ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА ТЕОРІЯ КОДУВАННЯ

УДК 004.8 + 004.056

В. В. Лукічов, Ю. В. Баришев, Н. Р. Кондратенко, В. І. Маліновський

МЕТОД АДАПТИВНОГО БАГАТОШАРОВОГО ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ СТЕГАНОГРАФІЇ ТА КРИПТОГРАФІЇ

Вінницький національний технічний університет, м. Вінниця

Анотація. Наведено аналіз відомих розв'язків задачі поєднання стеганографічних та криптографічних методів для досягнення багатошарового захисту інформації. Результати аналізу дозволили виявити тенденції та перспективи розвитку цих методів. За результатами аналізу виконано постановку задачі дослідження щодо адаптації використовуваних криптографічних та стеганографічних методів для досягнення найкращого рівня захисту, який є необхідним в критичних системах. Визначено метрики на основі, яких можливо здійснювати вибір найкращого поєднання методів криптографічного та стеганографічного захисту. Представлено метод багатошарового захисту інформації, який поєднує в собі криптографічний та стеганографічний підходи для забезпечення підвищеного рівня захисту конфіденційності та цілісності інформації. Запропоновано ввести критерії вибору криптографічних перетворень таким чином, щоб їх поєднання разом зі стеганографічними давала найкращий ефект. Наведено приклад реалізації методу для доведення концепції. Розроблено алгоритм, що реалізує запропонований метод адаптивного багатошарового захисту інформації. Визначено перспективу подальших досліджень.

Ключові слова: стеганографія, криптографія, кібербезпека, критичні системи, метрики.

Abstract. An analysis of known solutions to the problem of steganographic and cryptographic methods combining to achieve multilayer information protection is presented. Results of the analysis allowed us to identify trends and prospects for the development of these kink of methods. Based on the results of the analysis, the research task was determined concerning the adaptation of the used cryptographic and steganographic methods in order to achieve the best level of protection, which is needed at critical systems. Metrics were defined, those allowed to choose the best combination of cryptographic and steganographic protection methods parameters. A method of multilayered information protection is presented, which combines cryptographic and steganographic approaches to ensure an increased level of information's confidentiality and integrity protection. It is proposed to introduce criteria for the selection of cryptographic transformations in such a way that their combination together with steganographic transformations gives the best impact. An instance of the proposed method implementation is given in order to prove the concept. An algorithm has been developed that implements the proposed method of adaptive multilayer information protection. The perspective of further research is determined.

Key words: steganography, cryptography, cyber security, critical systems, metrics.

DOI: https://doi.org/10.31649/1999-9941-2023-58-3-4-11.

Вступ

Захист інформації є актуальною проблемою в сучасному світі, де цифрові зображення широко використовуються в різних галузях, включаючи критичні системи такі, як медицина, банкінг, правоохоронну діяльність та багато інших. Завдяки методам стеганографії є можливість приховувати факт передавання інформації. Таким чином, конфіденційність даних захищається завдяки тому, що зловмисникам складно її виявити. Водночас криптографічні методи дозволяють приховати зміст даних. Поєднання цих підходів дозволяє побудувати багатошаровий захист даних. Так, спочатку зловмиснику потрібно виявити факт передавання даних, а потім розкрити їх зміст, шляхом розшифрування.

Актуальність

Підсилення захисту інформації, прихованої в зображення, застосуванням методів шифрування є природним. Більше того, завдяки властивості шифрування перетворювати вихідне повідомлення у шифротекст, статистичні властивості якого подібні до статистичних властивостей випадкових чисел, відрізнити видобуті внаслідок стегоаналізу дані від шумів становить складну задачу без знання використаного стеганографічного методу вбудовування даних. Таким чином такі методи можуть бути застосовані в задачах кібербезпеки критичних систем, де висуваються підвищені вимоги щодо захисту конфіденційності. Наразі відомі підходи до поєднання стеганографічних методів захисту з криптографічними. Однак попри те, що ці підходи передбачають використання різних контейнерів, різних алгоритмів вбудовування та різних криптографічних алгоритмів – вони залишаються поза увагою дослідження ступеня синергії цих складових. При цьому вибір певних алгоритмів може як покращувати показники якості захисту інформації, так їх й погіршувати. Внаслідок цього постає актуальна задача вимірювання та врахування явища синергії між ними та побудова методу захисту інформації на основі визначення найкращої комбінації.

