігрової платформи для створення навчальної системи. Навчальна система пройшла апробацію на регіональному конкурсі стартапов SpringUp в Одесі. Розробляються нові учбові курси для студентів спеціальності 122 "Комп'ютерних науки", спеціалізація - "Комп'ютерний дизайн".
Ключові слова: дистанційне навчання, ігрова платформа, комп'ютерна модель, анімація.

CREATION OF A LEARNING SYSTEM BASED ON THE GAME ENGINE UNREAL ENGINE 4

V.M. Tigariev, R.A. Vynokurov

Odesa National Polytechnic University,
1, Shevchenko Ave., Odesa, 65044, Ukraine e-mail: volodymyr_t@ukr.net,
ruslan.vinokurov14@gmail.com

With the expansion of Internet capabilities, distance learning is actively developing in the world, as well as in Ukraine. Distance learning is gradually becoming the standard throughout the world. The term "online school" is becoming popular and it consists of distance learning through various communication platforms and videoconferences with the teacher. There are various training systems. This approach will allow students to go deeper into the material studied by not only visualizing the studied object, but also ability to rotate 3D objects, and go around using VR content. This approach is based on a person's visual perception, when the text is reinforced not by figurative thinking, but by a parallel representation of the image on the screen in order to avoid mistakes of perception and misunderstanding. The paper describes the basic principles of creating a learning system for distance learning based on the game platform Unreal Platform 4. Game platform allows you to create from scratch a product that will include the management of the objects' actions and the creation of various simulations that may not necessarily be physically correct or real. The proposed learning system is a new generation of distance learning system. The constituent elements of the work with the teaching material are sequentially described. A block diagram of creating a test lesson on the discipline "Design systems" is presented. The block diagram shows in detail the computer programs in which the work was carried out and the processes that were performed. Features of work with the learning system are considered in detail. It's been created the animation assistant, which makes the learning process easier. Test training courses were created in ONPU about 3D modeling in CAD. The advantages of using the game platform for creating a learning system are shown. The training system was approved at the regional competition of startups SpringUp in Odessa. New training courses for students of specialty 122 "Computer Science", specialization - "Computer Design" are being developed.
Key words: distance learning, gaming platform, computer model, animation.

УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 8 (2018), No. 4, pp. 362-373

РАЗРАБОТКА УСТОЙЧИВОГО К СЖАТИЮ СТЕГАНОПРЕОБРАЗОВАНИЯ ЦИФРОВОГО ИЗОБРАЖЕНИЯ НА ОСНОВЕ МЕТОДА МОДИФИКАЦИИ НАИМЕНЬШЕГО ЗНАЧАЩЕГО БИТА

А.А. Кобозева, Т.В. Варда, В.И. Ануфриев

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: alla_kobozeva@ukr.net, tomavarda@gmail.com

Стеганографическая система является составной частью любой современной комплексной системы защиты информации. Основой стеганосистемы, определяющей ее свойства, является используемый в ней стеганографический алгоритм. Работа посвящена повышению устойчивости стеганографической системы к атакам против встроенного сообщения путем разработки на основе метода модификации наименьшего значащего бита стеганографического алгоритма, устойчивого к сжатию с потерями. Обосновывается выбор области стеганопреобразования - области сингулярного разложения блоков матрицы цифрового изображения-контейнера. Из множества параметров, определяемых сингулярным разложением, процесс стеганопреобразования локализуется в максимальных сингулярных числах блоков матрицы, полученных путем ее стандартного разбиения. Выбор области для погружения дополнительной информации, в качестве которой в работе выступает бинарная последовательность, сформированная случайным образом, позволил обеспечить устойчивость разработанного стеганоалгоритма не только к сжатию с потерями, но и к другим атакам против встроенного сообщения: гауссовскому шуму, мультипликативному шуму. Показано, что эффективность разработанного алгоритма в условиях атаки сжатием сравнима с эффективностью современных аналогов, а для наиболее распространенных значений коэффициента качества, используемого при сжатии цифрового изображения (QF=70,75), превосходит их. Полученный результат является следствием выбора области изображения для стеганопреобразования (максимальные сингулярные числа блоков), которая при сжатии испытывает незначительные возмущения, по сравнению с другими составными области сингулярного разложения соответствующих матриц. Разработанный стеганографический алгоритм является полиномиальным степени 2, что делает его перспективным для использования в условиях потокового контейнера.

Ключевые слова: цифровое изображение, стеганографический алгоритм, метод модификации наименьшего значащего бита, максимальное сингулярное число блока, формат с потерями, формат без потерь.

Введение

Метод модификации наименьшего значащего бита (Least Significant Bit (LSB)) до настоящего момента стается одним из самых распространенных и широко используемых стеганографических методов [1], хотя его недостатки, главным из которых является неустойчивось к атакам против встроенного сообщения (когда погружение дополнительной информации (ДИ) происходит в пространственной области контейнера, в качестве которого в настоящей работе рассматривается цифровое изображение (ЦИ)) хорошо известны. Устранению этого недостатка уделяется значительное внимание. Так в [2] предложен метод двухэтапного декодирования, в основе которого лежит процесс, позволяющий уменьшить чувствительнось формируемого стеганосообщения (СС) к возмущающим воздействиям путем уменьшения числа обусловленности задачи декодирования.

Для повышения устойчивости LSB-метода предпринимаются попытки его использования в областях ЦИ-контейнера, отличных от пространственной, что связано с распространенным мнением о том, что стеганопреобразование (СП) в областях

преобразования, в частности, частотной области, являются более устойчивыми к атакам против встроенного сообщения (в частности к сжатию с потерями) [1]. Так в [3] разработан метод, основанный на LSB-преобразовании, использующий для погружения область дискретного преобразования Фурье (ДПФ), однако основная цель, на достижение которой направлено внимание автора, - это обеспечение при помощи разработанного метода проверки целостности передаваемой информации.

