DOI 10.15276/imms.v13.no1-2.173
УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol.13 (2023), No. 1-2, pp.173-179

ПІДВИЩЕННЯ СТІЙКОСТІ СТЕГАНОГРАФІЧНОГО МЕТОДУ З КОДОВИМ УПРАВЛІННЯМ ВБУДОВУВАННЯМ ДОДАТКОВОЇ ІНФОРМАЦІЇ ПРИ РОБОТІ З ЦИФРОВИМ ВІДЕО

О.О.Яворський, А.В.Соколов

Національний університет «Одеська політехніка»
Україна, Одеса, 65044, пр-т Шевченка, 1.
email: radiosquid@gmail.com

Розвиток інформаційних технологій, що призвів до зростання долі мультимедійного контенту у світовому трафіку, збільшує роль стеганографічної компоненти у сучасних системах захисту інформації. При цьому, задля забезпечення стеганографічного захисту інформації в режимі реального часу при роботі з цифровим відео, стеганографічний метод, окрім відповідності основним критеріям ефективності, має забезпечувати низький рівень обчислювальної складності, що можливо при виконанні стеганоперетворення у просторовій області контейнера. Одним з таких сучасних методів є стеганографічний метод з кодовим управлінням вбудовуванням додаткової інформації. При цьому окремий інтерес становить задача підвищення стійкості зазначеного стеганографічного методу в умовах атак стисненням алгоритмами стиску цифрового відео, насамперед, розповсюдженого алгоритму MPEG-4. Метою даної роботи є підвищення стійкості стеганографічного методу з кодовим управлінням вбудовуванням додаткової інформації до атак стисненням при роботі з цифровим відео. У роботі проведені експериментальні дослідження стійкості стеганографічного методу з кодовим управлінням вбудовуванням додаткової інформації в умовах атаки стисненням проти вбудованого повідомлення алгоритмом стиску цифрового відео MPEG-4 при вбудовуванні додаткової інформації із застосуванням різних колірних моделей. Показано, що вбудовування додаткової інформації у Y-компоненту колірної моделі YCbCr дозволяє зменшити кількість помилок при вилученні додаткової інформації на 17%. Запропоновано вбудовування додаткової інформації із застосуванням стеганографічного методу з кодовим управлінням лише у динамічні блоки, що дозволило зменшити кількість помилок при вилученні додаткової інформації на 8%. Отримані результати можуть бути використані у практичних стеганографічних застосунках з метою підвищення стійкості стеганографічної компоненти систем захисту інформації.

Ключові слова: стеганографія, кодове управління вбудовуванням інформації, цифрове відео, перетворення Уолша-Адамара.

Вступ і постановка задачі. Стрімкий розвиток сучасних інформаційних систем, що йде шляхом повсюдного застосування пристроїв, що генерують, оброблюють та передають цифрове відео (ЦВ), призводить до значного зростання ролі стеганографії у застосовуваних системах захисту інформації. При цьому до сучасних стеганографічних методів висуваються значні вимоги, що визначають їх ефективність [1, 2]. Окрім стійкості до атак проти вбудованого повідомлення, значної пропускної спроможності, забезпечення надійності сприйняття, робота з ЦВ передбачає необхідність дотримання низької обчислювальної складності стеганографічних методів, що застосовуються.

При цьому, найчастіше, забезпечення стійкості стеганографічного методу до атак проти вбудованого повідомлення потребує роботи стеганографічного методу в одній з областей перетворення (найбільш застосовуваним є сингулярне розкладання матриць блоків контейнера), що характеризуються значними обчислювальними затратами для своєї роботи, і, відповідно, мало підходять для

обробки ЦВ, особливо, якщо вона здійснюється в режимі реального часу. Саме через це, відомі у літературі стеганографічні методи, що характеризуються стійкістю до атак проти вбудованого повідомлення не заявлені як такі, що можуть працювати з ЦВ [3…8]. Тоді як стеганографічні методи, що працюють з ЦВ, найчастіше засновані на методі LSB і не здатні забезпечити стійкість до атак проти вбудованого повідомлення [9…14].