Мета

Метою дослідження є покращення захисту конфіденційності даних при одночасному використання методів стеганографічного та криптографічного захисту за рахунок врахування явища синергії між ними.

Задачі

1. Проаналізувати відомі підходи одночасного використання методів стеганографії та криптографії для захисту конфіденційності даних.
2. Виконати постановку задачі розробки адаптивного багатошарового захисту інформації.
3. Розробити метод такого захисту як доведення концепції можливості такої розробки.

Аналіз відомих досліджень

Аналіз джерел показав широке поширення поєднання методів стеганографії та криптографії. Зокрема в роботі [1] запропоновано зашифрування секретних даних за допомогою блокового симетричного шифру AES в режимі роботи OFB, доєднання ключа шифрування до зашифрованих даних та вбудовування в зображення методом кластеризації найближчого центроїда. Основним недоліком такого підходу є зберігання ключа шифрування разом з даними, які зашифровані цим ключем з їх подальшим передаванням в одному контейнері. Таким чином, шифрування дозволило авторам покращити статистичні властивості відкритої інформації для ускладнення виконання криптоаналізу. Однак при цьому застосування криптографії не утворило ще один шар захисту, оскільки при успішному стегоаналізі розшифрувати дані не становитиме складності, оскільки зловмиснику буде доступним ключ шифрування.

В роботі [2] автори пропонують подвійне використання стеганографічного перетворення. Таким чином відкритий текст зашифровують, згодом вбудовують в один контейнер, якій вбудовують в інший контейнер. Автори розраховують, що внаслідок успішного стеганоаналізу зловмисником буде виявлено дані, які насправді є контейнером для приховування справжнього секрету. Відповідно зловмисник зупинить подальший аналіз, отримавши контейнер. На жаль, автори не зазначають використовувані криптографічні перетворення та спосіб розв’язання задачі ключового транспорту. Більше того вони пропонують використання методу LSB для вбудовування даних в зображення, який ефективний для окремих контейнерів як-то файли формату *.bmp, які не відповідають сучасним форматам, а тому привертають увагу потенційного зловмисника. Крім того, загальним недоліком робіт [1, 2] є забезпечення стійкості за рахунок концепції security by obscurity, який суперечить принципам Керкгоффса [3], прийнятих за найкращу практику сучасних методів захисту інформації.

Відомий підхід [4] який передбачає поєднання шифру AES-128, методу гешування SHA-256 та методу вбудовування LSB, використовуючи відеопотік HEVC (high-efficiency video coding) як контейнер. Для цього методу автори передбачають використання єдиного ключа, який зазнає процедуру розгортання на основі SHA-256 і використовує отримані геш-значення як ключ для шифрування та визначення місць вбудовування. Подібний підхід запропонований авторами [5], але вони використовують сталий ключ, шифр DES та аудіо-файли як контейнер. Недоліком цих методів є те, що при передаванні аудіо- та відеопотоків забезпечення сталої швидкості є важливішим за коректність передавання даних, відповідно повторного пересилання кадрів, що надійшли з помилками не відбувається, щоб не втрачати темп відображення користувачеві. Таким чином, існує ймовірність, що дані будуть пошкоджені під час передавання, а через зашифрування стане неможливим відновлення всіх прихованих даних, що слідують за пошкодженим кадром. Крім того, аудіо-файли та відео HEVC використовують методи ущільнення даних, а тому LSB не дозволяє досягти мінімуму спотворень відеопотоку при сталому обсязі даних для вбудовування.

Детальний аналіз відомих поєднань стеганографічних та криптографічних методів, наведений в роботі [6], відзначає відсутність оцінок стійкості результату такого поєднання. Крім того, автори [6] наголошують на недостатності аналізу відомих методів, оскільки у відомих роботах навіть у тих випадках, коли відбувається аналіз отриманих результатів, то він виконується методами стеганоаналізу, ігноруючи криптографічні складові запропонованих методів.