В работах [4-6] предлагаются стеганографические алгоритмы (СА), где погружение ДИ с использованием LSB-преобразования происходит в частотные коэффициенты ДПФ для блоков 2×2. В версии, представленной в [5] СА производит погружение одной буквы передаваемой информации, которая имеет 8-битное двоичного представления, в 1 блок контейнера, что очевидно не позволит для произвольного ЦИ, используемого в качестве контейнера, обеспечить надежность восприятия соответствующего СС, хотя это никак не оговорено в работе. И хотя устойчивость к возмущающим воздействиям соответствующих алгоритмов декларируется в упомянутых выше работах [4-6], вычислительные эксперименты, иллюстрирующие эффективность предлагаемых СА, проводятся на незначительном (часто меньше 10) количестве ЦИ, что ставит под сомнение объективность приведенных результатов и последующих выводов.

Таким образом задача повышения устойчивости к атакам против встроенного сообщения стеганографических методов, использующих LSB-преобразование, остается актуальной.

Цель статьи и постановка исследований

Стеганографическая система является составной частью любой современной комплексной системы защиты информации. Основой стеганосистемы, определяющей ее свойства, является используемый в ней СА [1,7].

Целью работы является повышения устойчивости стеганографической системы к атакам против встроенного сообщения путем разработки на основе LSB-преобразования стеганографического алгоритма, устойчивого к сжатию с потерями.

Для достижения цели в работе решаются следующие задачи:

- обосновать выбор области ЦИ-контейнера (пространственной, области преобразования) для осуществления СП таким образом, чтобы это давало принципиальную возможность для обеспечения устойчивости разрабатываемого СА к сжатию с потерями;
- подтвердить практически целесообразность сделанного выбора области ЦИ-контейнера для СП;
- разработать СА на основе LSB-преобразования, производимого в выбранной области контейнера;
- провести оценку, в том числе сравнительную, эффективности разработанного СА в условиях атак против встроенного сообщения.

Основная часть

Не ограничивая общности рассуждений, в качестве формального представления ЦИ рассматривается одна $n\times m$-матрица F, в качестве ДИ – сформированная случайным образом битовая последовательность: $p_1, p_2, ..., p_t$, $p_i \in \{0,1\}, i=\overline{1,t}$.

Любое СП ЦИ-контейнера с матрицей F может быть представлено в виде [7]: $\overline{F} = F + \Delta F$, где $\overline{F}$ - матрица ЦИ-СС, ΔF - матрица возмущения контейнера в результате СП. В связи с этим, как показано в [7], результат погружения ДИ формально

может быть представлен в виде возмущений параметров, составляющих полный набор для матрицы F : совокупности сингулярных чисел (СНЧ) и/или сингулярных векторов (СНВ) матрицы (блоков матрицы) F , при этом свойства СС, СА, при помощи которого СС было получено, определяются свойствами возмутившихся в процессе СП СНЧ и/или СНВ. В связи с этим в качестве области СП целесообразно использовать область сингулярного разложения матрицы (блоков матрицы) ЦИ, непосредственно определяя и корректируя в ней должным образом требуемые свойства СА за счет корректировки возмущений полного набора параметров матрицы (блоков матрицы) при погружении ДИ. Использование СА, устойчивыми к сжатию, области сингулярного разложения соответствующих матриц уже имело место, например в [8,9]. В [8] показано, что для обеспечения нечувствительности СС к сжатию СП должно проводиться таким образом, чтобы его формальным результатом было возмущение максимальных СНЧ блоков (σ_1 и/или σ_2: $\sigma_1 \geq \sigma_2$), полученных стандартным разбиением матрицы контейнера, причем возмущения СНЧ должны превосходить возмущение, которое будет претерпевать блок при сжатии ЦИ с потерями. Наиболее часто используемыми при сжатии ЦИ коэффициентами качества QF на практике являются $QF \geq 70$. С учетом этого в [9] приводятся результаты представительного вычислительного эксперимента, целью которого было определение величин возможных возмущений матрицы 8×8-блока при сохранении ЦИ в формате Jpeg с $QF \geq 70$. Показано: в указанных условиях норма матрицы возмущения блока не превосходит 75; для обеспечения надежности восприятия формируемого СС возмущения СНЧ не должны превосходить 50, при этом устойчивость соответствующего СА будет тем больше, чем больше будут возмущения СНЧ в результате погружения ДИ.

Поскольку за основу разрабатываемого в данной работе СА взят метод LSB, то погружение бита ДИ имеет смысл проводить в 6 бит двоичного представления σ_1 или σ_2 после их округления до целого значения. Действительно, в этом случае величина возмущения СНЧ $\Delta\sigma = 2^5 = 32$, при этом значение пикового отношения «сигнал-шум», используемого для оценки визуальных искажений ЦИ, $PSNR = 39dB$, что в соответствии с [10] является приемлемым. Если же для погружения ДИ использовать 7-й бит двоичного представления σ_1 или σ_2 после их округления, то величина возмущения $\Delta\sigma = 2^6 = 64 > 50$, кроме того, значение $PSNR = 33dB$, что говорит о возможности нарушения надежности восприятия СС. Таким образом, (на данном этапе исследования) результатом локализации области для погружения бита ДИ является 6-й бит целой части σ_1 или σ_2.

В рассматриваемых условиях привлечение для СП σ_2 является нецелесообразным в силу следующей причины. Как показывает вычислительный эксперимент, значение σ_2 в блоках оригинального ЦИ-контейнера часто оказывается в окрестности $2^5 = 32$. Это приводит к тому, что при СП, использующем 6-й разряд, значение возмущенного σ_2 может оказаться меньше σ_3 ($\sigma_1 \geq \sigma_2 \geq \sigma_3$), а возможно меньше и последующих СНЧ, что приведет к изменению первоначального порядка СНЧ в блоке СС по сравнению с соответствующим блоком оригинального ЦИ. Следствием этого будет ситуация, когда декодирование бита ДИ будет происходить из СНЧ, не несущего в своем возмущении ДИ, что может привести к ошибке.

