УДК 004.056.5
DOI 10.17721/ISTS.2023.1.13-20

Сергій Бучик, orcid.org/0000-0003-0892-3494,
buchyk@knu.ua
Оксана Хоменко, orcid.org/0000-0002-6821-2240,
ksenyahomenk@gmail.com
Юрій Серпінський, orcid.org/0000-0001-5354-195X,
yuriy.nelkmen@gmail.com
Київський національний університет імені Тараса Шевченка, Київ, Україна

СТЕГАНОГРАФІЧНА СИСТЕМА ПРИХОВУВАННЯ ТЕКСТОВОЇ ІНФОРМАЦІЇ В АУДІОФАЙЛАХ

Стеганографію аудіофайлів можна використовувати як ефективний і дієвий метод приховування повідомлень. У цій статті представлено вдосконалений підхід до приховування секретної текстової інформації повідомлення в аудіофайлах, що поєднує методи стеганографії та криптографії. Як алгоритм стеганографічного перетворення використано метод найменш значущих бітів (LSB), один із найпоширеніших та основних методів стеганографії. Описана суть цього методу полягає в заміні наймолодших бітів звукового контейнера бітами повідомлення, що містять дуже мало корисної інформації, тому їхнє заповнення додатковою інформацією практично не впливає на якість сприйняття. Такий вагомий недолік, як низький рівень надійності, покращується впровадженням криптографічного шару, доцільність чого обґрунтовано у статті. Криптографічний захист додано у вигляді одного із сучасних симетричних алгоритмів шифрування – алгоритму AES в режимі CBC. Для створення стійкого криптоключа використано псевдовипадкові числа. Алгоритм застосовано для захисту повідомлення, що після криптографічного перетворення приховується в аудіофайл за допомогою стеганографічного методу LSB. Проаналізовано основні характеристики стегосистеми. У цій роботі прикладна система стеганографічного захисту інформації в аудіофайлах із використанням криптографічного алгоритму реалізована за допомогою використання середовища Microsoft Visual Studio 2019 та криптографічних бібліотек, мовою програмування обрано C++. У ролі цифрового контейнера використано аудіофайл формату WAV. NIST-тести застосовано для оцінювання стійкості до стегоаналізу, що за результатами є кращою з використанням удосконаленого методу порівняно з класичним підходом LSB. Крім того, стеганографічний алгоритм оцінюється візуально шляхом порівняння початкового аудіофайлу та стегофайлу з прихованим повідомленням. Результати аналізу вказують на відсутність слідів стеганографії. На основі отриманих результатів можна стверджувати про надійність та ефективність використання запропонованого підходу, тому використання LSB-AES техніки може бути запропоновано для забезпечення безпечної передачі даних.

Ключові слова: *стеганографія; шифрування; Least Significant Bit; алгоритм AES-CBC; NIST-тести.*

1. ВСТУП

Для забезпечення конфіденційності застосовують не лише методи криптографії, а й методи стеганографії. Хоча кожна із цих наук має свої сфери застосування, вони можуть поєднуватися для підвищення ефективності захисту інформації (наприклад, для передачі криптографічних ключів) або ж для формування надійної безпечної системи зв'язку [1].

Стеганографія – наука приховування повідомлень, але не шляхом їхнього перетворення на щось нерозпізнаване, як це відбувається у криптографії, а шляхом того, щоб вони залишалися непоміченими [2]. Загалом, стеганографія може використовувати у вигляді контейнерів будь-що від таких цифрових носіїв інформації, як зображення, аудіо та відео, до мережних протоколів еталонної моделі OSI.

У цьому дослідженні увага приділяється лише стеганографії в аудіосередовищі. Застосування стеганографії в аудіо є складним, оскільки слухова система людини (HAS) чутливіша до невеликих змін у аудіоданих, ніж візуальна система людини (HVS) [3].

2. АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Деякі з досліджень, опублікованих в області аудіостеганографії, розглядають набір таких загальних підходів, як *Least Significant Bit (LSB), Echo Hiding, Spread Spectrum (SS), Phase Coding*, розглянутих у [4].

Схема приховування даних у відео- та аудіофайлах, запропонована в [5], використовує 4LSB та алгоритм фазового кодування для збереження якості відеофайлу навіть після вбудовування секретних даних. Застосування аудіостеганографії з текстом шифрування потокового шифру RC4 розроблено в [6]. Запропонований підхід [7] до аудіостеганографії використовував комбінацію обчислення коефіцієнта DCT і схеми шифрування AES для покращення безпеки модуля. У [15] запропоновано метод заокруглення значень елементів зображення для модифікації найменшого біта у задачах стеганографічного захисту.

Розроблені стеганографічні методи можна застосовувати як для прихованого зберігання інформації, так і для захисту авторських прав на різноманітні об'єкти інтелектуальної власності шляхом укладення цифрових ідентифікаційних міток і "водяних знаків".

