DOI : 10.26565/2519-2310-2023-2-05
УДК 004.056.5

ДОСЛІДЖЕННЯ МОЖЛИВОСТЕЙ ЗАСТОСУВАННЯ СТЕГАНОГРАФІЧНИХ ТА КРИПТОГРАФІЧНИХ АЛГОРИТМІВ ДЛЯ ПРИХОВУВАННЯ ІНФОРМАЦІЇ

Микита Бодня[1], Марина Єсіна[1,2], Володимир Пономар[1,2]

[1]Харківський національний університет імені В. Н. Каразіна, майдан Свободи, 4, Харків, 61022, Україна
bodnia2020kb12@student.karazin.ua, m.v.yesina@karazin.ua ORCID: https://orcid.org/0000-0002-1252-7606
[2]АТ «ІІТ», вулиця Коломенська, 15, Харків, 61166, Україна
Laedaa@gmail.com ORCID: https://orcid.org/0000-0001-5271-2251

Надійшла до редакції 17 листопада 2023 р. Переглянута 18 грудня 2023 р. Прийнята 25 грудня 2023 р.

Анотація: Організація захисту інформації завжди було актуальною задачею особливо після появи інформаційно-комунікаційних систем. Базисними направленнями в області захисту інформації, які прийшли зі стародавніх часів є криптографія та стеганографія. Криптографія реалізує захист інформації шляхом перетворення інформації у нечитабельний вигляд. Стеганографія дозволяє приховати інформацію в різних контейнерах, при цьому факт наявності інформації залишається непоміченим для випадкових спостерігачів. У статті розглядаються підходи до криптографії та стеганографії, концепція гібридного застосування криптографічних та стеганографічних методів для забезпечення подвійного рівня захисту даних, загальна архітектура криптографічних та стеганографічних систем. Традиційними криптографічними системами, які застосовуються в сучасних системах захисту інформації є симетричні та асиметричні криптосистеми. Хоча симетричні системи еволюціонували з появою нових математичних перетворень, але вони мають суттєвий недолік. Він полягає в потребі додаткової передачі секретного ключа отримувачу. Така стратегія вимагає використання захищеного каналу зв'язку, оснащеного технічними системами захисту. При цьому існує ризик несанкціонованого доступу, який може спричинити компрометацію секретного ключа. Виходячи з вищенаведених проблем симетричних криптосистем, при розробці механізмів захисту, перевагу віддають асиметричним алгоритмам. Проведено аналіз криптосистеми RSA, яка ґрунтується на асиметричному підході шифрування. Ця система використовується в сучасних протоколах автентифікації та забезпечення конфіденційності в інформаційних системах та Інтернеті. Проведено дослідження швидкодії програмних модулів генерації ключової пари, шифрування та розшифрування для системи RSA, шляхом зміни загальних параметрів алгоритму (модуля перетворень, розміру вихідних даних). Результати часових вимірювань наведені в таблиці, на базі яких побудовані залежності часу від модифікації конкретних параметрів. Досліджено стеганографічний алгоритм модифікації найменш значущого біту (НЗБ), який застосовується для приховування даних в зображеннях. Нині існує широкий спектр стеганоалгоритмів, які розробляються на базі особливостей сенсорних систем людини (системи зору або слуху). Розглядаються властивості зорової системи людини, які використовуються в стеганографії.

Ключові слова: *криптографія, стеганографія, ключ, інформаційне повідомлення, асиметрична криптосистема, симетрична криптосистема, криптограма, стеганограма..*

1.Вступ

Інформація завжди займала провідне місце в житті людини. Поняття «інформація» [1] можна інтерпретувати як сукупність публічно оголошених або документованих відомостей, які охоплюють явища природи, навколишнього середовища та різноманітні області діяльності соціуму й держави. Вагомість і класифікація інформації визначається її вмістом. Поява інформаційно-комунікаційних систем і глобальних мереж спрощує доступність й обмін інформацією. Стрімкий технологічний прогрес призвів до появи загроз несанкціонованого доступу, порушення конфіденційності, цілісності інформації, фальсифікації даних тощо. Поряд з цим питання забезпечення інформаційної безпеки (ІБ) завжди було актуальним, починаючи зі стародавніх часів і до теперішнього моменту. Основними напрямами, що впроваджують надійні механізми забезпечення ІБ є криптографія і стеганографія [2].

Для розв’язання проблем ІБ широко використовуються відповідні алгоритми криптографії і стеганографії. Сучасні системи ІБ розробляються з реалізацією перспективних криптографічних і стеганографічних методів захисту. Система інформаційної безпеки (СІБ) [1]

призначена для забезпечення безпеки інформації, яка циркулює у інформаційно-телекомунікаційній системі (ІТС) від неавторизованих сторін. Сучасні СІБ оснащені відповідними апаратними модулями безпеки, котрі спрямовані на протидію фізичним загрозам. Ці модулі містять інтегровані мікропроцесори, що здатні виконувати потрібні математичні обчислення для реалізації відповідних криптографічних та стеганоалгоритмів.

Криптографія – наука про методи захисту інформації від несанкціонованого доступу чи модифікації. Метою криптографії є реалізація захисту інформації шляхом спеціального її перетворення (шифрування). Загальною ідеєю криптографії є конвертування вмісту даних в нерозбірливий вигляд. Повернення зашифрованого тексту у вихідний стан здійснюється за допомогою спеціального ключа, яким володіє лише власник інформації або довірена сторона. Зловмисник гіпотетично може перехопити шифртекст в момент передачі по каналу зв'язку (КЗ), але не матиме можливість ознайомитися зі вмістом вихідного повідомлення, оскільки у нього не має секретного ключа необхідного для виконання процедури дешифрування (криптоаналіз). Криптографія забезпечує конфіденційність, цілісність та автентичність інформації, використовуючи математичні методи та алгоритми.

Стеганографія – наука про методи і способи зберігання та передачі інформації де сам факт передачі чи зберігання корисної – прихованої інформації, залишається в таємниці. Приховування інформаційних даних здійснюється в так звані контейнери (*зображення, аудіо файли, файлові системи тощо*). При вбудовуванні прихованих даних, різні стеганографічні методи використовують різні властивості природних сенсорних систем людини (насамперед зорових та звукових).Для вбудовування корисних повідомлень в стеганографії використовуються надмірності, якими характеризуються контейнери– переносники даних. Ці надмірності можуть бути природними чи штучними, в залежності від структури контейнерів. Наприклад, у кластерних файлових системах надмірність реалізується штучно, використовуючи для цього характеристики і структуру файлової системи[3-4].