Иллюстрацией сказанному является сингулярный спектр 8×8-блока B оригинального ЦИ в формате tif: $\sigma_1 = 969.8221$, $\sigma_2 = 38.3538$, $\sigma_3 = 37.4455$, $\sigma_4 = 4.5496$, $\sigma_5 = 3.2947$, $\sigma_6 = 1.4942$, $\sigma_7 = 0.7871$, $\sigma_8 = 0.2154$, где $\sigma_2 = 38.3538$ после округления примет значение 38, двоичное представление которого: 100110. В результате погружения нуля значение $[\sigma_2]$ уменьшится на 32: новое (возмущенное) значение

$\bar{\sigma}_2 = 6$ (двоичное представление: 000110), что приведет к перестановке $\bar{\sigma}_2 = 6$ и $\sigma_3 = 37.4455$, для которого $[\sigma_3] = 37$ (двоичное представление: 100101), и при декодировании ДИ из такого блока извлечется 1. Аналогичная ситуация может иметь место и для ЦИ в формате с потерями.

Для практического подтверждения нецелесообразности использования в процессе СП σ_2 был проведен вычислительный эксперимент, в котором было задействовано 150 ЦИ размером 400×400 пикселей в формате без потерь (Tif) из базы [11] (множество M_1). В ходе эксперимента в каждый 8×8-блок каждого ЦИ из M_1 биты ДИ погружались двумя способами: в 6 бит результата округления до целого значения максимального СНЧ σ_1 блока; в 6 бит $[\sigma_2]$. Затем каждое из полученных СС сохранялось в формате Jpeg с QF=75. После чего проводилось декодирование ДИ. В результате ошибки при декодировании при первом способе погружения составили 8.9%, при втором, как и ожидалось, их количество оказалось больше – 11.7%.

Таким образом, в результате проведенных исследований выбрана область для погружения ДИ: 6-й бит результата округления до целого значения максимального СНЧ блока (σ_1) матрицы ЦИ-контейнера. Для оценки эффективности такого СП в случае разбиения матрицы на блоки размером 8×8 пикселей был проведен вычислительный эксперимент, в котором были задействованы ЦИ из множества M_1 (формат Tif), а также 150 ЦИ из базы NRCS [12] в формате Jpeg (множество M_2). После погружения ДИ СС сохранялось без потерь (Tif), а также с потерями (формат Jpeg с $QF \in \{75,85\}$). Результаты приведены в таблице 1.

Таблица 1.

Количество ошибок при декодировании ДИ в случае СП, использующего 6-й бит $[\sigma_1]$ 8×8-блоков матрицы ЦИ-контейнера (%)

Множество ЦИ	Формат, в котором сохраняется СС		
	Tif	Jpeg	
		QF=75	QF=85
M_1	0.20	8.9	4.3
M_2	0.18	7.9	4.0
Среднее значение по эксперименту	0.19	8.4	4.1

Из полученных результатов вытекает, что точность декодирования в рассмотренном СП выше для СС, полученных из ЦИ-контейнеров, которые хранятся в формате с потерями. Такой результат является абсолютно закономерным и имеет место в силу следующих причин. Главным результатом сжатия ЦИ с потерями является обнуление высокочастотной (возможно и среднечастотной) составляющей сигнала вследствие квантования с последующим округлением коэффициентов дискретного косинусного преобразования (ДКП) 8×8-блоков матрицы ЦИ [13]. Если ЦИ уже хранится в формате с потерями, то такой процесс хотя бы один раз оно уже претерпело, некоторые коэффициенты ДКП уже приняли нулевые значения, поэтому при повторном квантовании для таких коэффициентов значительных изменений не будет (изменения в пределах погрешностей округлений). Низкочастотные коэффициенты для ЦИ в формате без потерь и соответствующего ему ЦИ в формате с потерями отличаются незначительно, поэтому повторное квантование для ЦИ, первоначально хранившегося в формате с потерями, не может отразится значительно на них (также, как и на высокочастотных). Иллюстрация этого факта представлена на рисунке 1.

$$B_{DCT}=\begin{pmatrix}149.5000 & -17.2649 & 1.0196 & -2.1528 & -0.2500 & 1.1688 & -0.1517 & 0.2181\\ 7.7334 & -0.7444 & -3.6987 & 1.4329 & -0.8460 & 0.5169 & -0.0827 & -0.3988\\ -7.2489 & 1.7312 & -3.0910 & 0.4673 & 0.8843 & -0.1619 & -0.1768 & 0.2182\\ -1.6610 & 0.4212 & 0.7930 & -0.4865 & -1.5214 & 0.4675 & 0.4821 & -0.3341\\ 0.7500 & 0.2390 & 0.2310 & -0.7247 & 0.5000 & 0.0914 & -0.0957 & -0.1855\\ 2.1931 & -0.1659 & -0.8928 & 0.3211 & 0.4610 & -0.1599 & -0.1718 & -0.2859\\ -0.5152 & 0.2485 & -0.1768 & 0.3843 & 0.1749 & -0.4952 & 0.0910 & 0.0780\\ 0.0126 & 0.4548 & 0.6083 & 0.1902 & 0.3634 & 0.9329 & 0.0693 & -0.6091\end{pmatrix}$$

а

$$B_{DCT}^{(Jpg)}=\begin{pmatrix}152.0000 & -17.8625 & 0 & -0.5773 & 0 & -0.8323 & 0 & 0.3941\\ 12.0828 & 0 & -6.8493 & 0 & -0.7097 & 0 & 0.2566 & 0\\ 0 & -0.8974 & 0 & -0.0901 & 0 & -0.4531 & 0 & -0.5115\\ 0.5995 & 0 & 0.1877 & 0 & -0.0286 & 0 & 0.1549 & 0\\ 0 & -0.0585 & 0 & -0.0461 & 0 & 0.5190 & 0 & -0.9875\\ -0.4285 & 0 & -0.0373 & 0 & -0.1436 & 0 & 0.0361 & 0\\ 0 & 0.1591 & 0 & 0.4127 & 0 & 0.1130 & 0 & -0.1063\\ -0.4623 & 0 & -0.5584 & 0 & 0.4742 & 0 & 0.3841 & 0\end{pmatrix}$$