Підхід, запропонований в роботі [7], передбачає спочатку застосування методів стеганографії з подальшим шифруванням контейнеру. Завдяки застосуванню швидкого методу шифрування автори досягають високої швидкості перетворення, але, на жаль, запропонований метод шифрування не досліджувався щодо показників стійкості та будується на основі записування бітів двовимірного зображення в масив з трьома вимірами та накладанні масок. Як видно із зовнішнього вигляду зашифрованого зображення, наведеного авторами роботи [7], попри зашумленість, отриману внаслідок такого перетворення, все одно видно основні риси оригінального зображення, що свідчить про недостатню стійкість шифрування. Крім того, застосування шифрування до контейнера привертає увагу зловмисників до контейнерів.

В роботі [8] автори розглядають поєднання LSB з DES, Blowfish та дискретним косинусним перетворенням (як криптографічним перетворенням). Сильною стороною роботи [8] є використання MSE (Mean Square Error), SNR (signal-to-noise ratio) та PSNR (peak signal-to-noise ratio) як метрик для до-

слідження ефективності цих комбінацій. На жаль, використання застарілих методів шифрування Blowfish, який має слабкі ключі [9], та DES, вразливості якого були виявлені ще у 1991 році в роботі [10], подальший розвиток якої дозволив виявити низку ефективних атак [11]. Відповідно здобуті в роботі [8] результати не дозволяють забезпечити достатню стійкість криптографічного шару захисту, а тому стійкість забезпечується лише методами стеганографії.

Автори роботи [12] демонструють можливість багатошарового захисту для застосування в контейнерах на основі ланцюгів протеїнів. Для цього в [12] використовують специфічні методи шифрування та стеганографії, які враховують специфіку контейнеру. Зокрема запропонований підхід дозволяє генерувати ключ на основі аналізу молекул ДНК. Однак, попри перспективність застосування підходу в майбутньому, використання цього підходу для найбільш поширених інформаційних технологій наразі потребує додаткових ресурсів для придбання аналізаторів ланцюгів протеїнів та їх інтеграції до інформаційних систем.

Постановка задачі

Результати аналізу досліджень показали перспективність застосування багатошарового захисту. Проте загальним недоліком робіт відсутність метрик вимірювання синергії використовуваних алгоритмів захисту та контейнерів. При цьому дослідження, представлені у [8], показали, що різні комбінації криптографічних алгоритмів при фіксованому типові контейнера та стеганографічного методу дозволяють досягти різного ступеня ефективності з точки зору метрик MSE, SNR та PSNR. Таким чином випливає, що існує актуальна задача вибору найкращих параметрів використання стеганографічних та криптографічних моделей та методів при багатошаровому захисті інформації.

Метод адаптивного багатошарового захисту інформації

В межах цього дослідження обрано найбільш поширений шлях поєднання стеганографічних та криптографічних методів – шифрування кроків:

Крок 1: Вибір криптографічного алгоритму.

Для прикладу обрано стійкий та глибоко досліджений алгоритм шифрування як-то AES для захисту та покращення статистичних показників інформації в зображеннях.

Крок 2: Вибір стеганографічного алгоритму.

З метою демонстрації можливості реалізації методу обрано алгоритм стеганографії Convolutional Neural Networks (CNN).

Крок 3: Визначення параметрів адаптації.

Попри те, що стійкі шифри мають формувати шифротекст, який за статистичними показниками аналогічний послідовності випадкових чисел, варто врахувати, що вбудовуються зазвичай невеликі за обсягом дані. Відповідно статистичні показники коротких повідомлень не завжди матимуть бажані статистичні показники (аналогічні послідовності випадкових чисел). Для таких випадків необхідно визначити ті показники шифрування, які можуть бути замінені для вибору найкращого варіанту. Наприклад, для наведеного прикладу з шифром AES таким показником є режим роботи блокового шифру (як-то CBC, OFB, CTR тощо).

Крок 4: Застосування адаптивної криптографії

Для прикладу, що розглядається цей крок реалізується шляхом шифрування повідомлення за допомогою AES в режимі роботи, визначеному на кроці 3.

Крок 5: Вбудовування зашифрованої інформації в контейнер.

Відповідно до наведеного прикладу цей крок передбачатиме використання методу CNN.

Внаслідок адаптації використовуваного криптографічного методу захисту до потреб стеганографічного досягається покращення синергії між цими методами. Що дозволяє покращити показники якості вбудовування інформації в контейнер.

