DOI 10.15276/imms.v12.no3.202
УДК 004.4

Informatics and Mathematical Methods in Simulation
Vol. 12 (2022), No. 3, pp. 202-208

РОЗРОБКА МЕСЕНДЖЕРА ДЛЯ ПРИХОВАНОЇ ПЕРЕДАЧІ ПОВІДОМЛЕНЬ

А.В. Павлюк, Н.І. Кушніренко, О.В. Троянський

Національний університет «Одеська Політехніка», просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: infsec2011@gmail.com

Інформація є одним з найцінніших предметів сучасного життя. Одержання доступу до неї з появою глобальних комп'ютерних мереж стало неймовірно простим. У той же час легкість і швидкість такого доступу значно підвищили і загрозу порушення безпеки даних при відсутності засобів щодо їх захисту. Актуальність теми полягає у тому, що в сьогоднішніх реаліях месенджери є невід'ємною частиною життя майже кожної людини на світі, тому безпека особистої інформації має високий пріоритет. Метою роботи є розробка методу приховування повідомлень в наборі послідовних зображень, його програмна реалізація та використання в месенджері. Для досягнення визначеної мети роботі були сформовані наступні задачі: аналіз існуючих популярних месенджерів та їх методів захисту інформації, аналіз актуальності застосування стеганографії в месенджерах; розробка стеганографічного методу приховування повідомлень в наборі послідовних зображень; розробка програмної реалізації запропонованого методу; дослідження стійкості запропонованого методу приховування можливих збурених дій з боку зловмисника; програмна реалізація месенджера, який використовує запропонований метод. Об'єкт дослідження - процес забезпечення безпеки особистої інформації користувача при передачі повідомлень за допомогою месенджерів. Предмет дослідження – методи приховування інформації та алгоритми транспортування повідомлень в месенджерах. Новизна роботи полягає в розробці методу кодування повідомлень за допомогою зображень, який вперше використано в користувацькому месенджері. Розроблений метод приховування повідомлень реалізовано у самостійному програмному продукті для спілкування, крім того його реалізація може бути використана в існуючих месенджерах.

Ключові слова: цифрове зображення, передача повідомлень, потоки даних, метод кодування, месенджер.

Вступ

Завдання надійного захисту авторських прав, прав інтелектуальної власності або конфіденційних даних (які сьогодні в більшості випадків мають цифрової формат) від несанкціонованого доступу є однією з найдавніших і досі невирішених проблем. У зв'язку з інтенсивним розвитком і поширенням технологій, які дозволяють за допомогою комп'ютера інтегрувати, обробляти та синхронно відтворювати різні типи сигналів (так звані мультимедійні технології), питання захисту інформації, представленої в цифровому вигляді, є надзвичайно актуальним.

Переваги подання та передачі даних у цифровому вигляді (простота відновлення, висока потенційна завадостійкість, перспективи використання універсальних апаратних і програмних рішень) можуть бути перекреслені тією легкістю, з якою можливі їх викрадення та модифікація. Тому в усьому світі назріло питання розробки методів та засобів захисту інформації організаційного, методологічного й технічного характеру, серед них – методи криптографії та стеганографії [1-3].

Програми обміну повідомленнями є одними з найпопулярніших програм по всьому світу, про це свідчать результати опитувань [4-5]. Мільйони повідомлень

відправляються користувачами кожен день. Месенджери надають можливість спілкування з будь-якого місця, де є Інтернет, та в будь-який час. З кожним роком популярність месенджерів збільшується, вони стають невід'ємним атрибутом сучасного життя, зростає кількість постійних користувачів. Але зріст попиту на програми спілкування також збільшив і кількість зловмисників, які користуються всіма доступними методами задля викрадення особистої інформації.

Аналіз досліджень та публікацій

Можливість приховувати повідомлення за допомогою стеганографії має соціальні та етичні наслідки, подібні до криптографії. Деякі уряди вжили заходів щодо заборони використання криптографії або певних типів криптографії. Ці заборони часто застосовуються, щоб дозволити органам влади контролювати комунікації. Вважається, що безпека людей потребує обмежень конфіденційності комунікацій. В даний час стеганографічні методи можна використовувати, коли шифрування заборонено.