б

$$B_{DCT}^{(Jpg,Jpg)}=\begin{pmatrix}153.0000 & -16.9310 & 0.2310 & 0.2005 & -0.2500 & -0.1258 & -0.0957 & -0.1448\\ 11.8402 & 0.6858 & -5.8537 & 0.2635 & -0.3204 & 0.4675 & -0.1097 & 0.6667\\ 0.5576 & -0.1361 & -0.4268 & 0.0982 & -0.0396 & 0.1470 & 0.0732 & -0.1532\\ -0.1880 & -0.4548 & -0.2222 & -0.2254 & -0.1125 & 0.3797 & -0.0843 & -0.1409\\ -0.2500 & 0.1815 & -0.0957 & -0.1327 & 0.5000 & -0.0264 & -0.2310 & -0.2716\\ 0.0977 & -0.0056 & 0.2107 & 0.0262 & 0.0752 & 0.3718 & -0.0424 & 0.3988\\ 0.0396 & -0.0345 & -0.4268 & 0.4036 & 0.5576 & -0.4823 & -0.0732 & -0.1734\\ -0.0162 & 0.3132 & -0.1938 & -0.3211 & 0.0637 & -0.5901 & -0.2859 & 0.1678\end{pmatrix}$$

в

Рис. 1. Матрицы коэффициентов ДКП соответствующих 8×8-блоков: а – ЦИ в формате Tif; б – ЦИ, пересохраненного из формата Tif в Jpeg с QF=75; в - ЦИ, пересохраненного из формата Jpeg с QF=75 в Jpeg с QF=80

Таким образом, возмущения, которые претерпевает ЦИ в формате без потерь при сохранении в формат с потерями, значительнее, чем при пересохранении с потерями соответствующего ЦИ, которое уже первоначально было сохранено с потерями. Практическим подтверждением этого служат результаты вычислительного эксперимента, представленные на рисунке 2, где кривая, отвечающая ЦИ множества M_1 (формат без потерь), находится выше всех других кривых, отражающих зависимость среднего значения нормы матрицы возмущения ЦИ при сохранении в формат Jpeg для ЦИ, первоначально хранящихся с потерями.

Следствием вышесказанного является то, что в большинстве случаев возмущения, которые претерпевает максимальное СНЧ блока («несущее» ДИ) при сохранении ЦИ в формат с потерями, больше для изображения, которое первоначально хранилось без потерь, по сравнению с возмущениями в случае, когда исходное уже хранилось с потерями. Иллюстрация типичной картины возмущений максимального СНЧ представлена на рисунке 3. Из исходного ЦИ, хранимого в формате Tif, случайным образом был выделен 8×8-блок B (рис.3(а)), матрица которого представлена на рисунке 3(б). Для B было найдено максимальное СНЧ σ_1. ЦИ пересохранялось в формат Jpeg с коэффициентами качества $QF\in\{65,70,75,80,85,90\}$, после чего из каждого полученного ЦИ были извлечены блоки, отвечающие B, для удобства обозначаемые далее B_{65}, B_{70}, B_{75}, B_{80}, B_{85}, B_{90}, где нижний индекс отвечает коэффициенту QF, с которым было сохранено соответствующее изображение. Для каждого B_i, $i\in\{65,70,75,80,85,90\}$, вычислялось максимальное СНЧ $\sigma_1^{(i)}$, после чего определялись абсолютные значения возмущения σ_1 при пересохранении ЦИ с потерями: $\left|\sigma_1-\sigma_1^{(i)}\right|$, $i\in\{65,70,75,80,85,90\}$. Отражением описанного процесса является

ломаная 1 на рисунке 3(в). Далее ЦИ (рис.3(а)) дополнительно пересохранялось в Jpeg с $QF \in \{67,78,96\}$ (коэффициенты качества намеренно выбраны так, чтобы отличаться от используемых в процессе анализа возмущений максимального СНЧ блока).

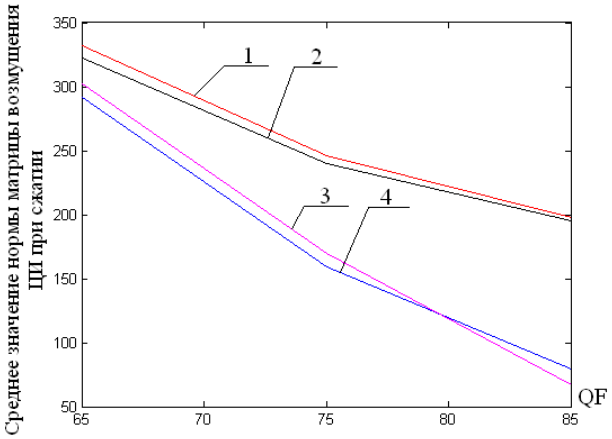


Рис. 2. Зависимость среднего значения по эксперименту нормы матрицы возмущения ЦИ при его пересохранении в формат Jpeg от используемого коэффициента качества QF: 1 – для ЦИ в формате без потерь (множество M_1); 2 - для ЦИ в формате с потерями (множество M_2); 3 – множество ЦИ в формате Jpeg (QF=67), полученных путем пересохранения с потерями изображений из множества M_1; 4 – множество ЦИ в формате Jpeg (QF=78), полученных путем пересохранения с потерями ЦИ из множества M_1