Для видобування інформації необхідно виконати обернений процес до зазначеного в методі: спочатку видобути з контейнера приховану інформацію, а згодом розшифрувати її. На рисунку 1 наведено алгоритм, що реалізує запропонований метод.

Для досягнення найкращих показників синергії пропонується використовувати комбінацію метрик SNR, PSNR та MSE. У випадку, коли показники якості, що відображаються цими метриками будуть суперечити одна одній, пропонується прийняття рішення за мажоритарним принципом.

Експериментальні дослідження застосування методу

Для доведення концепції розглянемо приклад застосування методу. Нехай секретним повідомленням є таке “The quick brown fox jumps over the lazy dog”, подане у кодуванні UTF-8. Як метод шифрування оберемо AES-128. Для того, щоб секретне повідомлення було зручніше обробляти його необхідно представити у вигляді рядка байтів, доповненого нулями до довжини блоку шифра. Як параметри адаптації оберемо ключі шифрування та режим роботи блокового шифру {key, modeOfOperations}. Було роз-

роблено програмний засіб мовою Dart на основі реалізації AES в бібліотеці з відкритим кодом Pointy Castle. На вхід розробленої програми надходили повідомлення та параметри адаптивного шифрування представлені в таблиці 1.

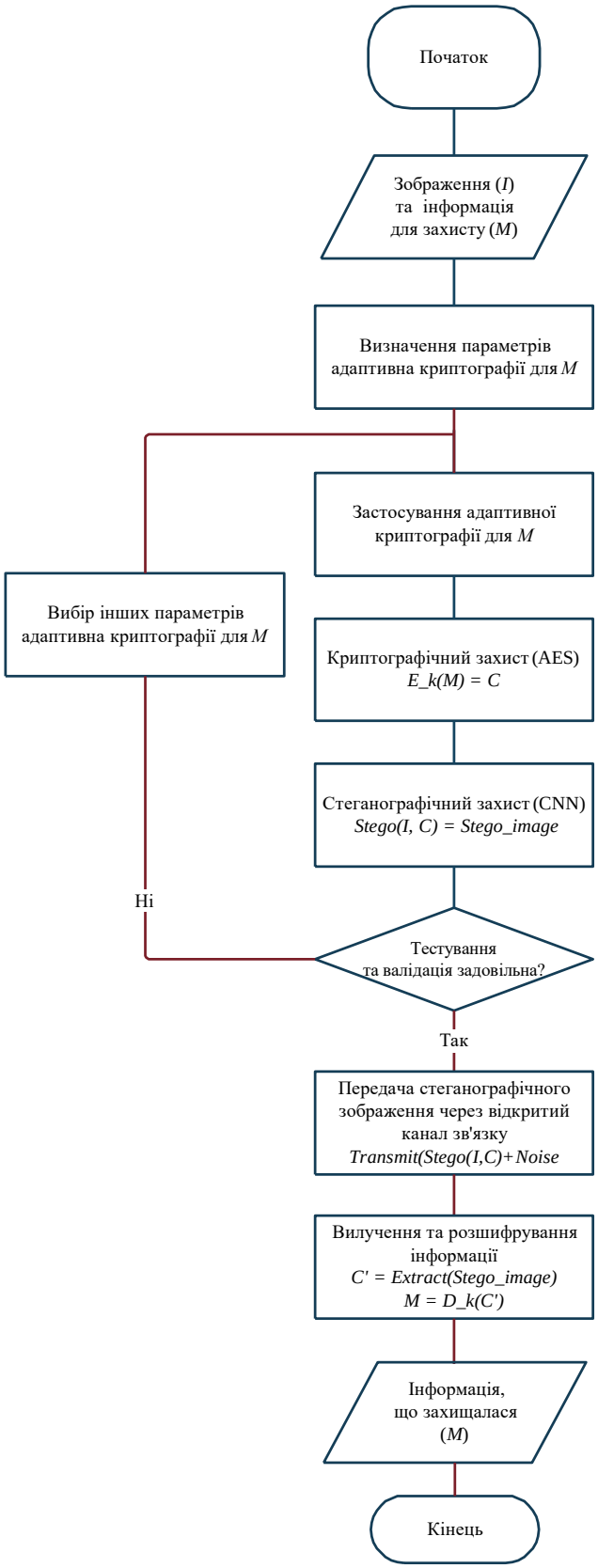

Рисунок 1 – Алгоритм багатошарової системи захисту інформації в зображеннях

Таблиця 1 – Параметри адаптивного шифрування

Назва параметрів	Значення параметрів
Повідомлення	0x717569636b2062726f776e20666f78206a756d7073206f76657220746865206c617a7920646f67000000000000000000
Ключ 1	0x0102030405060708090a0b0c0d0e0f
Ключ 2	0x0f0e0d0c0b0a09080706050403020 1
Режим шифрування 1	CBC
Режим шифрування 2	CTR

Внаслідок зашифрування отримано варіанти потенційних шифротекстів для стеганографічного вбудовування в контейнер, наведені в таблиці 2.

Таблиця 2 – Отримані варіанти шифротекстів

Використані параметри шифрування	Значення шифротексту
{Ключ 1, CBC}	0xad3c3e6b346855b3cc4f1a62d9709004396d608c6cf0b85cd460d6381ad9c6ca96a2c5118564c24a9add945510fcb94f
{Ключ 1, CTR}	0x733243f172c2feffa5d75cdb4835d4325880fb2ece35303f53b77ef9c848f06ab83881c1deba35b145bec1608d9415a6
{Ключ 2, CBC}	0xffab26ecb4f3aa6e9d3abf3aa85cc35c1f1b430f121bb03bd711743cc383758dfdcd86dd5545e6d9a97b7878ef948c58
{Ключ 2, CTR}	0xdd0869271f057b09f48cf74e9a6a1a2da497876bf79e2a4aacf5d30b07c978526585341d2715b429faf4332be7515474

Наступним кроком реалізації методу є вибір поміж отриманих шифротекстів того, який дозволить досягти найкращої синергії на основі значень метрик MSE, SNR та PSNR. Для дослідження синергії було використано три зображення як контейнери вбудовування інформації, наведені на рис. 2.