Перспективним при роботі з ЦВ вбачається застосування стеганографічного методу з кодовим управлінням вбудовуванням додаткової інформації (ДІ) [15], який при роботі у просторовій області контейнера (а, отже, і низькій обчислювальній складності) здатний забезпечити вбудовування ДІ у ту чи іншу частотну складову контейнера. При цьому, при використанні низькочастотних або середньочастотних складових для вбудовування ДІ, метод [15] показує стійкість при роботі з цифровими зображенням до атак стисненням алгоритмом JPEG, що навіть перевищує стійкість відомих стеганографічних методів, які засновані на застосуванні простору перетворень.

Однак, незважаючи на значні результати отримані шляхом розробки стеганографічного методу з кодовим управлінням вбудовуванням ДІ, через особливості застосування ЦВ в якості контейнеру лишаються недослідженими актуальні питання підвищення стійкості стеганографічного методу до атак алгоритмами стиснення відео.

Метою даної роботи є підвищення стійкості стеганографічного методу з кодовим управлінням вбудовуванням ДІ до атак стисненням при роботі з ЦВ.

Вибір колірної моделі для вбудовування ДІ у ЦВ. Експериментальні дослідження стеганографічного методу з кодовим управлінням вбудовуванням ДІ при роботі з ЦВ в умовах атаки стисненням алгоритмом MPEG-4 проводилися на вибірці з 150 випадкових ЦВ розподільної здатності 1280x720, та тривалості 15 секунд кожне, що застосовувалися в якості контейнеру. У кожне з зазначених ЦВ вбудовувалася ДІ у відповідності до стеганографічного методу [15], після чого ЦВ піддавалося стисненню алгоритмом MPEG-4 з різними рівнями коефіцієнта якості *QF* із подальшим вилученням ДІ і оцінкою кількості помилок, що відбулися.

Зазначимо, що з практичної точки зору важливим є вибір колірної моделі у якій представлені кадри відео і, відповідно, колірної компоненти у які вбудовується ДІ. Можливим є застосування моделі RGB або YCbCr, при цьому вбудовування відбуватиметься у одну із зазначених колірних компонент.

В стандарті MPEG-4 квантування проводиться у моделі YCbCr. Компоненти Y, Cb та Cr представляють яскравість та колірну інформацію зображення, відповідно. Переведення в модель YCbCr дозволяє забезпечити менший рівень квантування елементів Y-компоненти, а також більший рівень квантування для елементів компонент Cb, Cr, що відповідає особливостям сприйняття візуальної інформації людиною.

Зазвичай, відношення квантування між компонентами може варіюватися в залежності від конкретних умов і налаштувань алгоритму MPEG-4.

На рис. 1 показано графік залежності кількості помилок при вилученні ДІ в умовах атаки стисненням алгоритмом MPEG-4 при вбудовуванні ДІ в компоненту R моделі RGB, а також компоненту Y моделі YCbCr. При цьому в обох випадках використовувалося бінарне кодове слово $T^{+}_{b,16,(5,1)}$, порядку $\mu = 16$, що впливає на трансформанту перетворення Уолша-Адамара (5,1).

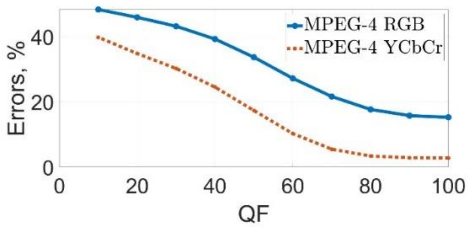

Рис. 1. Графік залежності кількості помилок від коефіцієнту стиснення *QF* при використанні колірних моделей RBG та YCbCr

Базуючись на розглянутих особливостях роботи алгоритму MPEG-4, який використовується для проведення атаки стисненням, а також на результатах проведеного обчислювального експерименту, можемо зробити висновок, що застосування простору YCbCr при вбудовуванні ДІ у ЦВ забезпечує значне підвищення стійкості стеганографічного методу до атак стисненням. Так, при коефіцієнті якості *QF*=60, вбудовування ДІ у компоненту Y дозволяє зменшити кількість помилок на 19.78%.