З розвитком систем, які володіють великими обчислювальними потужностями почався стрімкий розвиток комп'ютерної криптографії та стеганографії. Сучасні обчислювальні системи здатні оперативно обробляти та перетворювати великі масиви даних, що в свою чергу, спонукає створення нових стеганографічних методів, які ускладнюють процес детектування повідомлень, а криптографічні ключі генеруються таким чином, щоб виключити ймовірність їх вгадування. Таким чином, проявляється тенденція комплексування застосування криптографічних і стеганографічних методів захисту інформації задля підвищення загального рівня безпеки [5]. Симбіоз криптографії і стеганографії є критично необхідним при обміні чутливої інформації між абонентами сучасних ІТС на фоні постійного ускладнення спектру загроз безпеки та зростання можливостей апаратного оснащення [6].

Криптографічні методи широко використовуються для побудови систем автентифікації, шифрування даних для захисту конфіденційної інформації в мережах, підтвердження цілісності та автентичності даних. Криптографія застосовується в банківському секторі для забезпечення безпеки персональних даних клієнтів та інформації щодо банківських операцій. Поряд з цим, стеганографія використовується для захисту авторських прав, забезпечення безпеки конфіденційної інформації при її передачі через мережі, публікації анонімних матеріалів або звітів, проведення потайної комунікації в умовах, при яких неможливо застосувати класичні (*з різних причин*) криптографічні методи тощо.

Метою цієї статі є аналіз структурних схем стеганографічноїі криптографічної систем захисту інформації та дослідження можливостей застосування відразу обох векторів захисту у їх комбінації.

2. Структурна схема стеганографічної системи

Узагальнена структурна схема стеганографічної системи представлена на рис.1, де вона розглядається, як специфічна реалізація системи зв'язку [2].

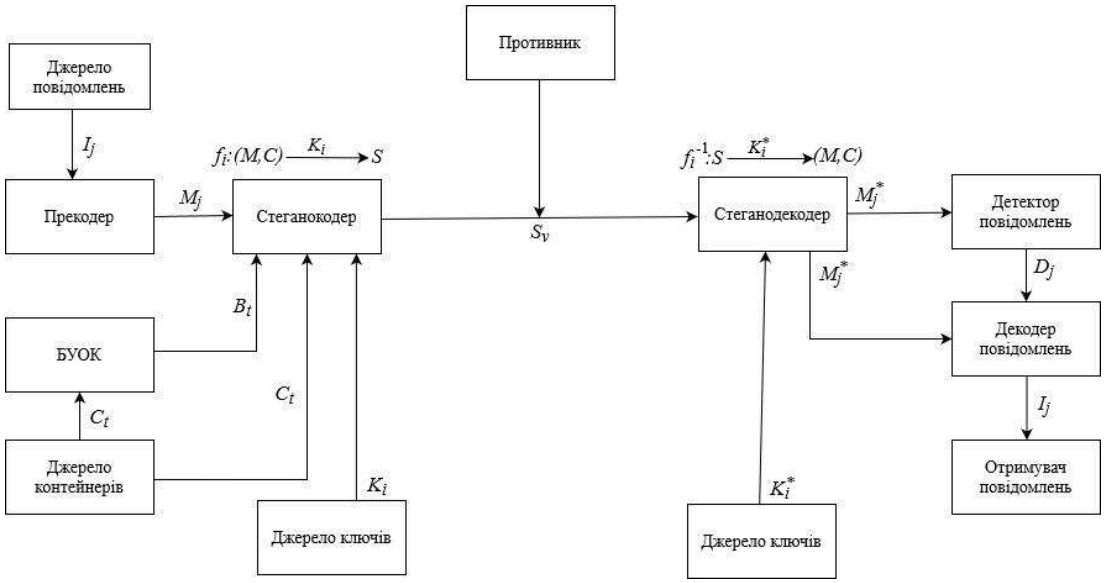

Рис. 1 –Узагальнена структурна схема стеганографічної системи
Fig. 1 - Generalized structural scheme of the steganographic system

В рамках даної схеми, джерело повідомлень генерує масив інформаційних повідомлень, яке представлено множиною $I=\{I_1,I_2,\ldots,I_n\}$. Повідомлення I_j є одним з повідомлень множини I, яке перетворюється прекодером. Результатом перетворення є сформоване повідомлення $M_j \in M$,де M_j –потайне інформаційне повідомлення, яке необхідно приховати в контейнері, $M=\{M_1,M_2,\ldots,M_n\}$ – множина можливих секретних повідомлень [2]. Процес генерації інформаційних повідомлень джерелом повідомлень можна уявити випадковим процесом. Розподіл ймовірностей випадкового процесу визначається сукупним розподілом ймовірностей випадкових величин в рамках даного процесу. Тоді можна представити випадковий процес у вигляді множини $P_M=\{P(M_1),P(M_2),\ldots,P(M_n)\}$,складові якої є ймовірностями випадкових величин випадкового процесу. Джерело контейнерів формує спектр пустих контейнерів, який представлений множиною $C=\{C_1,C_2,\ldots,C_l\}$. Результатом роботи джерела контейнерів є випадковий контейнер C_t, який входить до складу множини C. Саме функціонування пристрою генерування контейнерів може бути охарактеризоване, як випадковий процес. Оскільки поява будь-якого контейнера з множини C є випадковою, кожному елементу множини C може бути присвоєно відповідні ймовірності. Випадковий процес генерування контейнерів може бути описаний множиною ймовірностей $P_C=\{P(C_1),P(C_2),\ldots,P(C_l)\}$, елементи якої є розподілені ймовірності між випадковими величинами цього процесу. Після створення контейнера, блок урахування особливостей контейнера (БУОК), аналізує контейнер C_t для виділення особливостей, які будуть враховуватися при вбудовуванні приховуваного інформаційного повідомлення M_j. Контейнер $C_t \in C$, з визначеними БУОК властивостями B_t, поступає на стеганокодер, де здійснюються спеціальні операції з вбудовування (*або інкапсуляції*) стеганографічних даних (*контенту*). Резуль-

татом здійснення інкапсуляції секретних повідомлень до контейнерів є стеганограми (*тобто, заповнені контейнери)*, де $S=\{S_1,S_2,\ldots,S_m\}$– множина утворених стеганограм.

Тривіальне подання стеганографічного вбудовування інформації [7] можна подати у вигляді множини відображень $f:\{f_1,f_2,\ldots,f_k\}$, де $f_i:(M,C)\to S$, $i=1,2,\ldots,k$.В аналогії з виразом інкапсуляції контенту, можна відобразити процедуру вилучення інформаційних даних у вигляді множини обернених відображень $f^{-1}:\{f_1^{-1},f_2^{-1},\ldots,f_k^{-1}\}$, де $f_i^{-1}:S\to(M,C)$, $i=1,2,\ldots,k$. У відображенні $f_i\in f$ кожному елементу множини S ставиться у відповідність елемент множин «*M*» та«*C*».