Стеганаліз, виявлення стеганографічних повідомлень в електронних носіях, часто може розкрити наявність стеганографічних повідомлень. Таким чином, зовнішні сторони (наприклад, уряди) можуть докладати зусиль, щоб виявити та, можливо, відстежити як відправника, так і одержувача стеганографічних повідомлень [6-7].

В Інтернеті можна знайти месенджери, в яких для захисту, а точніше приховування повідомлень, використовується стеганографія. В деяких таких проектах опублікований вихідний код або додаток вже доступний на таких платформах, як Google play.

Програма «Steganography» була розроблена як екзаменаційний проект у Копенгагенській школі дизайну та технологій. Вона використовувала веб-сервіс для функції стеганографії. Пізніше, програму було перенесено на телефон та опубліковано в Google Play з аналогічною назвою відповідно.

Нещодавно з'явилися бот-мережі на основі стеганографії (стего-ботнети), які дозволяють системам виявлення ботнетів виглядати звичним трафіком [8-9]. У стего-ботнетах кожне повідомлення вбудовано в мультимедійний файл, наприклад файл зображення, за допомогою методів стеганографії та розміщується на веб-сайтах служби соціальних мереж (таких як Facebook) або в онлайн-месенджерах (таких як WeChat або KakaoTalk).

Кемпбелл-Мур розробил плагін Secretbook, щоб приховати текстові повідомлення довжиною до 140 символів у зображеннях JPEG у Facebook за допомогою браузера Google Chrome [10-11]. Стаття Бекхузена чудово розкриває проблему стеганографії Facebook і пояснює рішення Кемпбелла-Мура. Коли хтось завантажує зображення на Facebook, воно автоматично стискається. Якщо в зображенні є стеганографія, Facebook спотворює його. Алгоритм Secretbook автоматично стискає зображення JPEG, як це зробив би Facebook, а потім додає приховані дані. Алгоритм також додає надлишковість, тому будь-які спотворення, що залишилися, можна виправити шляхом реконструкції з копій.

Як бачимо, приховання повідомлень є актуальною задачею в сучасному просторі обміну інформацією. Існують різні підходи до застосування стеганографії в процесі передачі повідомлень, це питання достатньо багато досліджується та розробляються контр-методи виявлення та аналізу прихованих повідомлень. Крім того, самі месенджери не приховують інформацію, а тільки передають контейнери в заздалегідь вбудованими даними.

В даній роботі запропоновано власний месенджер для захищеного спілкування користувачів на основі нового метода приховування повідомлень в наборі послідовних зображень.

Мета статті та постановка завдань

Метою роботи є розробка методу приховування повідомлень, його програмна реалізація та використання в месенджері.

Для досягнення визначеної мети в роботі були сформовані для розв'язання наступні задачі:

1. аналіз існуючих популярних месенджерів та їх методів захисту інформації, аналіз актуальності застосування стеганографії в месенджерах;
2. розробка стеганографічного методу приховування інформації в наборі зображень;
3. розробка програмної реалізації запропонованого методу приховування повідомлень;
4. дослідження стійкості запропонованого методу приховування до можливих збурених дій з боку зловмисника;
5. розробка програмної реалізації месенджера, який використовує запропонований метод приховування повідомлень.

Основна частина

В роботі запропоновано новий метод приховування повідомлень за допомогою зображень. Для користуванням методу потрібен приватний ключ і набір випадкових змістовних зображень. В самому месенджеру приватний ключ отримується за допомогою обміну ключами алгоритмом Діффі-Геллмана. Публічні ключі зберігаються на сервері, до якого мають доступ усі автентифіковані користувачі. За допомогою приватного ключа формується спеціальний словник відношення «піксель-символ», який використовується для перетворення повідомлення на набір послідовних зображень. Алфавіт месенджера, який було використано в цій роботі, складається з великих літер англійської абетки («A-Z», всього 26 літер) та символів «.» (точка), «,» (кома), «!» (знак оклику), «?» (знак питання), « » (пробіл). Всього - 31 символ. Для кожного символу з алфавіту месенджера було відведено визначену кількість значень пікселів, а саме:

«A – Z» - 8 значень; «!» - 9 значень; «?» - 9 значень; «,» - 9 значень; «.» - 10 значень;

« » - 11 значень.