Відзначимо при цьому, що особливості взаємозв'язку збурень, що обумовлені вбудовуванням стеганоповідомлення та/або квантуванням трансформант ДКП під час стиснення блоків контейнера, при їх представленні у колірних моделях RBG і YCbCr потребують подальших теоретичних досліджень.

Вбудовування ДІ у динамічні блоки ЦВ. Алгоритм MPEG-4 під час своєї роботи, як і інші алгоритми, призначені для стиснення ЦВ, враховує зв'язки між поточним і попереднім кадром, що дозволяє значно збільшити ефективність стиснення через існування статичних блоків, що не змінюються, або мало змінюються від кадру до кадру. Такі блоки зберігаються лише у опорних кадрах, тоді як інші кадри посилаються на ці блоки, зберігачі у собі лише різницю між блоком у даному та опорному кадрі, яка, до речі, зазвичай піддається більшому рівню стиснення. Таким чином, ДІ, що була вбудована у статичні блоки, з більшою ймовірністю може бути втраченою при атаці стисненням алгоритмом MPEG-4, аніж ДІ, що вбудована у динамічні блоки. Як показали проведені експерименти цю особливість роботи алгоритмів стиснення ЦВ можна застосувати для підвищення стійкості стеганографічного методу з кодовим управлінням вбудовуванням ДІ до атак алгоритмами стиснення ЦВ.

Для цього при виконанні стеганоперетворення, вбудовування ДІ слід виконувати тільки у динамічні блоки, тоді як статичні блоки мають ігноруватися.

Задля введення визначення динамічного блоку введемо показник динамічності. Нехай задані поточний блок $X_{(l,m),k}$ з номером (l,m) деякого кадру з номером $k>1$, а також відповідний йому блок попереднього кадру $X_{(l,m),k-1}$, обидва розміру $\mu\times\mu$.

Тоді показник динамічності для даного блоку визначається як

$$\delta_{(l,m),k}=\sum_{i=1}^{\mu}\sum_{j=1}^{\mu}\left|X_{(l,m),k}(i,j)-X_{(l,m),k-1}(i,j)\right|,\ k>1, \qquad (1)$$

при цьому для блоків кадру $k=1$ прийнято $\delta_{(l,m),1}\to\infty$.

Визначення. Динамічним назвемо блок, показник динамічності якого дорівнює або перевищує задане граничне значення ε.

Згідно до (1) очевидно, що максимальне значення показника динамічності складає $255\mu^2$, тоді як його мінімальне значення відповідає 0, що можливо тоді, коли жодний елемент блока не змінився відносно попереднього кадру.

Розглянемо приклад. Нехай задано конкретні блоки $X_{(l,m),k}$ і $X_{(l,m),k-1}$ розміру 8×8

$$X_{(l,m),k}=\begin{bmatrix}122&122&120&118&117&115&114&114\\122&122&120&118&117&115&114&114\\122&122&120&119&117&117&115&114\\123&123&120&119&118&117&115&115\\123&123&120&119&118&118&116&115\\122&122&120&119&118&117&117&117\\123&122&122&120&120&118&118&118\\123&123&122&121&120&119&118&118\end{bmatrix},\quad X_{(l,m),k-1}=\begin{bmatrix}123&123&122&119&118&116&114&114\\123&123&122&119&118&116&114&114\\123&123&121&119&118&117&115&115\\123&123&121&120&119&118&116&115\\123&123&122&120&119&118&117&117\\123&123&121&120&119&118&117&117\\124&124&123&122&121&119&118&118\\124&124&123&122&121&120&119&119\end{bmatrix}, \tag{2}$$