Більшість програмних рішень, де в ролі контейнера використовується звуковий сигнал, пропонує для вбудовування інформації тільки метод LSB, що можна спробувати пояснити складністю реалізації альтернативних методів. Запропонований у цій статті підхід реалізовано комбінацією двох – стеганографічної та криптографічної – технік.

3. МЕТА РОБОТИ

Метою цієї роботи є покращення алгоритму LSB для приховування текстової інформації у звукових файлах шляхом додаткового використання криптографічного методу та псевдовипадкових чисел для створення стійкого криптоключа, а також оцінювання, як удосконалення підходу впливає на основні критерії стеганографічної системи.

4. ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

У розробленій програмній реалізації вдосконалено один із базових методів стеганографії – техніку Least Significant Bits. Класична інтерпретація методу заміни найменш значущого біта можлива шляхом заміни останніх значущих бітів у контейнері на біти приховуваного повідомлення. Нижче наведено загальні основні кроки техніки LSB [8]: байти аудіофайлу перетворюються на бітову послідовність; усі символи повідомлення перетворюються на еквівалентну двійкову систему; найменш значущий біт аудіо замінюються на біт повідомлення.

Для вдосконалення стеганографічної техніки впроваджено додатковий криптографічний захист у вигляді алгоритму AES-CBC, за яким секретне повідомлення перед убудуванням шифрується на основі криптоключа-пароля.

Алгоритм AES реалізовано в режимі роботи CBC (Cipher Block Chaining), що дозволяє шифрувати повідомлення більшої довжини шляхом сегментування інформації блоками фіксованої довжини і застосуванням до першого сегменту операції XOR із випадковим значенням вектора ініціалізації. Указаний вектор ініціалізації може бути рівним нулю, що не є нерекомендованим з погляду алгоритму. Результат цієї операції зашифрований за допомогою ключа, і, таким чином, маємо новий зашифрований блок. Далі до наступного блоку повідомлення застосовується XOR разом з отриманим на попередньому кроці зашифрованим текстом, що також шифрується для наступних блоків.

Як варіант, значення вектора ініціалізації можна було зробити програмно фіксованим, проте в цьому програмному рішенні його значення генерується під час кожної спроби та використовується для отримання прихованого повідомлення з аудіофайлу в подальшому.

Таким чином, відповідно до рис. 1, на вхід програми подається аудіофайл-контейнер, повідомлення та криптоключ. Вхідний аудіофайл та зашифроване криптографічним алгоритмом повідомлення програмно конвертуються до бінарного представлення. Потім за стеганографічним алгоритмом біти повідомлення замінюють визначені біти вхідного аудіофайлу, що формують вихідний аудіофайл з убудуванням.

Враховуючи, що кожен семпл аудіофайлу містить 1 біт повідомлення, послідовність після вкладення не буде відрізнятися від вихідної за умови, що найменш значущий біт вихідної послідовності збігається з вкладеним бітом інформації. Інакше, значення останнього біта буде з імовірністю 50 % збільшено, або зменшено, на 1.

Процес знаходження прихованого повідомлення, що схематично зображено на рис. 2, є зворотним. Користувачу потрібно знати пароль, вектор ініціалізації (IV). З використанням правильного пароля та значення IV біти повідомлення буде відновлено, розшифровано і перетворено на текстову форму.

Щодо пароля, то він формується на вибір: задається користувачем або, за бажанням, генерується, з використанням псевдовипадкових чисел. Для отримання псевдовипадкового числа поєднано два генератори:

• mersenne twister – "Вихрь Мерсенна", а точніше mt19937, заснований на властивості простих чисел;

• std::random_device – рівномірно розподілений генератор випадкових чисел, для генерації істинно випадкових чисел, що виробляє недетермінований випадкове число.