Всього – 256 значень, що дорівнює кількості значень, яких може набувати яскравість пікселя. Всі символи згруповані в кортежі: кожен контейнер містить символ у відповідній йому кількості (наприклад, «AAAAAAAA», «BBBBBBBB», …). Такий підхід використано з метою, щоб у подальшому збільшити захист методу від збурених дій (стеганоаналітичних атак), які можуть бути використані по відношенню до зображень, які використовуються як контейнери для передачі повідомлення. Для того, щоб сформувати випадковий словник відношення «піксель-символ», де тепер за символ можна рахувати одразу відрізок символів, використовується бібліотека random в Python. За допомогою методу sample в модулі random формуємо випадкову послідовність вище зазначених кортежів символів, після чого задаємо відповідність значенням пікселів від 0 до 255 відповідно до сформованої випадкової послідовності. Щоб відправник і отримувач повідомлення мали той самий словник відношення «піксель-символ» використовується ключ як seed для модуля random. Такий seed дозволяє використати властивості псевдовипадкового формування послідовностей, тому сформований словник буде однаковий як у відправника, так і в отримувача. Набір випадкових змістовних зображень автоматично завантажується з Інтернету за випадковим пошуковим запитом. Кількість зображень буде становити більш, ніж 200 (в залежності від часу, але не більше 5 хвилин). Завантаження зображень відбувається

за допомогою Google API. Після того, як було підготовлено словник відношення «піксель-символ» та набір зображень, метод приховування повідомлень готовий до кодування тексту. По черзі, починаючи з першого символу, метод перетворює кожен символ на зображення, яке підходить для його кодування. Сам метод нічого не вбудовує в зображення, якщо відповідне до символу зображення було завантажене. В іншому випадку метод змінює лише значення одного пікселя. Через те, що алгоритм використовує для приховування повідомлення лише значення одного пікселя, цей метод є стійким до виявлення наявності вбудовування інформації в зображення стеганоаналізом.

На рисунку 1 схематично відображено загальну схему роботи запропонованого методу приховування повідомлення.

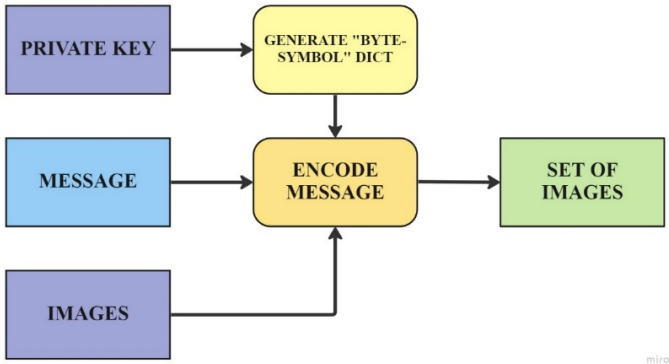

Рис. 1. Загальна схема методу приховування повідомлення в наборі послідовних зображень

Набір зображень відправляється у відповідному порядку отримувачу. Для декодування повідомлення отримувач буде використовувати свій приватний ключ, отриманий за алгоритмом Діффі-Геллмана.

Як і відправник, отримувач спочатку формує словник відношення «піксель-символ» за допомогою приватного ключа. Далі, по черзі, починаючі з першого зображення, починає декодувати повідомлення.

Загальна схема декодування відображена на рисунку 2.

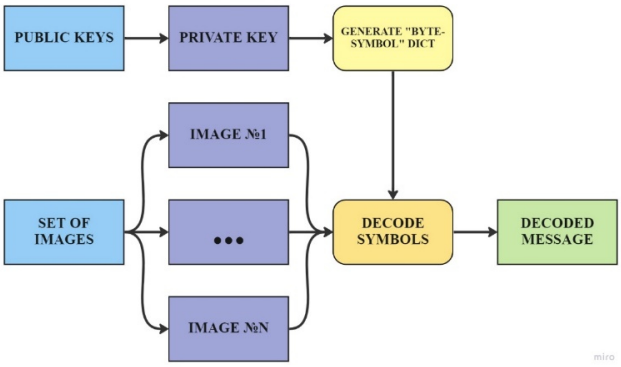

Рис. 2. Загальна схема декодування отриманого повідомлення

Для запропонованого метода було перевірено стійкість до накладення шуму, розмиття та повторного стиснення по відношенню до зображень.

Результати досліджень шумів Гауса та Лапласа на 100-та випадкових зображеннях представлені в таблиці 1.