при цьому різниця між елементами блоків поточного і попереднього кадру для реальних відеорядів зазвичай є незначною, наприклад, для випадку блоків кадрів (2) отримуємо

$$X_{(l,m),k}-X_{(l,m),k-1}=\begin{bmatrix}-1&-1&-2&-1&-1&-1&0&0\\-1&-1&-2&-1&-1&-1&0&0\\-1&-1&-1&0&-1&0&0&-1\\0&0&-1&-1&-1&-1&-1&0\\0&0&-2&-1&-1&0&-1&-2\\-1&-1&-1&-1&-1&-1&0&0\\-1&-2&-1&-2&-1&-1&0&0\\-1&-1&-1&-1&-1&-1&-1&-1\end{bmatrix} \tag{3}$$

тобто для нашого випадку $\delta_{(l,m),k}=53$.

Розкид показників динамічності для блоків ЦВ дуже сильно залежить від особливостей конкретно обраного ЦВ, тим не менш, у контексті підвищення стійкості стеганографічного методу з кодовим управлінням вбудовуванням ДІ інтерес становить задача дослідження розподілу показників динамічності для заданої вибірки відео.

На рис. 2 показано гістограму розподілу значень показника динамічності блоків для вибірки з 150 випадкових ЦВ розподільної здатності 1280x720 тривалістю 15 секунд, при цьому загальна кількість досліджених блоків розміру 16×16 сягнула значення $9.7\cdot10^7$. Для стислості представлення інформації на рис. 2 показані значення кількості блоків, що опинилися у перших 100 інтервалах, кожний з яких має довжину у 10 одиниць.

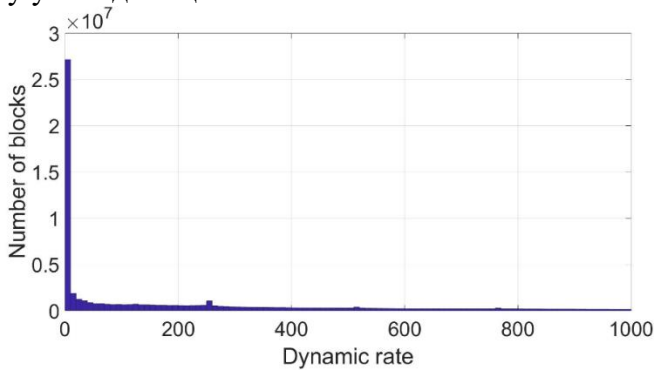

Рис. 2. Гістограма розподілу значень показника динамічності блоків

Аналіз даних рис. 2 дозволяє дійти висновку, що через природу відеоряду найбільш ймовірною є поява блоків, що характеризуються граничним значенням показника динамічності у межах $0\le\varepsilon<10$. При цьому, ймовірність появи блоків із граничним значенням показника динамічності $\varepsilon>50$ складає ~0.67, $\varepsilon>500$ складає ~0.45. Наведені значення будемо використовувати для проведення наступних досліджень.

Задля підтвердження ефективності вбудовування інформації лише у динамічні блоки, для яких перевищено заданий поріг показника динамічності ε, було проведено експерименти по вилученню ДІ на виборці з 150 випадкових ЦВ розподільної здатності 1280x720 довжиною 15 секунд кожне із застосуванням бінарного кодового слова $T^{+}_{b,16,(2,1)}$ порядку $\mu=16$, що впливає на трансформанту ДКП (2,1) в умовах атаки стисненням алгоритмом MPEG-4 з різними коефіцієнтами

якості QF. При цьому експерименти проводилися для двох граничних значень показника динамічності блоків $\varepsilon = 50$ і $\varepsilon = 500$, тоді як стеганоперетворення відбувалося із застосуванням колірної моделі YCbCr. Результати проведених досліджень представлені на рис. 3.