У стеганосистемах для здійснення процесів вставки (інкапсуляції) та вилучення контенту використовуються відповідні секретні ключі. Такий підхід застосовується для підвищення стійкості до детектування повідомлень зловмисником, забезпечення стійкості стеганографічного алгоритму проти можливих атак та зниження ймовірності несанкціонованого вилучення повідомлення зловмисником. Ці ключі породжуються джерелом ключів, звідки вони надходять до стеганокодеру. Управління стеганокодером здійснюється за допомогою секретних ключів. Тож визначимо множину ключів $K=\{K_1,K_2,\ldots,K_k\}$ таким чином, що кожне відображення $f_i\in f$ задається секретним ключем K_i, де $i=1,2,\ldots,k$:

$$f_i:(M,C)\xrightarrow{K_i}S. \tag{1}$$

Кожному відображенню f_i відповідає метод вбудування інформаційного повідомлення $M_i\in M$ в контейнер $C_i\in C$ за допомогою секретного ключа K_i. Аналогічним чином визначимо множину секретних ключів $K^*=\{K_1^*,K_2^*,\ldots,K_k^*\}$ для обернених відображень $f_i^{-1}\in f^{-1}$, які позначають процедуру вилучення інформаційних даних з контейнеру:

$$f^{-1}{}_i:S\xrightarrow{K_i^*}(M,C). \tag{2}$$

Кожному оберненому відображенню $f_i^{-1}\in f^{-1}$ відповідає спосіб вилучення інформаційних даних з контейнера за допомогою секретного ключа K_i^*. Важливо підкреслити, що в основному в стеганографічних перетвореннях використовується один ключ $(K_i=K_i^*)$ для забезпечення узгодженості між процесами вбудовування та вилучення даних. Випадковий процес генерування секретних ключів можна подати у вигляді множини ймовірностей:

$$\begin{aligned} P_K&=\{P(K_1),P(K_2),\ldots,P(K_k)\},\\ P_{K^*}&=\{P(K_1^*),P(K_2^*),\ldots,P(K_k^*)\}. \end{aligned} \tag{3}$$

У (3) кожному ключу $K_i\in K=\{K_1,K_2,\ldots,K_k\}$ відповідає певна ймовірність $P(K_i)$, а ключу $K_i^*\in K^*=\{K_1^*,K_2^*,\ldots,K_k^*\}$ відповідає ймовірність $P(K_i^*)$. Кожному відображенню $f_i\in f$ відповідає секретний ключ K_i. Формування стеганограми (заповненого контейнера) здійснюється за допомогою відображення f_i, яке однозначно задається ключем K_i за повідомленням M_j та контейнером C_t з урахуванням особливостей даного контейнеру B_t. Сформована стеганограма задається наступним співвідношенням:

$$\begin{aligned} &S_v=f_i(K_i,M_j,C_t),\\ &j\in[1,2,\ldots,n],\ t\in[1,2,\ldots,l],\ i\in[1,2,\ldots,k],\ v\in[1,2,\ldots,m],\ m\ge n \end{aligned} \tag{4}$$

Створена стенограма S_v передається каналом зв'язку на приймальну сторону, під час передачі вона може бути перехоплена противником. Після отримання стеганограми отримувачем, стеганодекодер реалізує зворотне відображення $f_i^{-1} \in f^{-1}$ з множини стеганограм S до множин повідомлень «*M*» і порожніх контейнерів «*C*» під управлінням ключа K_i^*:

$$\left(M_j, C_t\right) = f_i^{-1}\left(K_i^*, S_v\right). \quad (5)$$

Слід підкреслити, що при передачі стеганограми через мережу під впливом завад або противника можливе спотворення заповненого контейнера. На приймальній стороні маємо поєднання стеганограми і результатів «впливу» на неї в процесі передачі по КЗ. Отриману комбінацію можна подати у вигляді $S_v + \partial$, де $\partial -$ величина, що визначає степінь спотворення стеганограми під випливом зовнішніх факторів. В результаті виконання процедури вилучення стеганодекодером, отримаємо певну оцінку можливого інформаційного повідомлення та порожньому контейнеру:

$$\left(M^*{}_j, C^*{}_t\right) = f_i^{-1}\left(K_i^*, S_v + \partial\right). \quad (6)$$

Для робастних стеганографічних систем[2] незначне спотворення стеганограми $\left(\partial \neq 0\right)$ не призведе до повного руйнування вбудованого повідомлення M_j, в ідеальному випадку оцінка повідомлення M_j^* співпадатиме з вихідним повідомленням M_j. Тому для робастних стеганосистем справедливе наступне співвідношення:

$$\left(M_j, C_t\right) = f_i^{-1}(K_i^*, S_v + \partial). \quad (7)$$

Крихкі стеганографічні системи [2,7]нестійкі до впливу на заповнений контейнер, тому будь-яке спотворення стеганограми $\left(\partial \neq 0\right)$ призводить до руйнування вбудованого повідомлення $\left(M_j^* \neq M_j\right)$, тобто для крихких систем виконується наступна нерівність:

$$\left(M_j, C_t\right) \neq f_i^{-1}(K_i^*, S_v + \partial). \quad (8)$$

На базі отриманої оцінки M_j^* спеціальна функція детектування «приймає рішення» про наявність чи відсутність прихованого повідомлення в переданому контейнері S_v. Завадостійкий декодер використовує рішення апарату детектування повідомленьD_j для винесення бінарного рішення (так/ні) про присутність чи відсутність невиправної помилки в отриманому повідомленні. Операція декодування здійснюється в декодері, де базисними функціями пристрою декодування є зіставлення вилученої оцінки з одним із можливих повідомлень M_jй перетворення їх у вихідний формат повідомленняI_j, що надається отримувачу.

3. Структурна схема криптографічної системи

Криптографічна система – комплекс взаємопов'язаних криптографічних алгоритмів, засобів захисту інформації, нормативної, експлуатаційної документації, необхідних для реалізації захищеності інформації, що зберігається, обробляється або передається [8]. Методологія криптографічного захисту інформації повинна забезпечувати високий (заданий) рівень захисту даних при передачі або зберіганні в інформаційному просторі. Узагальнену структурну схему криптографічної системи проілюстровано на рис. 2, де спектр повідомлень, представлено множиною *«M»*, яка формується джерелом повідомлень.

Інформаційне повідомлення M_i є одним з можливих повідомлень множини M. Кожному інформаційному повідомленню $M_i \in M = \{M_1, M_2, \ldots M_n\}$ відповідає певна ймовірність $P(M_i)$, оскільки кожне повідомлення є реалізацією випадкового процесу.

Розподіл ймовірностей випадкового процесу можна подати у вигляді множини ймовірностей $P(M)=\{P(M_1),P(M_2),\ldots,P(M_n)\}$.