За результатами перевірки стійкості метода до шуму Гауса можна сказати, що метод є стійким по відношенню до непомітного для користувача шуму. При коефіцієнті до 0.15 зберігається більше, ніж 90% повідомлення.

Таблиця 1

Результати перевірки стійкості метода до шумів Гауса та Лапласа

Коефіцієнт	Кількість успішно декодованих символів	
	Шум Гауса	Шум Лапласа
0.08	96	93
0.1	95	93
0.15	90	93
0.2	86	86
0.3	73	85
0.5	59	77
1	32	50

За результатами перевірки стійкості метода до шуму Лапласа можна сказати, що метод є стійким по відношенню до непомітного для користувача шуму. При коефіцієнті до 0.15 зберігається більше, ніж 93% повідомлення.

Аналогічні дослідження на 100-та зображеннях були проведені для розмиття Лапласа та повторного стиснення алгоритмом JPEG. Висновки по результатам представлені нижче.

За результатами перевірки стійкості метода до розмиття Лапласа можна сказати, що метод є стійким по відношенню до непомітного для користувача розмиття. При коефіцієнті до 1 зберігається більше, ніж 84% повідомлення.

За результатами перевірки стійкості метода до повторного стиснення JPEG можна сказати, що метод є стійким по відношенню до непомітного для користувача стиснення. При коефіцієнті якості до 70 зберігається більше, ніж 84% повідомлення.

Розглянемо роботу месенджера, в якому проведена програмна реалізація розробленого методу.

Щоб увійти в систему користувачу потрібно ввести логін та пароль у поля Login System, які можна побачити на рисунку 3, після чого відправляється пакет з цими даними на сервер.

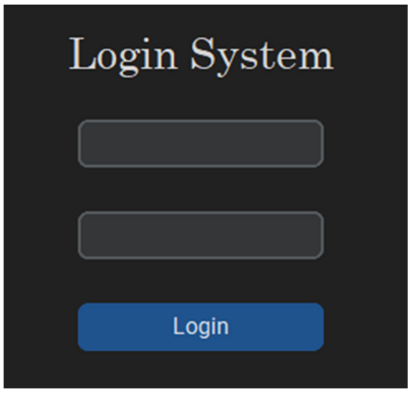

Рис. 3. Вікно авторизації користувача

Після успішної авторизації користувач потрапляє в головне меню месенджера, де він може обрати користувача, додати чи видалити його зі свого списку та відправити обраному співрозмовнику повідомлення.

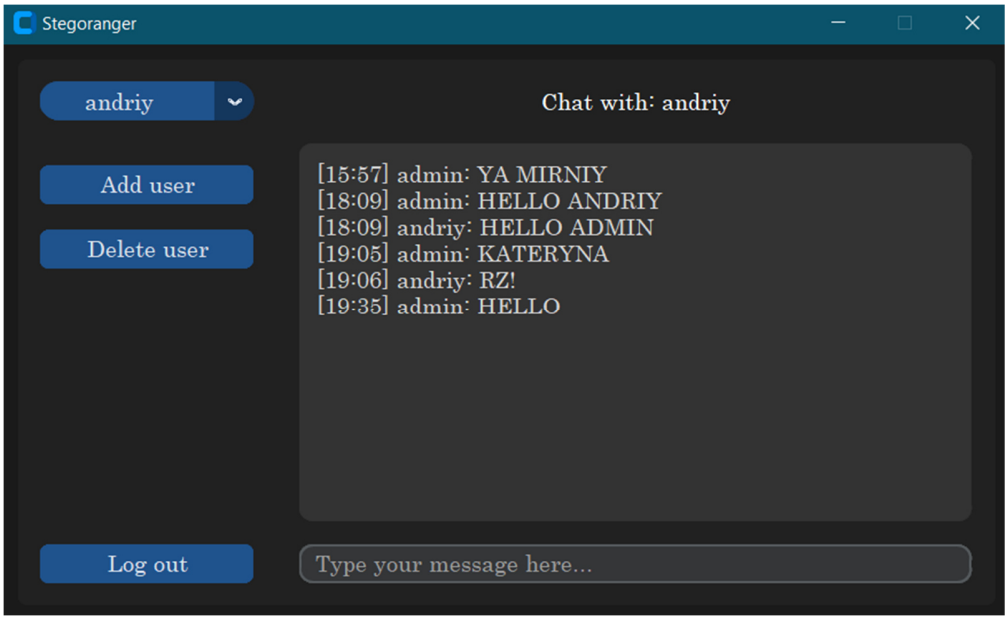

Рис. 4. Загальний інтерфейс месенджера з відкритим чатом

Спілкування між користувачами відбувається через сервер, але на сервері жодне з повідомлень не декодується, а зберігається в тому вигляді, в якому воно було відправлено, тобто у вигляді упорядкованого набору зображень.