(A (B (C

Рисунок 2 – Контейнери для вбудовування шифротекстів

За результатами вбудовування було проведено визначення обраних метрик. Результати наведено в таблиці 3.

Вищий показник метрик PSNR і SNR означає, що якість стегозображення подібна до зображення вхідного. У випадку метрики MSE – нижче значення свідчить, що якість стегозображення подібна до

зображення оригінального контейнера. Таким чином, з таблиці 3 видно, що для різних контейнерів найкращими виборами будуть різні шифротексти, тобто від вибору конкретних значень параметрів криптографічного та стеганографічного захисту залежить стійкість остаточного результату. Так для зображень А та В найкращі показники забезпечує варіант {Ключ 2, CBC}, а для зображення С – {Ключ 1, CBC}. Отже, експеримент дозволив довести, що при поєднанні криптографічного та стеганографічного методів захисту за рахунок адаптації досягаються кращі показники якості приховування інформації порівняно з відомими методами, які обирають ці показники незалежно один від одного.

Таблиця 3 – Значення метрик MSE, SNR та PSNR

Використані параметри шифрування	Зображення А			Зображення В			Зображення С		
	MSE	SNR	PSNR	MSE	SNR	PSNR	MSE	SNR	PSNR
{Ключ 1, CBC}	0.000828	386686	78.9517	0.00036	785984	82.5655	**0.000936**	**25329494**	**78.4175**
{Ключ 1, CTR}	0.000844	379054	78.8651	0.000373	758679	82.4120	0.000958	24742144	78.3156
{Ключ 2, CBC}	**0.000803**	**398729**	**79.0849**	**0.00035**	**800386**	**82.6444**	0.000967	24528849	78.2787
{Ключ 2, CTR}	0.000822	389298	78.9809	0.000377	751223	82.3691	0.000966	24599537	78.2905

Висновки

В межах цього дослідження були розроблено метод багатошарового захисту цифрових зображень, що базується на комбінації криптографічних та стеганографічних підходів. На відміну від відомих підходів цей метод передбачає оптимізацію під час вибору використовуваних методів стеганографічного та криптографічного перетворень, а також контейнера. Проведений аналіз дозволив підтвердити актуальність подальших досліджень в цій галузі. На основі виконаного аналізу здійснена постановка задачі дослідження. Для доведення концепції можливості розв'язання поставленої задачі, запропоновано метод, реалізація кожного кроку якого була проілюстрована прикладами реалізації відповідних кроків. Розроблене програмне забезпечення дозволило поставити експеримент, який довів можливість покращення багатошарового захисту за умов адаптації їх параметрів.