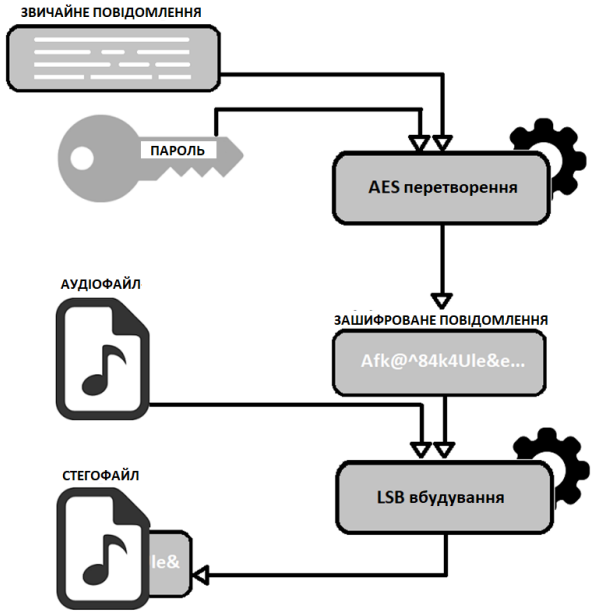

Рис. 1. Схема процесу приховування повідомлення за алгоритмом LSB-AES

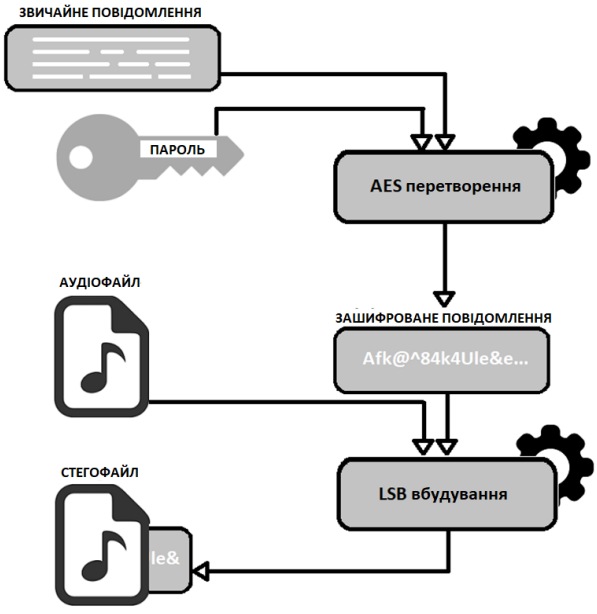

Рис. 2. Схема процесу витягування повідомлення за алгоритмом LSB-AES

У програмі для формування псевдовипадкових послідовностей один ГПВЧ ініціалізується результатом дії іншого ГВЧ (рис. 3), потім згенероване число використовується для генерації пароля.

Згенероване число безпосередньо застосовується для генерації пароля у разі вибору із 6 масивів цифр, англійських літер верхнього та нижнього регістрів, деяких знаків пунктуації чи спеціальних символів із повторенням операції до досягнення обраної довжини пароля.

```
std::random_device rd{};
std::mt19937 mersenne(rd());
```

Рис. 3. Ініціалізація генераторів

Загальний інтерфейс програми, яка була представлена в [14], зображено на рис. 4, 5.

5. ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ

У процесі застосування стеганографії важливими є такі характеристики [9]: пропускна здатність (capacity) – характеризує об'єм секретних даних відносно розміру файлу, в який можна вбудувати контейнер за допомогою визначеного методу; стійкість (robustness) – свідчить про стійкість стегофайлів до навмисних і ненавмисних атак; невидимість (invisibility) – описує схожість заповненого контейнера та пустого, являє собою рівень деградації контейнерів після приховування секретного повідомлення. Дотримання балансу всіх характеристик є важливим та дещо складним для реалізації. Загалом LSB є дуже простим методом і має перевагу у критерії невидимості, але цей метод стає слабким і передбачуваним, якщо виконувати його традиційно.

Пропускну спроможність стегоканалу можна знайти, використавши формулу

$$size = \frac{F}{BPS} - 132, \qquad (1)$$

де F – розмір файлу-контейнера, BPS – кількість байт на семпл (ця програма розрахована на BPS, яке дорівнює 16 байт).

Оскільки відбувається просто заміна молодшого біта, логічним є твердження, що додавання криптографічної складової до методу ніяк не впливає на пропускну здатність створюваного системою захищеного каналу зв'язку, яка може бути збільшена лише у випадках підвищення ступеня заповнення контейнера.

Розроблений стеганографічний інструмент побудовано таким чином, що він не змінює властивості аудіофайлів задля вбудування бітів повідомлення, не залишає жодних підозрілих підписів. Тому у разі аналізу стегофайлу таким способом не можна виявити наявність прихованих повідомлень, і тим більше, ідентифікувати використання саме цієї утиліти, що і є перевагою.