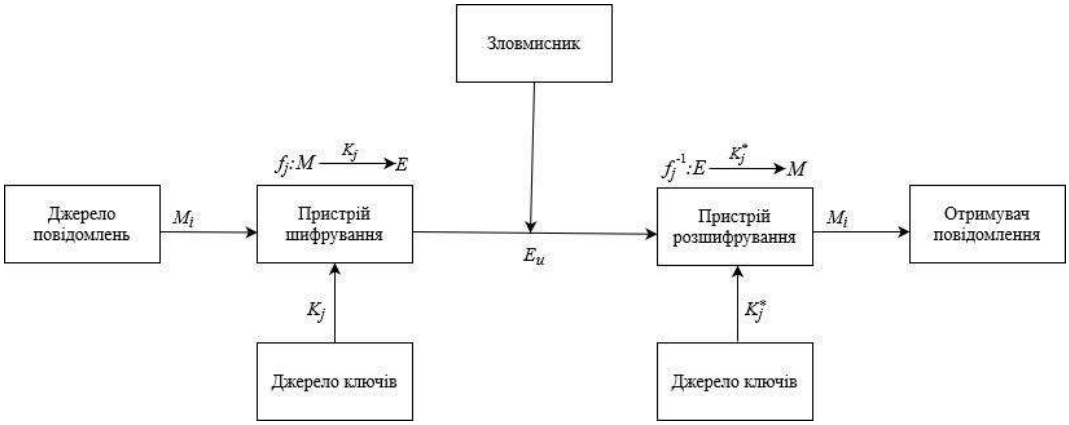

Рис. 2 –Узагальнена структурна схема криптографічної системи

Fig. 2–A generalized structural diagram of a cryptographic system

Множина $E=\{E_1,E_2,\ldots E_v\}$ позначає криптограми шифрованих повідомлень. Криптограма E_u представляє собою шифртекст вихідного повідомлення M_i. Процедуру шифрування здійснює пристрій шифрування, на вхід якого надходить повідомлення M_i. Процес шифрування можна представити у вигляді відображення $f_j \in f$ множини вихідних повідомлень M, у множину криптограм E. Оскільки відображення $f_j \in f$ сюр'єктивне та ін'єктивне (рис. 3), а множини M та E рівнопотужні, то існує обернене відображення $f_j^{-1} \in f^{-1}$, яке позначає процедуру розшифрування повідомлення [8].

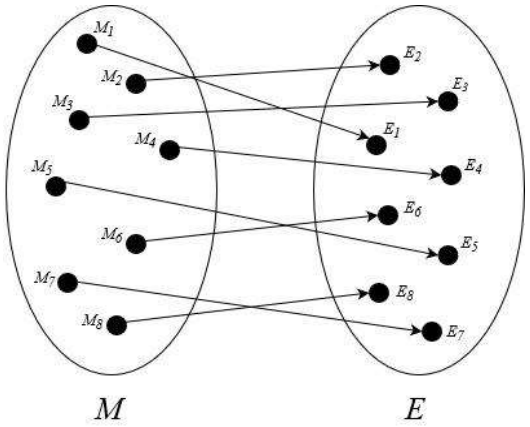

Рис. 3 –Сюр'єктивність та ін'єктивність відображення f_i

Fig. 3–Surjectivity and injectivity of reflection f_i

Джерело ключів створює потік ключів $K=\{K_1,K_2,\ldots,K_k\}$ чи $K^*=\{K_1^*,K_2^*,\ldots,K_k^*\}$, в загальному випадку $K_j \neq K_j^*$. При цьому, якщо $K_j = K_j^*$, то система симетрична, і навпаки, якщо $K_j \neq K_j^*$–асиметрична [8]. Оскільки породження ключів джерелом ключів є випадковим процесом, то кожному ключу $K_j \in K$ можна присвоїти певну ймовірність $P(K_j)$, а ключам $K_j^* \in K^*$ – ймовірність $P(K_j^*)$. Даний випадковий процес можна представити у вигляді розподілу ймовірностей $P(K)=\{P(K_1),P(K_2),\ldots,P(K_k)\}$ для ключів $K_j \in K$ і $P(K^*)=\{P(K_1^*),P(K_2^*),\ldots,P(K_k^*)\}$, та ключів

$K_j^* \in K^*$. Управління пристроєм шифрування здійснюється за допомогою ключа K_j, а пристроєм розшифрування – ключем K_j^*. Для всіх $j = 1,2,\ldots,k$ відображення $f_j \in f$ задається ключем K_j:

$$f_j : M \xrightarrow{K_j} E. \quad (9)$$

Кожне відображення $f_j \in f$ визначає спосіб шифрування повідомлення $M_i \in M$ ключем K_j (*рис. 4*). Відповідно, ключем K_j^* задається обернене відображення $f_j^{-1} \in f$, яке позначає спосіб розшифрування повідомлення за допомогою ключа K_j^* (*див. рис. 5*):

$$f_j^{-1} : E \xrightarrow{K_j^*} M. \quad (10)$$

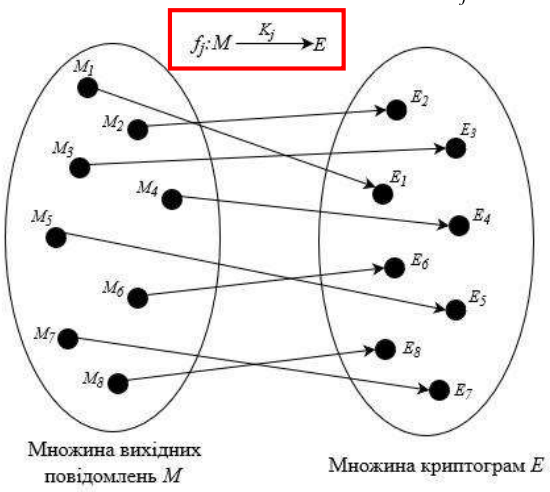

Рис. 4 –Відображення (9) множини вихідних повідомлень в множину криптограм

Fig. 4 - Mapping (9) of a set of output messages into a set of cryptograms

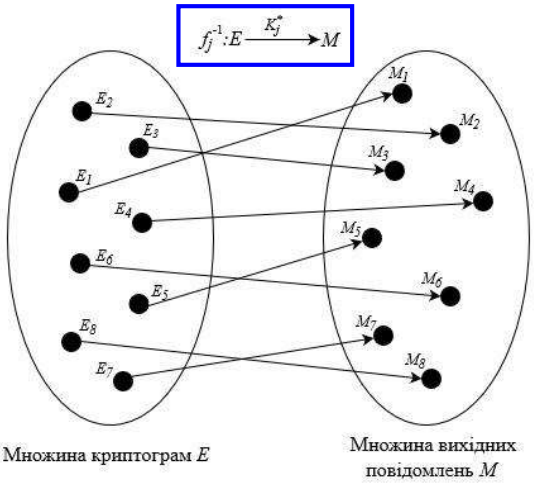

Рис. 5 –Обернене відображення (10) множини криптограм в множину вихідних повідомлень

Fig. 5 - Inverse mapping (10) of a set of cryptograms into a set/multiple of outgoing messages

Ключ K_j дозволяє зашифрувати один елемент з множини M, навпаки ключем K_j^* можливо отримати лише один елемент з криптограми E_u. Криптограма E_u формується за допомогою відображення $f_j \in f$, яка співвідноситься з ключем K_j за повідомленням M_i:

$$E_u = f_j(K_j, M_i). \quad (11)$$

Сформована криптограма E_u передається каналом зв'язку на приймаючу сторону. В момент передачі шифртекст E_u може бути перехоплений зловмисником. Пристрій розшифрування здійснює перетворення криптограми E_u у вихідне повідомлення M_i. Відновлення вихідного повідомлення здійснюється за допомогою оберненого відображення f_j^{-1}, яке пов'язане з ключем K_j^*:

$$M_i = f_j^{-1}(K_j^*, E_u). \quad (12)$$

Вилучене з криптограми повідомлення M_i надходить отримувачу.