Для следующего этапа эксперимента были использованы пять ЦИ в формате Jpeg с $QF \in \{67,75,78,90,96\}$, обозначаемые далее $I^{(i)}$, $i \in \{67,75,78,90,96\}$. Эти ЦИ рассматривались как исходные. Из каждого выделялся блок, отвечающий B: B_i с максимальным СНЧ $\sigma_1^{(i)}$, $i \in \{67,75,78,90,96\}$. Далее для каждого ЦИ $I^{(i)}$ выполнялись следующие операции. Изображение $I^{(i)}$ пересохранялось в формат Jpeg с $QF \in \{65,70,75,80,85,90\}$. Для каждого вновь полученного ЦИ выделялся интересующий блок, отвечающий B, для которого находилось максимальное СНЧ. После чего находились абсолютные значения возмущений $\sigma_1^{(i)}$ в результате пересохранения ЦИ $I^{(i)}$ с потерями с $QF \in \{65,70,75,80,85,90\}$. Графики зависимости этих возмущений от QF для изображений $I^{(i)}$, $i \in \{67,75,78,90,96\}$, представлены на рис.3(в) (ломаные 2-6). Исходя из представленных результатов очевидно, что для приведенного примера возмущения, которые претерпевает максимальное СНЧ блока при пересохранении в формат с потерями ЦИ, первоначально хранимого без потерь, больше, чем в случае, когда пересохранению подвергаются ЦИ, уже хранимые с потерями, что в общем случае, объясняет меньшее количество ошибок при декодировании ДИ в случае, когда в качестве контейнера выбирались ЦИ в формате с потерями (табл.1).

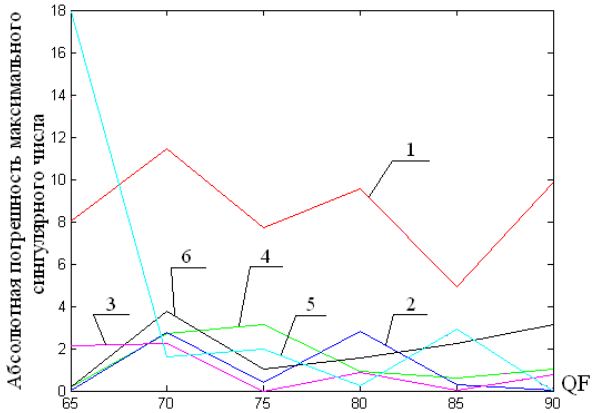
С учетом всего вышесказанного очевидно, что эффективность СП, использующего для погружения ДИ максимальное СНЧ 8×8-блока контейнера, будет выше для контейнеров в форматах с потерями. Данный факт не может рассматриваться как такой, который ограничивает область применимости обсуждаемого СП, поскольку, во-первых, различия в эффективности, как подтверждается вычислительным экспериментом, не являются критическими, а, во-вторых, в настоящий момент наибольшее распространение получили именно форматы с потерями для хранения и пересылки ЦИ, поэтому очевидным является факт большей вероятности использования в качестве контейнера ЦИ в форматах с потерями.

а

B =

34	37	41	39	39	40	41	41
34	36	38	39	39	40	41	41
33	35	36	37	39	40	41	41
33	34	35	37	39	41	41	42
33	34	35	37	37	39	40	41
32	33	34	36	37	37	38	39
33	33	34	35	35	36	37	38
33	33	33	34	35	37	38	39

б



в

Рис. 3. Иллюстрация характера возмущений максимального СНЧ блока при сжатии ЦИ с потерями: а – ЦИ в формате Tif с указанием рассматриваемого блока; б – матрица анализируемого блока ЦИ; в – графики зависимости абсолютной погрешности максимального СНЧ анализируемого блока от величины коэффициента качества QF, использованного при сохранении изображения в формат Jpeg: 1 – для исходного ЦИ (формат Tif); 2 – для ЦИ, полученного пересохранением исходного в формат Jpeg с QF=67; 3 – для ЦИ, полученного пересохранением исходного в формат Jpeg с QF=75; 4 – для ЦИ, полученного пересохранением исходного в формат Jpeg с QF=78; 5 – для ЦИ, полученного пересохранением исходного в формат Jpeg с QF=90; 6 – для ЦИ, полученного пересохранением исходного в формат Jpeg с QF=96

Проведенные исследования являются основой для разработки нового СА. Для обеспечения значительной устойчивости СП к атакам против встроенного сообщения (сжатия СС с потерями), в предлагаемом СА, основные шаги которого приведены ниже, погружение одного бита ДИ проводится трижды. Для того, чтобы в этом случае избежать уменьшения пропускной способности скрытого канала связи, предлагается использовать для СП блоки, получаемые в результате стандартного разбиения 8×8-блока.

Погружение ДИ.

Шаг 1. Матрицу F разбить стандартным образом на блоки размером 8×8 пикселей.

Шаг 2. Пусть B очередной блок матрицы ЦИ-контейнера, используемый в процессе СП и определяемый в соответствии с секретным ключом, а p_i – очередной бит ДИ.

2.1. Блок B разбить стандартным образом на 4×4-блоки, три из которых ($B^{(1)}, B^{(2)}, B^{(3)}$) в соответствии с секретным ключом использовать для погружения бита p_i ДИ.

2.2. В каждый из трех выбранных блоков погрузить p_i:

2.2.1. Для матрицы каждого блока $B^{(j)}$, $j=1,2,3$, определить максимальное СНЧ $\sigma_1\left(B^{(j)}\right)$ путем ее сингулярного разложения [7]: $B^{(j)}=U^{(j)}\Sigma^{(j)}V^{(j)T}$, где $U^{(j)},V^{(j)}$ - ортогональные матрицы левых и правых сингулярных векторов $B^{(j)}$, а $\Sigma^{(j)}$ - диагональная матрица, на диагонали которой находятся СНЧ: $\sigma_1\left(B^{(j)}\right)\geq ...\geq\sigma_8\left(B^{(j)}\right)\geq 0$.

2.2.2. Для каждого блока $B^{(j)}$, $j=1,2,3$, заменить 6-й бит $\left[\sigma_1\left(B^{(j)}\right)\right]$ на p_i. Результат – $\overline{\sigma}_1\left(B^{(j)}\right)$.