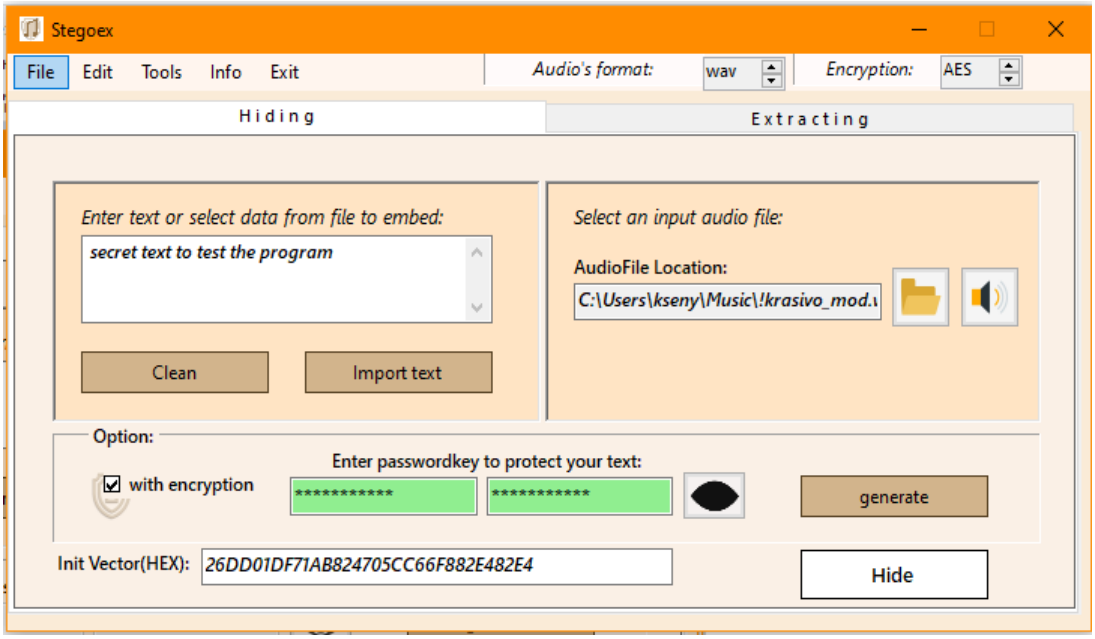

Рис. 4. Загальний інтерфейс прикладної програми. Модуль приховування з прикладом заповнення даних

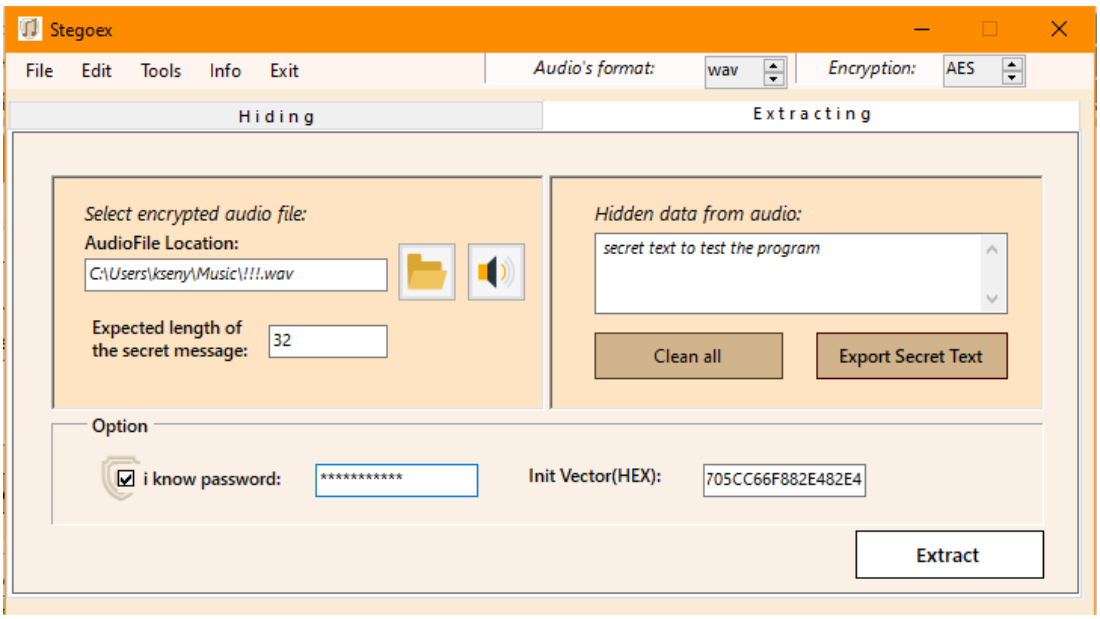

Рис. 5. Загальний інтерфейс прикладної програми. Модуль витягнення з прикладом заповнення даних

Як відомо, молодші розряди містять дуже мало корисної інформації. Їхнє заповнення додатковою інформацією практично не впливає на якість сприйняття. Тому загалом різниця між порожнім і заповненим контейнерами повинна бути не відчутна для органів сприйняття людини. Якість сигналу збільшується зі збільшенням розміру сигналу, оскільки пропорція відношення бітів сигналу до кількості бітів повідомлення збільшується, таким чином, спотворення зменшується.

Спотворення, що вносяться методом заміни найменш значущого біта в реальному звуковому сигналі, можна візуально виявити шляхом аналізу спектра сигналу. Перевірка чутності спотворень (іншими словами, можливості виявлення вкладень) проводиться візуально за допомогою звукового редактора Audacity 1.3 (рис. 6). На основі порівняння осцилограм можна стверджувати про відсутність прихованих повідомлень.