4. Сутність традиційних криптосистем для реалізації захищеності інформації

Шифрування– це процедура направлена на забезпечення захисту інформації шляхом перетворення її у нечитабельний вигляд. Доступ до вмісту конфіденційних даних можливо отримати лише після виконання процедури розшифрування за допомогою секретного ключа.

Цим ключем володіє лише власник ключа чи довірена сторона. Секретні ключі повинні зберігатися в секреті, в захищеному середовищі, оскільки компрометація ключа призведе до несанкціонованого доступу до вмісту конфіденційних даних. Алгоритми шифрування використовують різноманітні математичні операції: - арифметику в полях Галуа $GF(q)$, математичні операції в групах точок еліптичних кривих, в групах простих чисел, модульну арифметику, перетворення Фур'є тощо. Управління процесами шифрування й розшифрування здійснюється за допомогою секретного ключа, тому криптосистеми класифікуються за способом використання ключів на дві групи: - симетричні і асиметричні. В асиметричних криптосистемах (рис. 6) генеруються 2 ключі: - відкритий та секретний. Відкритий ключ використовується для реалізації процедури шифрування, а секретний ключ застосовується для виконання розшифрування повідомлення. В симетричних криптосистемах (рис. 7) для процедур шифрування та розшифрування використовується лише один секретний ключ [9].

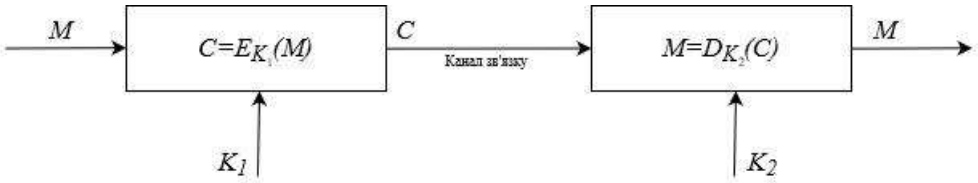

Рис. 6 – Спрощена модель асиметричної криптосистеми
Fig. 6 – A simplified model of an asymmetric cryptosystem

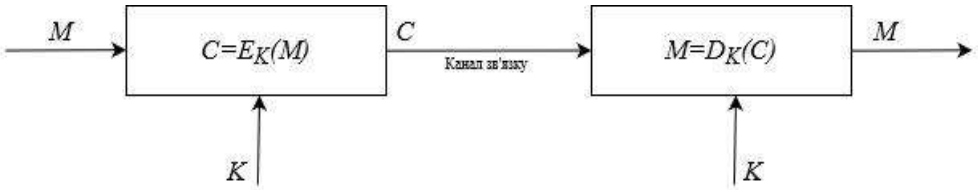

Рис. 7 – Спрощена модель симетричної криптосистеми
Fig. 7 – A simplified model of a symmetric cryptosystem

Сучасні криптографічні протоколи базуються на криптографії з відкритим ключем. В електронних комунікаціях для шифрування інформації використовуються *асиметричні* криптосистеми при передачі інформації по відкритих КЗ. В *симетричних* криптосистемах присутня проблема розподілу ключів [8], незалежно від структури криптографічного алгоритму. Перед початком сеансу обміну даними між двома сторонами, одна з них повинна згенерувати секретний ключ та передати іншої. При цьому для передачі ключа потрібно використовувати захищений КЗ, при цьому існує ризик компрометації секретного ключа, оскільки немає гарантії, що зловмисник не зможе обійти системи захисту. У табл.1 наведено спрощений опис характеристик симетричних та асиметричних криптосистем.

Розглянемо алгоритм RSA, який належить до криптографії з відкритим ключем. Шифр RSA, названий на честь його винахідників Ріверса (RonRivers), Шаміра (AdiShamir) і Адлемана (LeonardAdleman) [9-11]. Криптосистема RSA базується на застосуванні односторонньої функції [9] утворення добутку двох великих чисел, що є простішою задачею порівняно з розкладанням великого числа на прості множники [11]. Безпека криптосистеми RSA ґрунтується на факторизації великих чисел. Основною ідеєю алгоритму є генерування простих чисел для обчислення їх добутку, що визначає модуль n, який буде використовуватися в процедурах шифрування та розшифрування. Метою криптоаналізу в парадигмі RSA є знаходження секретного ключа d ключової пари (d,e), де e – відкритий ключ.

Таблиця 1 – Стислий опис класичних криптосистем

Table 1 – Brief description of classical cryptosystems

Тип системи	Характеристика
Асиметрична	*Для процедури шифрування і розшифрування використовуються 2 різні ключі. Асиметричні алгоритми потребують значно більше обчислювальних ресурсів порівняно із симетричними. Алгоритми асиметричної криптографії програють симетричним за швидкодією. Ключовою перевагою асиметричних криптосистем є використання ключів великої довжини (512 – 4096 біт), що позначається на швидкодії алгоритму. Асиметрична криптографія використовується у протоколах SSL (Secure Sockets Layer) та TSL (Transport Layer Security) для забезпечення безпеки обміну даними в мережі Інтернет.*
Симетрична	*Шифрування і розшифрування реалізується за допомогою 1 ключа, попередньо узгодженого між суб'єктами комунікації. Алгоритми симетричної криптографії за швидкодією перевершують асиметричні. Довжина ключа в симетричних системах помітно менша (40 – 256 біт). Область застосування симетричних криптосистем охоплює захист конфіденційної інформації фінансових установ, комерційних компаній та державних установ.*

Алгоритм RSA складається з трьох етапів:

1. Генерація ключової пари.
2. Шифрування інформаційного повідомлення M.
3. Розшифрування зашифрованого повідомлення C.

Генерація загальносистемних параметрів і ключів системи RSA має наступні кроки:

1. Обираються два простих числа p та q, які тримаються в секреті.
2. Обчислюється модуль n, що визначається співвідношенням $n = pq$.
3. Обчислюється функція Ейлера для модуля n, $\varphi(n) = (p-1)(q-1)$.
4. Вибирається таке значення відкритого ключа e, щоб воно було взаємно простим стосовно $\varphi(n)$, а саме $(\varphi(n), e) = 1$.
5. Визначається таке значення секретного ключа d, щоб $de \equiv 1 \bmod \varphi(n), \quad d < \varphi(n)$.