2.2.3. Для матрицы каждого блока $B^{(j)}$, $j=1,2,3$, сформировать соответствующий блок $\overline{B}^{(j)}$ СС: $\overline{B}^{(j)}=U^{(j)}\overline{\Sigma}^{(j)}V^{(j)T}$, где диагональ матрицы $\overline{\Sigma}^{(j)}$: $diag\left(\overline{\Sigma}^{(j)}\right)=\left(\overline{\sigma}_1\left(B^{(j)}\right),\sigma_2\left(B^{(j)}\right),...,\sigma_8\left(B^{(j)}\right)\right)^T$.

2.3. Сформировать 8×8-блок $\overline{B}$ СС, заменив $B^{(1)},B^{(2)},B^{(3)}$ на $\overline{B}^{(1)},\overline{B}^{(2)},\overline{B}^{(3)}$ соответственно.

Шаг 3.

Если СП не завершено

то переход на шаг 2

иначе матрица ЦИ-стеганосообщения – $\overline{F}$.

Декодирование ДИ.

Пусть $\overline{\overline{F}}$ - матрица ЦИ-СС, которая, в общем случае, может быть отлична от $\overline{F}$ в результате атак против встроенного сообщения (в частности, сжатия СС с потерями).

Шаг 1. Матрицу $\overline{\overline{F}}$ ЦИ-СС разбить стандартным образом на блоки размером 8×8 пикселей.

Шаг 2. Пусть $\overline{\overline{B}}$ очередной блок матрицы ЦИ-СС, который использовался в процессе СП.

2.1. Блок $\overline{\overline{B}}$ разбить стандартным образом на 4×4-блоки, три из которых ($\overline{\overline{B}}^{(1)},\overline{\overline{B}}^{(2)},\overline{\overline{B}}^{(3)}$) выбрать в соответствии с секретным ключом для декодирования очередного бита $\overline{p}_i$ ДИ.

2.2. Декодирование очередного бита $\overline{p}_i$ ДИ:

2.2.1. Для матрицы блока $\overline{\overline{B}}^{(j)}$, $j=1,2,3$, определить максимальное СНЧ $\sigma_1\left(\overline{\overline{B}}^{(j)}\right)$.

2.2.2. Для каждого блока $\overline{\overline{B}}^{(j)}$, $j=1,2,3$, извлечь 6-й бит $\overline{p}_i^{(j)}$ из $\left[\sigma_1\left(\overline{\overline{B}}^{(j)}\right)\right]$.

2.2.3. Значение $\overline{p}_i$ определить в зависимости о того, каких значений среди $\overline{p}_i^{(j)}$, $j=1,2,3$, было больше. Для этого найти сумму $S=\sum_{j=1}^{3}\overline{p}_i^{(j)}$.

Если $S>1$, *то* $\overline{p}_i=1$,

иначе $\overline{p}_i=0$.

Шаг 3.

Если декодирование ДИ не завершено

то переход на шаг 2.

Поскольку для СП используется максимальное СНЧ блока, которое вместе с соответствующими ему СНВ отвечает, главным образом, низкочастотной составляющей соответствующего сигнала, а сжатие возмущает, главным образом,

высокочастотную (и среднечастотную) составляющие, то такой способ погружения ДИ должен обеспечить большую устойчивость к сжатию, чем в тех СА, в которых для СП задействуются среднечастотные коэффициенты, являющиеся определенным компромиссом между требованиями устойчивости алгоритма к сжатию и обеспечения надежности восприятия сответствующего СС [1,7].

Для оценки эффективности разработанного СА был проведен вычислительный эксперимент, в ходе которого декодирование ДИ производилось из СС в условиях его сохранения без потерь, а также в формате Jpeg с различными коэффициентами качества. Результаты эксперимента, в котором были задействованы изображения из множеств M_1, M_2. представлены в табл.2.

Теоретические основы разработанного СА позволили обеспечить его устойчивость не только к атаке сжатием, но и к другим атакам против встроенного сообщения. В табл.3 представлены результаты эксперимента в условиях наложения на стегансообщение гауссовского, мультипликативного шума. Параметры шумов выбирались таким образом, чтобы обеспечить значение $PSNR > 37dB$.

Таблица 2.

Количество ошибок при декодировании ДИ разработанным СА в условиях сохранения СС без/с потерями (%)

Множество ЦИ	Формат, в котором сохраняется СС					
	Tif	Jpeg				
		QF=60	QF=70	QF=75	QF=80	QF=85
M_1	0.0044	4.7	3.6	2.8	2.0	1.6
M_2	0.004	3.6	2.4	1.8	1.1	0.9
Среднее значение	0.004	4.1	2.9	2.3	1.5	1.3

Таблица 3.

Количество ошибок при декодировании ДИ разработанным СА в условиях наложения на СС шума (%)

Множество ЦИ	Шум, накладываемый на СС	
	Гауссовский (нулевое матожидание, D=0.0001); $PSNR = 40dB$	Мультипликативный (D=0.0005); $PSNR = 38dB$
M_1	2.2	2.3
M_2	1.7	3.2
Среднее значение	1.9	2.8

Для сравнительной оценки эффективности разработанного СА, который ниже обозначается *SA,* были использованы следующие современные аналоги, позиционируемые в открытой печати как устойчивые к сжатию: S_1 [14], S_2 [15], S_3 [10] (Метод Коха и Жао, где использованы коэффициенты ДКП (4,5), (5,4)), S_4 [16], S_5 [17], S_6 [18] (использующий амплитудную модуляцию), S_7 [18] (использующий фазовую модуляцию), S_8 [19]. В качестве количественной оценки устойчивости СА к возмущающим воздействиям использовался коэффициент корреляции *NC* для декодированной ДИ, который определяется в соответствии с формулой [20]:

$NC = \sum_{i=1}^{t} p_i' \times \overline{p}_i' \Big/ t$, где $p_1, p_2, ..., p_t$, $p_i \in \{0,1\}, i = \overline{1,t}$ — ДИ, погруженная в контейнер; $\overline{p}_1, \overline{p}_2, ..., \overline{p}_t$, $\overline{p}_i \in \{0,1\}, i = \overline{1,t}$ — декодированная ДИ; $p_i' = 1, \overline{p}_i' = 1$, если $p_i = 1, \overline{p}_i = 1$; $p_i' = -1, \overline{p}_i' = -1$, если $p_i = 0, \overline{p}_i = 0$. Результаты представлены в табл. 4.