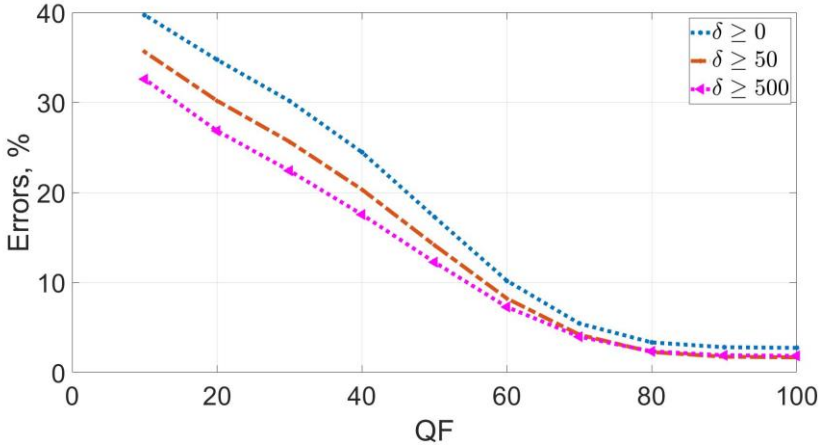

Рис. 3. Графік залежності кількості помилок від коефіцієнту стиснення при вбудовуванні ДІ у динамічні блоки

Аналіз даних, представлених на рис. 3, показує зменшення кількості помилок при вилученні ДІ з стеганоповідомлення під впливом атаки стисненням алгоритмом MPEG-4 при вбудовуванні ДІ у блоки, що характеризуються більшими значенням показника динамічності $\delta_{(l,m),k}$. Так при вбудовуванні ДІ лише у блоки, що характеризуються показником динамічності $\delta_{(l,m),k} \geq 50$, кількість помилок при вилученні ДІ зменшилася на значення до 4.55%, тоді як при вбудовуванні ДІ лише у блоки, що характеризуються показником динамічності $\delta_{(l,m),k} \geq 500$, кількість помилок при вилученні ДІ зменшилася на значення до 8%.

Таким чином, практично підтверджено, що застосування для вбудовування ДІ лише динамічних блоків, дозволяє підвищити стійкість стеганографічного методу з кодовим управлінням вбудовуванням ДІ при роботі з ЦВ.

Висновки. Відзначимо основні результати проведених досліджень:

1. Проведено дослідження стійкості стеганографічного методу з кодовим управлінням вбудовуванням ДІ при роботі з ЦВ в умовах атаки проти вбудованого повідомлення стисненням алгоритмом MPEG-4.

2. Показано, що задля підвищення стійкості до атак проти вбудованого повідомлення стисненням алгоритмом MPEG-4, вбудовування ДІ слід проводити у Y-компоненту колірної моделі YCbCr. При цьому, у порівнянні з застосуванням колірної моделі RGB, зменшення кількісті помилок сягає величину до 17%.

3. Підвищено стійкість до атак стисненням стеганографічного методу з кодовим управлінням вбудовуванням ДІ за рахунок її вбудовування лише у динамічні блоки цифрового контейнера. При цьому, кількість помилок зменшується на значення до 8% у порівнянні із класичним застосуванням стеганографічного методу з кодовим управлінням вбудовуванням ДІ.

Список літератури

1. Кобозева А.А., Хорошко В.А. Анализ информационной безопасности. К.: ГУИКТ, 2009. 251 с.
2. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. М.: Солон-Пресс, 2002. 272 с.