Результат:

1. Загальносистемні параметри p, q, n, $\varphi(n)$.
2. Секретний ключ $\{d, n\}$.
3. Відкритий ключ $\{e, n\}$.

Криптограма в системі RSA обчислюється за наступним правилом:

$$C \equiv M^e \bmod n. \tag{13}$$

Розшифрування зашифрованого повідомлення обчислюється за допомогою формули:

$$M \equiv C^d \bmod n. \tag{14}$$

У табл. 2 наведені результати продуктивності програмного модуля генерування ключової пари криптосистеми RSA, а рис. 8 відображає залежність часу генерування ключів від розміру модуля (*пакет моделювання MATLAB*).

Таблиця 2 – Результати генерування ключової пари для системи RSA

Table 2 – Key pair generation results for RSA system

№	Довжина модуля, біт	Час створення, секунди
1	*512*	*0,025*
2	*768*	*0,045*
3	*1024*	*0,141*
4	*2048*	*1,636*

У табл. 3 наведено результативність швидкодії виконання програмних модулів шифрування й розшифрування для криптографічної системи RSA в залежності від розміру файлу та довжини модуля перетворення.

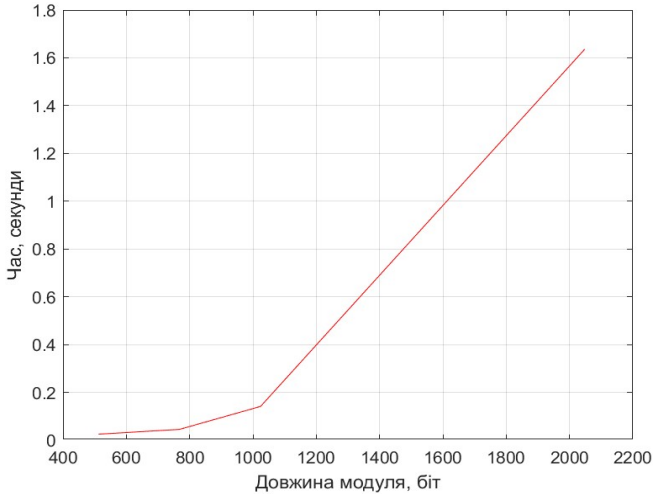

Рис. 8 – Залежність часу генерування ключової пари від розміру модуля
Fig. 8 – Dependence of key pair generation time on module size

Таблиця 3 – Оцінка швидкодії шифрування та розшифрування для системи RSA
Table 3 – Evaluation of encryption and decryption performance for the RSA system

Розмір файлу	Розмір модуля перетворення, біт	Час шифрування, секунди	Час розшифрування, секунди
219 КБ	*512*	*0,068*	*0,875*
	768	*0,089*	*1,520*
	1024	*0,127*	*2,347*
	2048	*0,184*	*7,988*
4,43 МБ	*512*	*1,391*	*18,151*
	768	*1,731*	*31,173*
	1024	*2,497*	*48,524*
	2048	*3,775*	*165,003*
8,65 МБ	*512*	*2,700*	*35,256*
	768	*3,401*	*61,187*
	1024	*4,889*	*94,335*
	2048	*7,388*	*325,451*

На рис. 9 проілюстровано залежність часу виконання програмного модуля шифрування і розшифрування для шифру RSA в залежності від розміру файлу та довжини модуля перетворення.

5. Приховування інформації в просторовій області нерухомих зображень

Приховування криптограм в контейнерах, наприклад, графічних зображеннях, дозволяє підвищити рівень безпеки захисту інформації. Основна ідея стеганографічного захисту полягає в тому, що приховування даних здійснюється таким чином, щоб це не було помітно для не проінформованого спостерігача. Методи приховування даних в зображеннях використовують властивості зорової системи людини (ЗСЛ) та класифікуються на 2 групи: низькорівневі (*фізіологічні*) та високорівневі (*психофізіологічні*) [2,7]. До низькорівневих властивостей слід віднести наступні:

1. Слабка чутливість до незначної зміни яскравості.

2. Слабка чутливість до незначної зміни контрасту.
3. Частотна чутливість.
4. Ефект маскування.
5. Слабка чутливість до незначної зміни яскравості синього кольору.

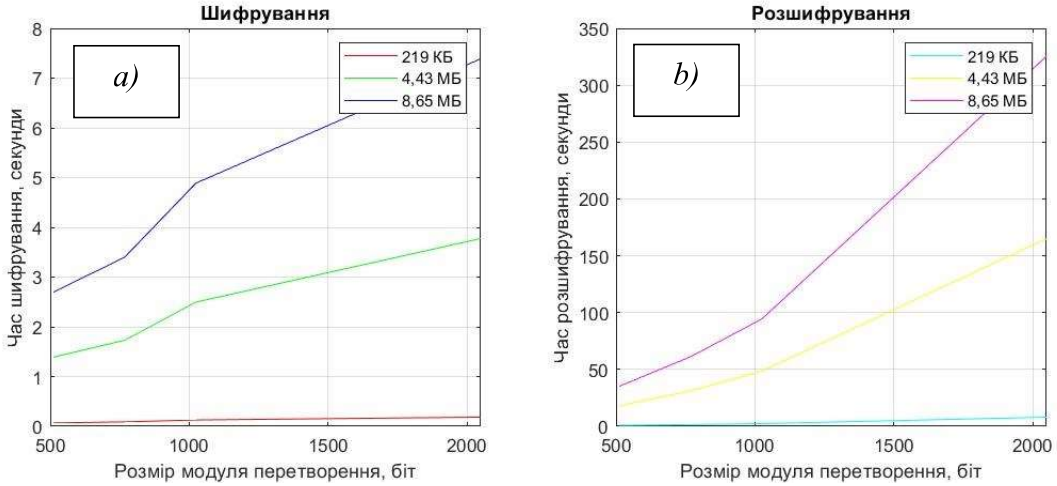

Рис. 9 – Час шифрування (*a*) і розшифрування (*b*) для різних довжини модуля перетвореннята розміру файлу

Fig. 9 – Encryption (*a*) and decryption (*b*) times for different lengths of the transform module & file size

До високорівневих властивостей слід віднести наступні [12]:

1. Чутливість до кольору – деякі кольори привертають більше уваги людини порівняно з іншими кольорами. Ефект помітності підвищується, коли відтінок заднього тла суттєво відрізняється від кольорів об'єктів розташованих на ньому [7].
2. Чутливість до розміщення – передусім, людині властиво розглядати центральну ділянку зображення, а вже потім звертати увагу на його околиці.
3. Чутливість до зовнішніх подразників – рух очей людини залежить від таких факторів як конкретна ситуація або наявність додаткової інформації, інструкцій щодо способу перегляду.
4. Чутливість до контрасту – різкі контрастні області зображення та значні перепади яскравості викликають до себе більше уваги.
5. Чутливість до розміру – великі за розміром області зображення більш помітні порівняно з меншими. При цьому існує поріг насичення, коли подальше збільшення розміру не має істотного значення.
6. Чутливість до форми – у людини значно більше уваги викликають довгі та тонкі об'єкти, у порівнянні з однорідними та округлими.