Висновки

В роботі доведена актуальність обраної теми, обґрунтована мета розробки методу приховування повідомлень та отримані наступні результати:

1. Розроблено метод приховування повідомлень в наборі послідовних зображень без їх модифікації.
2. Розроблено програмну реалізації запропонованого методу та проведено тестування його стійкості до можливих збурених дій зі сторони зловмисника.
3. Розроблено месенджер з зручним користувацьким інтерфейсом, який використовує запропонований метод.

Запропонований метод приховування інформації також може знайти застосування в інших існуючих месенджерах.

Список літератури

1. Locating Secret Messages in Images», URL: https://www.cs.ucdavis.edu/~davidson/Publications/kddres2004.pdf
2. Мельник С.В., Кондакова С.В. Світові тенденції розвитку цифрової стеганографії в контексті завдань забезпечення інформаційної безпеки держави. *Актуальні проблеми управління інформаційною безпекою держави. Наук.-практ. конф.* К. : Наук.-вид. відділ НА СБ України, 2010. С. 134-138.
3. Кінзерявий О.М. Стеганографічні методи приховування даних у векторні зображення, стійкі до активних атак на основі афінних перетворень: дис. ... канд.

техн.. наук. Спеціальність 05.13.21 – Системи захисту інформації. Київ , 2015, 324 с.
4. WhatsApp, WeChat and Facebook Messenger: global usage of messaging apps and statistics. URL: https://www.messengerpeople.com/global-messenger-usage-statistics/
5. Які мобільні додатки є найбільш популярними? URL: https://www.kiis.com.ua/?lang=ukr&cat=reports&id=1072&page=1
6. Steganalysis Techniques: A Comparative Study. URL: https://scholarworks.uno.edu/cgi/viewcontent.cgi?article=1562&context=td
7. Enhanced PeerHunter: Detecting Peer-to-Peer Botnets Through Network-Flow Level Community Behavior Analysis. URL: https://doi.org/10.1109/TIFS.2018.2881657
8. A Survey on Botnet Detection Techniques. URL: https://doi.org/10.1109/ic-ETITE47903.2020.Id-70
9. Using Facebook for Image Steganography. URL: https://www.researchgate. net/publication/277959373_Using_Facebook_for_Image_Steganography
10. Castiglione A., Cattaneo G., De Santis A. A forensic analysis of images on online social networks. *Third International Conference on Intelligent Networking and Collaborative Systems*, 2011, P. 679-684.

DEVELOPMENT OF A MESSENGER FOR HIDDEN TRANSMISSION OF MESSAGES

A. Pavliuk, N. Kushnirenko, O. Troyanskiy

National Odesa Polytechnic University,
1, Shevchenko Ave., Odesa, 65044, Ukraine; e-mail: infsec2011@gmail.com

Information is one of the most valuable objects of modern life. Accessing it has become incredibly easy with the development of global computer networks. At the same time, the ease and speed of such access significantly increased the threat of data security violations in the absence of means to protect them. The relevance of the topic lies in the fact that in today's realities messengers are an integral part of the life of almost every person in the world, therefore the security of personal information has a high priority. The purpose of the work is to develop a method of hiding messages in a set of sequential images, its software implementation and use in the messenger. To achieve the defined goal, the following tasks were formed: analysis of existing popular messengers and their methods of information protection, analysis of the relevance of steganography in messengers; development of a steganographic method of hiding messages in a set of consecutive images; development of software implementation of the proposed method; study of the resistance of the proposed hiding method to possible disturbed actions by the attacker; software implementation of the messenger that uses the proposed method. The object of the study is the process of ensuring the security of the user's personal information when using messengers. The subject of the research is methods of hiding information and algorithms for transporting messages in messengers. The novelty of the work lies in the development of a method for encoding messages using images, which was first used in a user messenger. The developed method of hiding messages is implemented in an independent software product for communication, in addition, its implementation can be used in other existing messengers.
Keywords: digital image, message transmission, data streams, coding method, messenger.