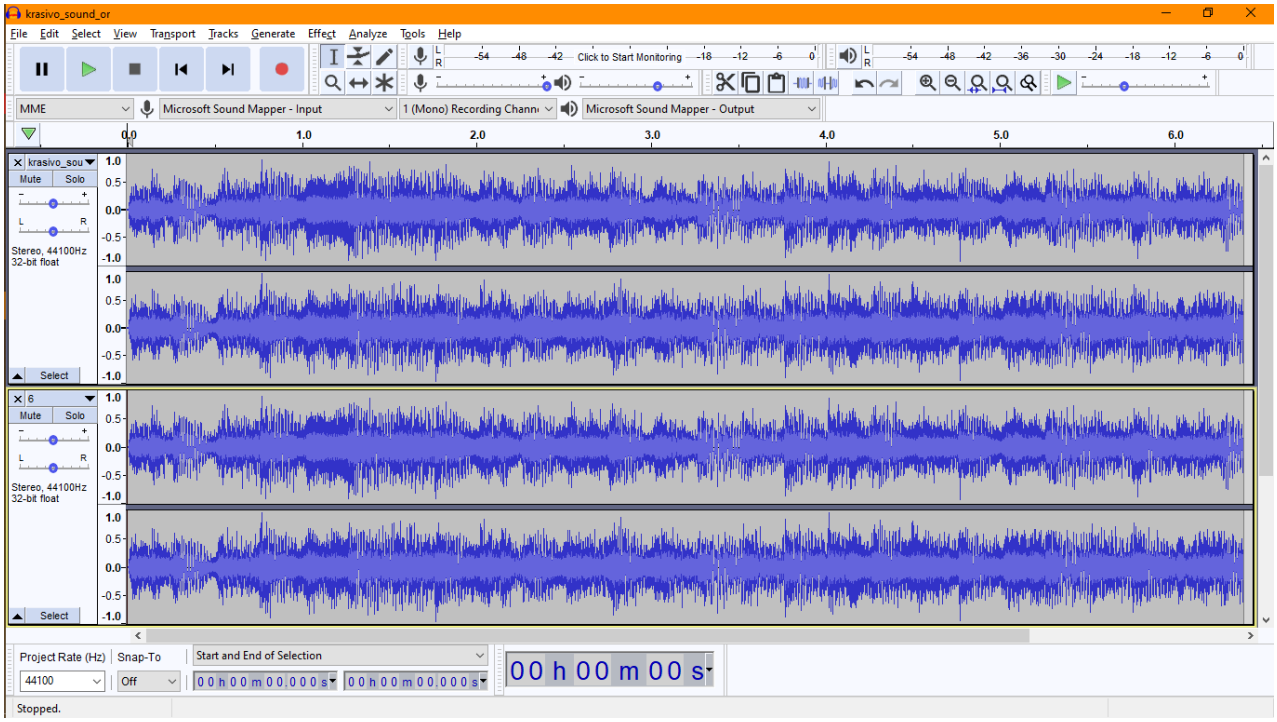

Рис. 6. Осцилограма "пустого" аудіофайлу (зверху) з прихованим повідомленням (знизу)

Основна ідея – використання методу з криптографією замість звичайного в покращенні статистичних властивостей об'єкта, таким чином, цей метод вкладення стає стійкішим, зокрема і до статистичних методів стегоаналізу. Ще більшої стійкості надає використання саме алгоритму AES, що також передбачає вектор ініціалізації, який використовується із секретним ключем аби уникнути повторів у процесі шифрування даних, що робить неможливим для хакерів, що використовують атаку за словником, розшифрувати за-шифроване повідомлення шляхом виявлення шаблона.

Відомо, що існують різні стегоаналітичні методи, у тому числі такі, що засновані на дослідженні статистичних властивостей видобутих повідомлень [10, 11]. Тому для оцінювання стійкості досліджуваного методу вбудовуване повідомлення піддається тестуванню на псевдовипадковість за допомогою так званих NIST-тестів [12], на основі яких розроблене готове рішення [13] використовується в роботі. Ці тести зосереджено на різних типах невипадковості, які можуть існувати в послідовності і їхньою ціллю є визначення міри випадковості отриманих двійкових послідовностей.

Було проведено тестування на псевдовипадковість криптографічно перетвореного повідомлення (рис. 7) та звичайного (рис. 8) завдовжки 40 кб. На основі отриманих результатів можна стверджувати про відсутність стеганографічних вкладень у вбудуванні зашифрованого повідомлення, оскільки кількість успішно пройдених тестів становить більшість, а точніше – 86,67 %, чого не можна сказати про результат тестування для звичайного повідомлення, де цей показник становить лише 20 %.

6. РЕЗУЛЬТАТИ

Варто розуміти, що використання поширених стеганографічних методів знижує ентропію бітів аудіофайлу, що може бути причиною тверджень щодо присутності секретних убудувань. Убудування секретного повідомлення, зашифрованого AES-CBC у аудіосигналі за допомогою методу LSB дозволяє усунути будь-які шаблони, що можуть бути створені у процесі застосування стеганалітичних методів. Попереднє шифрування прихованого повідомлення робить виявлення складнішим, оскільки зашифровані дані зазвичай мають більший ступінь випадковості. Відновлення прихованого повідомлення додає ще один рівень складності порівняно зі звичайним виявленням наявності прихованого повідомлення.