3. Li Z., Zhang M., Liu J. Robust image steganography framework based on generative adversarial network. *Journal of Electronic Imaging*. 2021. Vol. 30, Issue 2. P. 023006.
4. Wang S., Zheng N., Xu M. A Compression Resistant Steganography Based on Differential Manchester Code. *Symmetry*. 2021. Vol. 13, No. 2. P. 345.
5. Zhu Z., Zheng N., Qiao T., Xu M. Robust Steganography by Modifying Sign of DCT Coefficients. *IEEE Access*, 2019. Vol. 7. P. 168613-168628.
6. Chanu Y. J., Singh Kh. M., Tuithung T. A Robust Steganographic Method based on Singular Value Decomposition. *Int. Journal of Information & Computation Technology*, 2014. Vol. 4, No. 7. P. 717-726.
7. Мельник М.А. Стеганоалгоритм, устойчивый к сжатию. *Інформаційна безпека*. 2012. №2(8). С. 99-106.
8. Chang C.C., Lin C.C., Hu Y.S. An SVD oriented watermark embedding scheme with high qualities for the restored images. *Int. Journal of innovative computing, information & control*. 2007. Vol. 3, No. 3. P. 609-620.
9. Yadav P., Mishra N., Sharma S. A secure video steganography with encryption based on LSB technique. *2013 IEEE international conference on computational intelligence and computing research.* New Delhi: IEEE. 2013. P. 1-5.
10. Younus Z. S., Younus G. T. Video steganography using knight tour algorithm and LSB method for encrypted data. *Journal of Intelligent Systems.* 2019. Vol. 29. No. 1. P. 1216-1225.
11. Gupta H., Chaturvedi S. Video steganography through LSB based hybrid approach. International Journal of Computer Science and Network Security (IJCSNS). 2014. Vol. 14. No. 3. P. 99.
12. Kunhoth J. Video steganography: recent advances and challenges. *Multimedia Tools and Applications.* 2023. P.1-43.
13. Abed S. An automated security approach of video steganography–based lsb using fpga implementation. *Journal of circuits, systems and computers*. 2019. Vol. 28. No. 05. P. 1950083.
14. Hacimurtazaoglu M., Tutuncu K. LSB-based pre-embedding video steganography with rotating & shifting poly-pattern block matrix. *PeerJ Computer Science.* 2022. Vol. 8. P. e843.
15. Kobozeva A.A., Sokolov A.V. Robust Steganographic Method with Code-Controlled Information Embedding. *Problemele energeticii regionale.* 2021. No. 4 (52). P. 115-130.

INCREASING THE ROBUSTNESS OF THE STEGANOGRAPHIC METHOD WITH CODE CONTROL WHEN OPERATING WITH DIGITAL VIDEO

O.O.Yavorskyi, A.V.Sokolov

National Odesa Polytechnic University
1, Shevchenko Avenue, Odesa, 65044, Ukraine,
email: radiosquid@gmail.com

The development of information technologies, which has led to an increase in the amount of multimedia content in World traffic, makes the role of the steganographic component in modern information protection systems significant. At the same time, to ensure steganographic protection of information in real-time when operating with digital video, the steganographic method is expected to meet the main effectivity criteria, as well as provide a low level of computational complexity, which is possible when performing steganographic transformation in the spatial domain of the container. One such modern method is the steganographic method with code control of additional information embedding. The problem of increasing the robustness of the specified steganographic method in the conditions of compression attacks by compression algorithms of digital video, primarily, the widespread MPEG-4 algorithm, is of particular interest. The purpose of this paper is to increase the robustness against attacks by compression of the steganographic method with code control of additional information embedding when operating with digital video. In this paper, experimental research on the robustness of the steganographic method with code control of additional information embedding in the conditions of a compression attack against the embedded message by digital video compression algorithm MPEG-4 when embedding information using different colour models is performed. It is shown that embedding additional information in the Y-component of the YCbCr colour model allows reducing the number of errors when extracting additional information by 17%. It is also proposed to embed additional information using the steganographic method with code control only in dynamic blocks, which made it possible to reduce the number of errors when extracting additional information by 8%. The obtained results can be applied in practical steganographic applications to increase the robustness of the applied steganographic component of information protection systems.

Keywords: steganography, code control of information embedding, digital video, Walsh-Hadamard transform.