З урахуванням вказаних властивостей побудовані відомі методи стеганографічної вставки інформації в нерухомі зображення, наприклад такі, як:

1. Метод вбудовування на основі зміни найменш значущих біт (*методи псевдовипадкової перестановки, блокового вбудовування та ін.*.).
2. Метод квантування.
3. Метод Куттера-Джордона-Боссона.
4. Метод вбудовування в частотній області на основі кодування різниць абсолютних значень дискретного косинусного перетворення (метод Коха-Жао).
5. Метод Бенгама–Мемона–Ео–Юнг.
6. Метод прямого розширення спектра.

На практиці, не всі стеганографічні методи приховування інформації в нерухоме зображення гарантують безпомилкове вилучення повідомлення. Для того, щоб правильно розшифрувати криптограму потрібно використовувати методи, які дозволяють вилучити повідомлення без спотворень. Альтернативним рішенням може бути застосування методів завадостійкого кодування (наприклад, коди Хеммінга, БЧХ коди чи коди Ріда-Соломона, які дозволяють виправити можливі помилки. Ці методи дозволяють корегувати помилки, тобто виявляти й вилучати їх, що збільшує надійність вилучення прихованої інформації.

6. Вставка даних в нерухомі зображення на основі модифікації найменш значущого біта

Метод заміни найменш значущого біту (НЗБ, *LSB – Least Significant Bit*) є найпростішим способом стегановставки інформації в нерухоме зображення без видимих спотворень контейнеру. Метод *LSB* ґрунтується на експлуатації 1-їнизькорівневої властивості ЗСЛ [12]. Суть методу полягає в заміні менш значущих бітів пікселів зображення на біти прихованого інформаційного повідомлення. При цьому людина не спроможна виявити ці зміни. Колір кожного пікселю представлений комбінацією трьох кольорових компонентів, т.з. RGB кольорова модель. Рівень інтенсивності кожної з RGB складових (рис. 10) може приймати значення $0\ldots255$ (всього $L_m = 256$ рівнів квантування) та кодується 8 бітами [7,12].

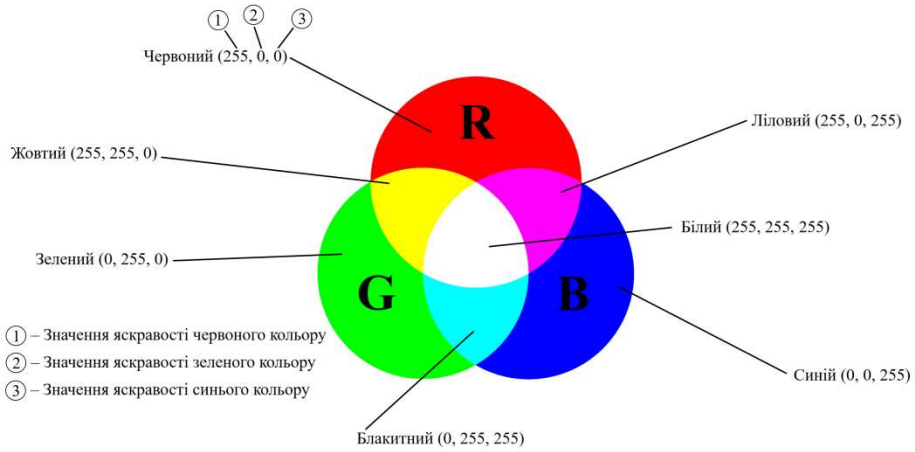

Рис. 10 – Модель RGB
Fig. 10 – RGB model

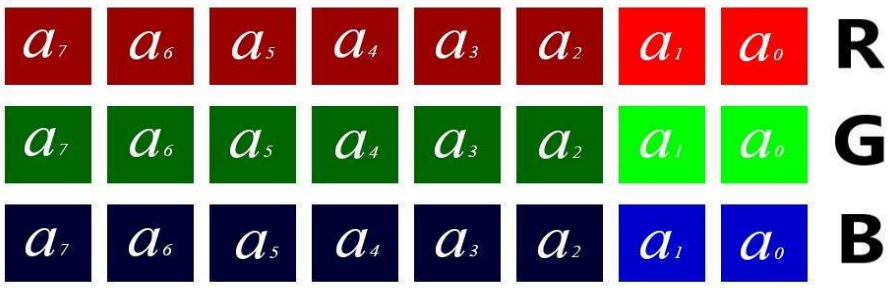

Рис. 11 –Бітове представлення кольорових компонентів
Fig. 11 – Bit representation of color components

Піксель являє собою одну точку зображення, яка містить рівні інтенсивності кожного з 3-х кольорових RGB каналів. Відповідні рівні інтенсивності кодуються 3 байтами (рис. 11), які в сукупності визначають потрібний відтінок кольору для конкретного пікселю. Отже, інформація про колір для певного пікселю представлена 24 бітами (3 байтами).

Відомо, що поріг чутливості ЗСЛ до зміни яскравості складає 2-3% [12]. Це означає, що, якщо модифікація рівня яскравості пікселів знаходиться нижче порога чутливості ЗСЛ, то він не виявить візуального викривлення зображення-контейнеру. При цьому менш «вагомі» (*тобто, молодші*) бітові розряди у цифровому зображенні, мають менший вплив на його візуальні характеристики в порівнянні зі старшими бітами [12], тому ці біти кольорових каналів (або градації сірого (визначається одним каналом)) можуть використовуватись для інкапсуляції бітів прихованого повідомлення. Перспективним вектором розробок є гібридне застосування криптографії та стеганографії: - приховування криптограм в контейнерах. В цьому разі для вбудовування методом НЗБ шифрованої інформації за допомогою криптосистеми RSA застосовується пустий контейнер (рис. 12). Кожен символ зашифрованого повідомлення, прочитаний в кодуванні ASCII, використовуючи команди середовища *MathCAD*, а вставка бітів криптограми зроблено в нульові біти (рис.11) послідовних байтів, масиву растрових даних червоного каналу (R).

В загальному випадку важливо розуміти, що для вставки прихованої інформації можна використовувати растрові дані будь-якого кольорового каналу, при цьому ЗСЛ не помічає спотворень зображення-контейнеру, оскільки його найменш значущий біт асоціюється з «шумом» та, за замовчуванням, не є важливим для візуальної оцінки вихідного зображення. Заповнений контейнер, який містить криптограму представлений на рис.13. З порівняння порожнього та заповненого контейнерів (*рис.12- 13*) можна стверджувати, що помітні ЗСЛ викривлення контейнеру, відсутні.