Результати проходження NIST-тестів показують перевагу застосування представленого підходу. Порівнюючи осцилограми, можна помітити візуальну відсутність відмінностей між гістограмами вихідного та стегосигналу.

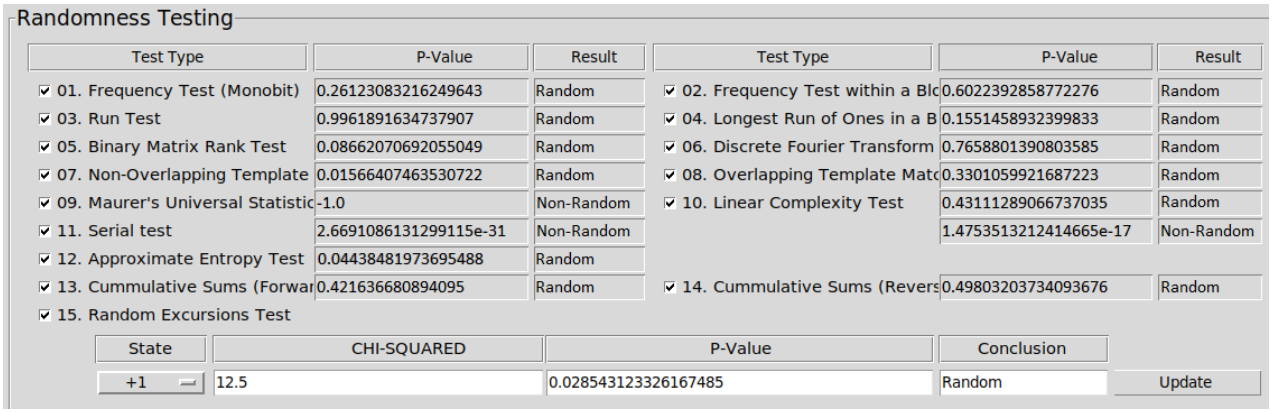

Рис. 7. Результати тестування зашифрованого повідомлення (86,67 % пройдено успішно)

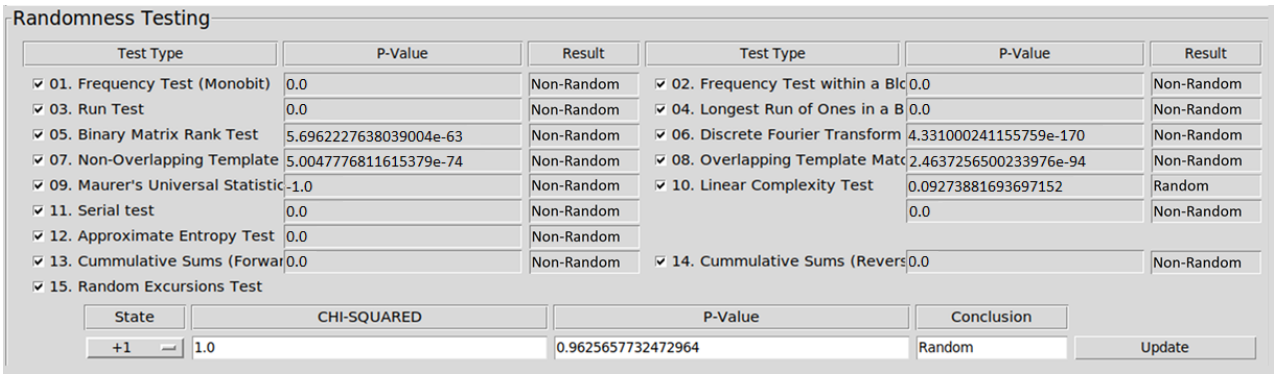

Рис. 8. Результати тестування звичайного повідомлення (лише 20 % пройдено успішно)

7. ВИСНОВКИ

У силу своєї простоти і прозорості реалізації метод LSB широко застосовують у стеганографії. Проте головним недоліком є надійність, яка може бути покращена з використанням надійного криптографічного алгоритму AES для захисту повідомлення. На основі покращеного стеганографічного алгоритму шляхом додаткового використання криптографічного методу розроблено та реалізовано стеганографічну утиліту для приховування текстової інформації у звукових файлах. Зокрема, використання елементів криптографії покращує статистичні властивості, таким чином, цей метод вкладення стає стійкішим до статистичних методів стегоаналізу, як показують результати NIST-тестів. Результати візуального аналізу вказують на відсутність слідів стеганографії. Тому запропонована вдосконалена техніка приховування зашифрованих даних у аудіосигналах характеризується кращою надійністю, що уможливлює її використання для забезпечення безпечної передачі даних між відправником та одержувачем у незахищених мережах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Hazra, T. K., Samanta, R., Mukherjee, N., & Chakraborty, A. K. (2017). Hybrid image encryption and steganography using SCAN pattern for secure communication. *In 8th Annual Industrial Automation and Electromechanical Engineering Conference (IEMECON)*, pp. 370–380. Bangkok.