Запропонований метод доцільно використовувати в системах, де висуваються підвищені вимоги до захисту конфіденційності даних таких, як критичні системи. Перспектива подальших досліджень в цьому напрямі передбачається в ідентифікації параметрів адаптації та застосуванні методів математичного моделювання для апроксимації задачі оптимального вибору, яка розв'язується на етапі адаптації параметрів криптографічних перетворень. Це пов'язано з дискретною природою вхідних даних. Зокрема у наведеному прикладі такими параметрами було обрано режим роботи блокового шифру.

Список літератури

[1] Shifa, A., Afgan, M. S., Asghar, M. N., Fleury, M., Memon, I., Abdullah, S., Rasheed, N. "Joint Crypto-Stego Scheme for Enhanced Image Protection With Nearest-Centroid Clustering" IEEE Access, vol. 6, 2018. pp. 16189-16206, 2018, doi: 10.1109/ACCESS.2018.2815037.

[2] Bandela, H. B., Babu, M. G., Venkata, D., Deepthi, V. "Crypto-Stego Technique for Secure Data Transmission." Journal of Physics: Conference Series. 1228, 012012, 2019. 11 p. doi:10.1088/1742-6596/1228/1/012012.

[3] Kerckhoffs, A. "La cryptographie militaire" Journal des sciences militaires IX: 5–38, 1883. pp. 161–191. http://www.petitcolas.net/fabien/kerckhoffs/

[4] Almomani, I., Alkhayer, A., El-Shafai, W. A. "Crypto-Steganography Approach for Hiding Ransomware within HEVC Streams in Android IoT Devices." Sensors, 22(6), 2281. 2022. https://doi.org/10.3390/s22062281

[5] Abikoye, O. C., Adewole, K. S., Oladipupo, A. J. "Efficient Data Hiding System using Cryptography and Steganography." International Journal of Applied Information Systems. Volume 4– No.11. 2012. pp. 6-11. doi: 10.5120/ijais12-450763.

[6] Jan, A., Parah, S.A., Hussan, M., Malik, B. A. "Double layer security using crypto-stego techniques: a comprehensive review." Health and Technology. 12, 2022. pp. 9–31. https://doi.org/10.1007/s12553-021-00602-1

[7] Rasras, R. J., AlQadi, Z. A., Sara, M. R. A. A "Methodology Based on Steganography and Cryptography to Protect Highly Secure Messages." Engineering, Technology & Applied Science Research, 9(1), 2019. pp. 3681–3684. https://doi.org/10.48084/etasr.2380
[8] Singhal, V., Singh, D., & Gupta S. K. "Crypto STEGO Techniques to Secure Data Storage Using DES, DCT, Blowfish and LSB Encryption Algorithms." Journal of Algebraic Statistics.Volume 13, No. 3, 2022. p. 1162-117. https://www.publishoa.com/index.php/journal/article/view/734/624
[9] Kara, O., Manap, C. "A New Class of Weak Keys for Blowfish. In: Biryukov, A. (eds) Fast Software Encryption." Lecture Notes in Computer Science, vol 4593. 2007. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-74619-5_11
[10] Biham, E., Shamir, A. "Differential cryptanalysis of DES-like cryptosystems." Journal of Cryptology 4, 1991. pp. 3–72. https://doi.org/10.1007/BF00630563
[11] Biham, E., Perle, S. "Conditional Linear Cryptanalysis - Cryptanalysis of DES with Less Than 242 Complexity" IACR Trans. Symmetric Cryptol., 2018, pp. 215-264.
[12] Mawla, N. A., Khafaji, H. K. "Enhancing Data Security: A Cutting-Edge Approach Utilizing Protein Chains in Cryptography and Steganography" Computers, 12(8), 166. 2023. https://doi.org/10.3390/computers12080166
[13] Pointy Castle. URL: https://github.com/bcgit/pc-dart