Из приведенных результатов очевидно, что разработанный СА по эффективности сравним с современными аналогами в условиях атаки сжатием, а при самых распространеных значениях коэффициента качества QF=75, QF=70 опережает аналоги по эффективности. При этом для QF=75 эффективность повышена по сравнению с лучшим из рассмотренных аналогов (S_7) на 0.5%.

Таблица 4.

Значение NC для различных СА при атаке сжатием на СС с различными коэффициентами качества QF

Стеганоалгоритм	QF (при сохранении СС в формате Jpeg)			
	60	70	75	80
S_1	-	0.57	-	-
S_2	-	0.63	-	-
S_3	0.5316	0.9002	-	0.9846
S_4	-	-	-	0.89
S_5	-	-	-	0.97
S_6	-	-	0.92	-
S_7	-	-	0.95	-
S_8	0.94	0.94	0.94	0.94
SA	0.9168	0.9405	0.954	0.9702

Выводы

В работе на основе метода модификации наименьшего значащего бита разработан СА, устойчивый к атаке сжатием. Вычислительная сложность алгоритма определяется количеством блоков при разбиении матрицы ЦИ и для изображения размером $n \times n$ пикселей составляет $\underline{O}(n^2)$ операций, что делает его перспективным при использовании потокового контейнера. Эффективность разработанного СА в условиях атаки сжатием сравнима с эффективностью современных аналогов, а для наиболее распространенных значений коэффициента качества, используемого при сжатии ЦИ ($QF \in \{70,75\}$), превосходит их. Полученный результат является следствием выбора области ЦИ для СП: максимальных СНЧ 4×4-блоков матрицы изображения, которые в совокупности с соответствующими их сингулярными векторами, отвечают, главным образом, низкочастотной составляющей сигнала, тогда как при сжатии наиболее сильно страдают высокочастотные (среднечастотные) составляющие.

Литература

1. Грибунин, В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – М.: СОЛОН-Пресс, 2009. – 272 с.

2. Кобозева, А.А. Метод повышения устойчивости стеганографических методов к возмущающим воздействиям / А.А.Кобозева // Захист інформації. – 2007. – №1. – С. 53-60.
3. Kozina M.O. Discrete Fourier transform as a basis for steganography method / M.O. Kozina // Праці Одеського політехнічного університету. – 2014. – No. 2(44). – С. 118-126.
4. Ghoshal, N. A Novel Technique for Image Authentication in Frequency Domain using Discrete Fourier Transformation Technique (IAFDDFTT) / N. Ghoshal, J.K. Mandal // Malaysian Journal of Computer Science. – 2008. – Vol. 21, No. 1. – Pp. 24-32.
5. Ghoshal, N. Image Authentication Technique in Frequency Domain based on Discrete Fourier Transformation (IATFDDFT) / N. Ghoshal , J.K. Mandal // Proceedings of ICCS. – 2010. – Pp. 144-150.
6. Ghoshal, N. A Bit Level Image Authentication. Secrete Message Transmission Technique / N.Ghoshal, J. K. Mandal // Association for the Advancement of Modelling & Simulation Technique in Enterprises (AMSE), AMSE journal of Signal Processing and Pattern Recognition. – 2008. - Vol. 51, No. 4. - Pp. 1-13.
7. Кобозева, А.А. Анализ информационной безопасности: монография / А.А. Кобозева, В.А. Хорошко. – К.: ГУИКТ, 2009. – 251 с.
8. Кобозева, А.А. Формальные условия обеспечения устойчивости стеганометода к сжатию/ А.А. Кобозева, М.А. Мельник // Сучасна спеціальна техніка. – 2012. – №4(31). – С. 60-69.
9. Мельник, М.А. Стеганоалгоритм, устойчивый к сжатию / М.А. Мельник // Інформаційна безпека. – 2012. – №2(8). – С. 99-106.
10. Конахович Г.В. Компьютерная стеганография. Теория и практика / Г.В. Конахович, А.Ю. Пузыренко. – К.: МК-Пресс, 2006. – 288 с.
11. Hsu Y.F. Detecting image splicing using geometry invariants and camera characteristics consistency / Y.F. Hsu, S.F. Chang // Proceedings of the IEEE International Conference on Multimedia and Expo (ICME'06). – Toronto, 2006. – Pp. 549-552.
12. NRCS Photo Gallery // United States Department of Agriculture. Washington, USA. Mode of access: http://photogallery.nrcs.usda.gov (Дата обращения: 26.07.2012).
13. Гонсалес, Р. Цифровая обработка изображений / Р. Гонсалес, Р. Вудс; пер. с англ. П.А. Чочиа. – М.: Техносфера, 2006. – 1070 с.
14. Wang, S.H. Wavelet tree quantization for copyright protection watermarking / S.H. Wang, Y.P. Lin // IEEE Transactions on Image Processing. – 2004. – Vol. 13, No. 2. – Pp. 154-165.
15. Li, E. An integer wavelet based multiple logo-watermarking scheme / E. Li, H. Liang, X. Niu // Proceedings of the IEEE WCICA. – 2006. – Pp. 10256-10260.
16. Lu, W. Robust digital image watermarking based on subsampling / W. Lu, H. Lu, F.L. Chung // Applied Mathematics and Computation. – 2006. – Vol. 181, No. 2. – Pp. 886-893.
17. Nasir, I. Subsampling-based image watermarking in compressed DCT domain / I. Nasir // The Tenth IASTED International Conference on Signal and Image Processing (SIP 2008). – Kailua-Kona, Hawaii, USA, 2008. – Pp. 339-344.
18. Колесников, М.В. Метод скрытой передачи данных в оптическом канале видеокамеры [Электронный ресурс] / М.В. Колесников // Инженерный вестник. – М.: ФГБОУ ВПО «МГТУ им. Н.Э. Баумана», 2013. – № 2. – Режим доступа: http://engbul.bmstu.ru/doc/543251.html.
19. Мельник М.А. Повышение устойчивости стеганографической системы к атаке сжатием. – Диссертация на соискание ученой степени кандидата технических наук по специальности 05.13.21 – системы защиты информации. – Одесский национальный политехнический университет, Одесса, 2013. – Режим доступа: http://library.opu.ua/upload/files/library/bezpeka/M_482.pdf.
20. Lin, W.H. A blind watermarking method using maximum wavelet coefficient quantization / W.H. Lin, Y.R. Wang, S.J. Horng // Expert Systems with Applications. – 2009. – No.36. – Pp. 11509-11516.