[2] Katzenbeisser, S., Petitcolas, F. A. P. (2000). Information Hiding Techniques for Steganography and Digital Watermarking (pp. 121–148). Artech.

[3] Basu, P. N., & Bhowmik, T. (2010). On embedding of text in audio-a case of steganography. In Proceedings. *Of International Conference on Recent Trends in Information, Telecommunication and Computing*, pp. 203–206.

[4] Navneet, K., & Sunny, B. (2014, May). A Survey on various types of Steganography and Analysis of Hiding Techniques. *International Journal of Engineering Trends and Technology*, *IJETT*, VII(8), 388–392.

[5] Bhagat, V. B., Kulurkar, P. N. (2015). Audio And Video Steganography. *Using Lsb And Phase Encoding Algorithm*, *IJPRET*, vol. 3, no. 9, 1640–1648.

[6] Jian, C. T., Wen, C. C., Binti Ab Rahman, N. H. & Hamid, I. R. B. A. (2017). Audio Steganography with Embedded Text. *IOP Conf.*, vol. 226, no. 1, pp. 1–10.

[7] Bandi, S., & Manjunatha Reddy, H. S. (2019). Combined audio steganography and AES encryption to hide the text and image into audio using DCT. *Int. J. Recent Technol. Eng.*, vol. 8, no. 3, 1732–1738.

[8] Pooyan, M., & Delforouzi, A. (2007, Dec.). LSB-based Audio Steganography Method Based on Lifting Wavelet Transform. *ISSPIT'07*. Egypt.

[9] Al-Ani, Z. K., Zaidan, A. A., Zaidan, B. B., Alanazi, & Overview, H. O. (2010). Main fundamentals for steganography. *J. Comp*, 2(3), 158–165.

[10] Korzhik, V., Fedyanin, I., Godlewski, A., & Morales-Luna, G. (2017). Steganalysis Based on Statistical Properties of the Encrypted Messages. Computer Network Security. MMM-ACNS 2017. *Lecture Notes in Computer Science*, vol. 10446, Springer, Cham. https://doi.org/10.1007/978-3-/319-65127-9_23.

[11] Akhrameeva, K., Korzhik, V., & Nguyen, C. (2020). Detection of Video Steganography with the Use of Universal Method Based on NIST-Tests. *Proc. of Telecom. Universities*, 6(1). 72–78.

[12] National Institute of Standards and Technology (2010), p. 131. (02.01.2023) https://www.nist.gov/publications/statistical-/test-suite-random-and-pseudorandom-numbergenerator-cryptographic.

[13] Python implementation of NIST's A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. (02.01.2023) https://github.com/stevenang/ randomness_testsuite

[14] Бучик, С. С., & Хоменко, О. В. (2021, 30 вер.). Прикладна програма приховування текстової інформації в аудіофайлах. *Прикладні системи та технології в інформаційному суспільстві: V Міжнар. наук.-практ. конф.,* К., pp. 27–32.

[15] Buchyk, S., Tolyupa, S. Symonychenko, Y., Symonychenko, A., & Platonenko, A. (2021, January 28). Improvement of Steganographic Methods based on the Analysis of Image Color Models. *Cybersecurity Providing in Information and Telecommunication Systems*, K., 2021, 11–124.

REFERENCES

[1] Hazra, T. K., Samanta, R., Mukherjee, N., & Chakraborty, A. K. (2017). Hybrid image encryption and steganography using SCAN pattern for secure communication. *In 8th Annual Industrial Automation and Electromechanical Engineering Conference (IEMECON)*, pp. 370–380. Bangkok.

[2] Katzenbeisser, S., Petitcolas, F. A. P. (2000). Information Hiding Techniques for Steganography and Digital Watermarking (pp. 121–148). Artech.

[3] Basu, P. N., & Bhowmik, T. (2010). On embedding of text in audio-a case of steganography. In Proceedings. *Of International Conference on Recent Trends in Information, Telecommunication and Computing*, pp. 203–206.

[4] Navneet, K., & Sunny, B. (2014, May). A Survey on various types of Steganography and Analysis of Hiding Techniques. *International Journal of Engineering Trends and Technology, IJETT*, VII(8), 388–392.

[5] Bhagat, V. B., Kulurkar, P. N. (2015). Audio And Video Steganography. *Using Lsb And Phase Encoding Algorithm, IJPRET*, vol. 3, no. 9, 1640–1648.

[6] Jian, C. T., Wen, C. C., Binti Ab Rahman, N. H. & Hamid, I. R. B. A. (2017). Audio Steganography with Embedded Text. *IOP Conf.*, vol. 226, no. 1, pp. 1–10.