Стаття надійшла: 12.12.2023

References

[1] Shifa, A., Afgan, M. S., Asghar, M. N., Fleury, M., Memon, I., Abdullah, S., & Rasheed, N. (2018). Joint Crypto-Stego Scheme for Enhanced Image Protection With Nearest-Centroid Clustering, IEEE Access, vol. 6, pp. 16189-16206, 2018, doi: 10.1109/ACCESS.2018.2815037.
[2] Bandela, H. B., Babu, M. G., Venkata, D., Deepthi, V. (2019) Crypto-Stego Technique for Secure Data Transmission. Journal of Physics: Conference Series. 1228, 012012. 11 p. doi:10.1088/1742-6596/1228/1/012012.
[3] Kerckhoffs, A. (1883). La cryptographie militaire. Journal des sciences militaires IX: 5–38, 161–191. http://www.petitcolas.net/fabien/kerckhoffs/ [in French]
[4] Almomani, I.; Alkhayer, A.; El-Shafai, W. A. (2022). Crypto-Steganography Approach for Hiding Ransomware within HEVC Streams in Android IoT Devices. Sensors, 22(6), 2281. https://doi.org/10.3390/s22062281
[5] Abikoye, O. C., Adewole, K. S., Oladipupo, A. J. (2012). Efficient Data Hiding System using Cryptography and Steganography. International Journal of Applied Information Systems. Volume 4–No.11. pp. 6-11. doi: 10.5120/ijais12-450763.
[6] Jan, A., Parah, S.A., Hussan, M., & Malik, B. A. (2022). Double layer security using crypto-stego techniques: a comprehensive review. Health and Technology. 12, pp. 9–31. https://doi.org/10.1007/s12553-021-00602-1
[7] Rasras, R. J., AlQadi, Z. A., & Sara, M. R. A. (2019). A Methodology Based on Steganography and Cryptography to Protect Highly Secure Messages. Engineering, Technology & Applied Science Research, 9(1), pp. 3681–3684. https://doi.org/10.48084/etasr.2380
[8] Singhal, V., Singh, D., & Gupta S. K., (2022). Crypto STEGO Techniques to Secure Data Storage Using DES, DCT, Blowfish and LSB Encryption Algorithms. Journal of Algebraic Statistics.Volume 13, No. 3, p. 1162-117. https://www.publishoa.com/index.php/journal/article/view/734/624
[9] Kara, O., Manap, C. (2007). A New Class of Weak Keys for Blowfish. In: Biryukov, A. (eds) Fast Software Encryption. FSE 2007. Lecture Notes in Computer Science, vol 4593. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-74619-5_11
[10] Biham, E., Shamir, A. (1991) Differential cryptanalysis of DES-like cryptosystems. Journal of Cryptology 4, pp. 3–72. https://doi.org/10.1007/BF00630563
[11] Biham, E., & Perle, S. (2018). Conditional Linear Cryptanalysis - Cryptanalysis of DES with Less Than 242 Complexity. IACR Trans. Symmetric Cryptol., 2018, pp. 215-264.
[12] Mawla, N. A., Khafaji, H. K (2023). Enhancing Data Security: A Cutting-Edge Approach Utilizing Protein Chains in Cryptography and Steganography. Computers, 12(8), 166. https://doi.org/10.3390/computers12080166
[13] Pointy Castle. URL: https://github.com/bcgit/pc-dart

Відомості про авторів

Лукічов Віталій Володимирович – к. т. н., доцент кафедри захисту інформації Вінницького національного технічного університету, м. Вінниця.

Баришев Юрій Володимирович – к. т. н., доцент кафедри захисту інформації Вінницького національного технічного університету, м. Вінниця.

Кондратенко Наталія Романівна – к. т. н., професор кафедри захисту інформації Вінницького національного технічного університету, м. Вінниця.

Маліновський Вадим Ігорович – к. т. н., доцент кафедри захисту інформації Вінницького національного технічного університету, м. Вінниця.

V. Lukichov, Y. Baryshev, N. Kondratenko, V. Malinovskyi

METHOD OF THE ADAPTIVE MULTILAYER INFOR-?ATION PROTECTION ON THE BASIS OF STEGANOG - APHY AND CRYPTOGRAPHY

Vinnytsia National Technical University, Vinnytsia