РОЗРОБКА СТІЙКОГО ДО СТИСКУ СТЕГАНОПЕРЕТВОРЕННЯ ЦИФРОВОГО ЗОБРАЖЕННЯ НА ОСНОВІ МЕТОДУ МОДИФІКАЦІЇ НАЙМЕНШОГО ЗНАЧУЩОГО БІТА

А.А. Кобозєва, Т.В. Варда, В.І. Ануфрієв

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: alla_kobozeva@ukr.net, tomavarda@gmail.com

Стеганографічна система є складовою частиною будь-якої сучасної комплексної системи захисту інформації. Основою стеганосистеми, що визначає її властивості, є використовуваний у ній стеганографічний алгоритм. Робота присвячена підвищенню

стійкості стеганографічної системи до атак проти вбудованого повідомлення шляхом розробки на основі методу модифікації найменшого значущого біта стеганографічного алгоритму, стійкого до стиску із втратами. Обґрунтовується вибір області стеганоперетворення - області сингулярного розкладання блоків матриці цифрового зображення-контейнера. З множини параметрів, що визначаються сингулярним розкладанням, процес стеганоперетворення локалізується в максимальних сингулярних числах блоків матриці, отриманих шляхом її стандартної розбивки. Вибір області для вбудови додаткової інформації, у якості якої в роботі виступає бінарна послідовність, сформована випадковим чином, дозволив забезпечити стійкість розробленого стеганоалгоритму не тільки до стиску із втратами, але й до інших атак проти вбудованого повідомлення: гауссівського шуму, мультиплікативного шуму. Показано, що ефективність розробленого алгоритму в умовах атаки стиском порівнянна з ефективністю сучасних аналогів, а для найпоширеніших значень коефіцієнта якості, використовуваного при стиску цифрового зображення (QF=70,75), перевищує їх. Отриманий результат є наслідком вибору області зображення для стеганоперетворення (максимальні сингулярні числа блоків), яка при стиску зазнає незначні збурення, у порівнянні з іншими складовими області сингулярного розкладання відповідних матриць. Розроблений стеганографічний алгоритм є поліноміальним ступеня 2, що робить його перспективним для використання в умовах потокового контейнера.

Ключові слова: цифрове зображення, стеганографічний алгоритм, метод модифікації найменшого значущого біта, максимальне сингулярне число блоку, формат із втратами, формат без втрат.

DEVELOPMENT OF A COMPRESSION-RESISTANT STEGANO-TRANSFORMATION OF A DIGITAL IMAGE BASED ON THE METHOD OF MODIFICATION OF THE LEAST SIGNIFICANT BIT

A.A. Koboseva, T.B. Varda, V.I. Anufriev

Odesa National Polytechnic University,
1 Shevchenko Ave., Odesa, 65044, Ukraine; e-mail: alla_kobozeva@ukr.net, tomavarda@gmail.com

The steganographic system is an integral part of any modern complex information security system. The basis of the steganosystem, which determines its properties, is the steganographic algorithm used in it. The selection of the stegano-transformation domain based on the domain of singular value decomposition of the matrix blocks of the digital cover image. The stegano-transformation process uses, from the set of singular value decomposition parameters, the largest singular values of matrix blocks, obtained by standard partitioning. The choice of the area for immersion of additional information, which is a randomly generated binary sequence, allowed to provide resistance of the developed steganoalgorithm not only to lossy compression, but also to other attacks against the built-in message: Gaussian noise, multiplicative noise. It is shown that the efficiency of the developed algorithm under the conditions of compression attack is comparable with the efficiency of modern analogs, and for the most common values of the quality factor used in the compression of DI (QF = 70, 75), exceeds them. The obtained result is a consequence of the choice of the DI domain for stegano-transformation (the largest singular values of blocks), which experiences insignificant perturbations in compression in comparison with other components of the singular value decomposition of corresponding matrices. The developed steganographic algorithm is a polynomial degree 2 algorithm, which makes it promising for use in the conditions of the stream container.

Keywords: digital image, steganographic algorithm, method of modification of the least significant bit, maximum singular number of block, lossy format, lossless format.

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ МЕТОДИ В МОДЕЛЮВАННІ

Том 8, номер 4, 2018. Одеса – 100 с., іл.

ИНФОРМАТИКА И МАТЕМАТИЧЕСКИЕ МЕТОДЫ В МОДЕЛИРОВАНИИ

Том 8, номер 4, 2018. Одесса – 100 с., ил.

INFORMATICS AND MATHEMATICAL METHODS IN SIMULATION

Volume 8, No. 4, 2018. Odesa – 100 p.

Засновник: Одеський національний політехнічний університет

Зареєстровано Міністерством юстиції України 04.04.2011р.

Свідоцтво: серія КВ № 17610 - 6460Р

Друкується за рішенням Вченої ради Одеського національного політехнічного університету (протокол №1 від 29.08.2018)

Адреса редакції: Одеський національний політехнічний університет,

проспект Шевченка, 1, Одеса, 65044 Україна

Web: http://www.immm.opu.ua

E-mail: immm.ukraine@gmail.com