[7] Bandi, S., & Manjunatha Reddy, H. S. (2019). Combined audio steganography and AES encryption to hide the text and image into audio using DCT. *Int. J. Recent Technol. Eng.*, vol. 8, no. 3, 1732–1738.

[8] Pooyan, M., & Delforouzi, A. (2007, Dec.). LSB-based Audio Steganography Method Based on Lifting Wavelet Transform. *ISSPIT'07*. Egypt.

[9] Al-Ani, Z. K., Zaidan, A. A., Zaidan, B. B., Alanazi, & Overview, H. O. (2010). Main fundamentals for steganography. *J. Comp*, 2(3), 158–165.

[10] Korzhik, V., Fedyanin, I., Godlewski, A., & Morales-Luna, G. (2017). Steganalysis Based on Statistical Properties of the Encrypted Messages. Computer Network Security. MMM-ACNS 2017. *Lecture Notes in Computer Science*, vol. 10446, Springer, Cham. https://doi.org/10.1007/978-3-/319-65127-9_23.

[11] Akhrameeva, K., Korzhik, V., & Nguyen, C. (2020). Detection of Video Steganography with the Use of Universal Method Based on NIST-Tests. *Proc. of Telecom. Universities*, 6(1). 72–78.

[12] National Institute of Standards and Technology (2010), p. 131. (02.01.2023) https://www.nist.gov/publications/statistical-/test-suite-random-and-pseudorandom-numbergenerator-cryptographic.

[13] Python implementation of NIST's A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. (02.01.2023) https://github.com/stevenang/randomness_testsuite

[14] Buchyk, S. S., & Khomenko, O. V. (2021, September 30). Applied program for hiding text information in audio files, Applied systems and technologies in the information society: V International Scientific and Practical Conference. K., pp. 27–32 [in Ukrainian].

[15] Buchyk, S., Tolyupa, S. Symonychenko, Y., Symonychenko, A., & Platonenko, A. (2021, January 28). Improvement of Steganographic Methods based on the Analysis of Image Color Models. *Cybersecurity Providing in Information and Telecommunication Systems*, K., 2021, 11–124.

Стаття надійшла до редколегії 27.01.2023

Steganographic system for hiding text information in audio files

Audio file steganography can be used as an effective and efficient method to hide messages, but it is a complex process because the human auditory system is sensitive to small changes in audio data. In this article an improved approach for hiding secret text message in audio is presented, combining steganography and cryptography. The Least Significant Bits (LSB) technique, one of the most common and basic methods of steganography, is used as an algorithm for steganographic transformation. The described point of this method is to replace the least significant bits of the audio container with message bits that contain not very useful information, so filling them with additional information has little effect on the quality of perception. Such a significant disadvantage as the low level of reliability is improved by the introduction of a cryptographic layer, the feasibility of which is justified in the article. Cryptographic protection has been added in the form of one of the modern symmetric encryption algorithms – the AES algorithm in the CBC mode. Pseudo-random numbers are used to create a stable cryptokey. The cryptoalgorithm is used to protect the message, which after cryptographic conversion is hidden in the audio file using the steganographic LSB method. The main characteristics of the stegosystem are analyzed. In this paper, the application system of steganographic protection of information in audio files using a cryptographic algorithm is implemented using the environment of Microsoft Visual Studio 2019 and cryptographic libraries, the programming language is C ++. A WAV audio file was used as the digital container. NIST tests were used to assess resistance to stegoanalysis, which according to the results is better using an improved method compared to the classical LSB approach. In addition, the steganographic algorithm is evaluated by visual analysis by comparing the original audio file and the stegofile with the hidden message. The results of the analysis indicate the absence of traces of steganography. Based on the obtained results, it can be argued about the reliability and efficiency of the proposed approach, so the use of LSB-AES technique can be proposed to ensure secure data transmission.

Keywords: *cteganography; encryption; Least Significant Bit; AES-CBC algorithm; NIST tests.*

Сергій Бучик,
д-р техн. наук, проф.
Професор кафедри кібербезпеки та захисту інформації факультету інформаційних технологій Київського національного університету імені Тараса Шевченка. Київ, Україна.

Serhii Buchyk,
Dr. Sci. (Engin.), Prof.
Professor at the Department of Cyber Security and Information Protection, Faculty of Information Technologies Taras Shevchenko Kyiv National University. Kyiv, Ukraine.

Оксана Хоменко,
студентка Київського національного університету імені Тараса Шевченка. Київ, Україна.

Oksana Khomenko,
Student of Taras Shevchenko Kyiv National University. Kyiv, Ukraine.

Юрій Серпінський,
студент Київського національного університету імені Тараса Шевченка. Київ, Україна.

Yuriy Serpinsky,
Student of Taras Shevchenko Kyiv National University. Kyiv, Ukraine.