"1.bmp"

Рис. 12 –Порожне зображення - контейнер
Fig. 12 – An empty image - container

"Stego.bmp"

Рис. 13 – Заповнений контейнер
Fig. 13 – Filled container

В наведеному прикладі, причина малої помітності видимих викривлень контейнеру обумовлена тим, що *max*спотворення, які вносяться до окремих пікселів в наслідок зміни їх яскравості (для випадку вставки даних повідомлення в нульові біти контейнеру), не перевищують величину 2^0, що лежить нижче порогу чутливості ЗСЛ до незначної зміни яскравості контейнеру [12]. Специфікацією формату **bmp24* загальна кількість рівнів квантування яскравості кожного окремого пікселю дорівнює $2^8=256$. Тоді оцінити поріг чутливості (ПЧ)ЗСЛ до незначної зміни яскравості зображення, можна як:

$$ПЧ = \frac{\Delta}{256} * 100\%, \quad (15)$$

де, Δ – величина внесених спотворень яскравості (*число рівнів квантування*) окремих пікселів при використанні методу НЗБ для приховування інформаційного повідомлення.

Високий рівень популярності методу НЗБ (*LSB)* зумовлений, тим, що він достатньо простий в реалізації та ефективний для приховування значних обсягів інформації в невели-

ких файлових об’єктах [7]. Метод *LSB* може бути вразливим до різних видів атак, існуючих як у пасивних, так і в активних сценаріях атак. Основний недолік *LSB* полягає у його високій чутливості до найменших спотворень контейнера[12], наприклад: - компресія нерухомих зображень та/чи геометричні атаки, можуть призвести до втрати прихованої інформації чи її хибного відображення прихованого контенту. Щоб нівелювати можливі спотворення вилученого повідомлення, внаслідок зовнішнього впливу на заповнений контейнер, слід додатково використовувати методи завадостійкого кодування (Хеммінга, БЧХ та ін.).

7.Висновки

1. Розглянуто узагальнені структурні схеми стеганографічної і криптографічної систем, їх специфікація та компоненти, виконано огляд традиційних криптосистем, що використовуються в сучасних комплексних системах захисту інформації. Запропоновано бліц-огляд основних особливостей стеганоалгоритму НЗБ, що використовується для приховування даних в зображеннях та властивості ЗСЛ, котрі враховуються відомими стеганографічними методами при інкапсуляції (вставці) стеганографічного контенту в структуру контейнерів.

2. За результатами аналізу, можна стверджувати, що стеганографічну та криптографічну системи можна розглядати, як специфічний варіант системи зв’язку і передачі даних. Абстрактне визначення стеганографічної системи включає наступні множини: - множина вихідних інформаційних повідомлень; - множина контейнерів; - множина стеганограм; - множини прямих та обернених відображень; - множини ключів-екстракторів даних, які відповідають цим відображенням. Абстрактне визначення криптографічної системи охоплює такі множини, як: - множина вихідних повідомлень; - множина криптограм; - множини прямих та обернених відображень і відповідні їм ключі.

3. Асиметричні системи криптографічного захисту, більш стійкі до атак компрометації секретних ключів, оскільки використовуються різні ключі для процедур шифрування/розшифрування. Вагомою перевагою асиметричних криптосистем є застосування ключів великої довжини в криптографічних алгоритмах, що дозволяє підвищити обчислювальну складність. Складні математичні операції та ключі великих розмірів уповільнюють виконання асиметричних алгоритмів у порівнянні з симетричними. Асиметричні алгоритми вимагають значно більше обчислювальних ресурсів для здійснення високорівневих обчислень.

4. Алгоритм RSA використовує асиметричний підхід й широко використовується в сучасних протоколах автентифікації та забезпечення конфіденційності інформації в глобальних мережах. Збільшення довжини модуля призводить до зростання часу генерації ключової пари. Графіки залежностей для процедур шифрування та розшифрування різняться, оскільки на розшифрування даних витрачається більше часу, ніж на їх шифрування. Причиною цього може бути істотна різниця відритого, секретного ключа. Збільшення розміру файлу та модулю перетворення, призводять до збільшення часу, який витрачається на виконання процедур шифрування і розшифрування для системи RSA.

5. У стеганографії існує широкий спектр методів для реалізації приховування даних в нерухомі зображення. Вилучення вихідного повідомлення з криптограми вимагає не лише відповідний секретний ключ, але й збереження цілісності криптограми. Виходячи з цього, можна стверджувати, що не всі методи придатні для приховування криптограм в контейнерах, оскільки вони не можуть гарантувати безпомилкового вилучення інформації. При виборі методу потрібно звертати увагу на ймовірність правильного вилучення. Додатковим рішенням з протидії можливим помилкам є методи завадостійкого кодування, які дозволяють виявляти та виправляти можливі помилки стеганографічного повідомлення.

6. Комплексне застосування методів криптографії та стеганографії дозволяє забезпечити високий рівень захисту інформації від потенційних атак.

References

[1] Zamula, O. A., Horbenko, Y. I., &Shumov, O. I. (2010). The Regulatory and Legal Framework of Information Security. Integrated Information Protection Systems. Kharkiv: KhNURE.[In Ukrainian]

[2] Kuznetsov, O. O., Yevseyev, S. P., & Korol, O. G. (2011). Steganography. Kharkiv: KhNEU.[In Ukrainian]

[3] Shekhanin, K., Gorbachova, L., & Kuznetsova, K. (2021). Comparative analysis and study of information carrier properties for steganographic data hidden in cluster filesystems. Computer Science and Cybersecurity, (1), 37-49.[In Ukrainian] https://periodicals.karazin.ua/cscs/article/view/17266/15910 DOI: 10.26565/2519-2310-2021-1-03

[4] Kuznetsov, A., Shekhanin, K., Kolgatin, A., Kuznetsova, K., & Demenko, Y. (2018). Hiding data in file structure. Computer Science and Cybersecurity, 9(1), 43-52.[In Ukrainian]https://periodicals.karazin.ua/cscs/article/view/12013

[5] Lesnaya, Y., Goncharov, M., & Malakhov, S. The results of modeling attempts of unauthorized extraction of stego-content for various combinations of an attack on the experimental steganographic algorithm. Scientific Collection *«Inter Conf»*, (141), 338–345. Retrieved from https://archive.interconf.center/index.php/conference-proceeding/article/view/2319/2348

[6] Yesina, M., & Shahov, B. (2021). Research of implementation of candidates of the second round of NIST PQC competition focused on FPGA Xilinx family. *Computer Science and Cybersecurity*, (1), 16-36. https://periodicals.karazin.ua/cscs/article/view/17265/15909 DOI: 10.26565/2519-2310-2021-1-02

[7] Konakhovych, G. F., Progonov, D. O., & Puzirenko, O. Yu. (2018). Computer steganographic processing and analysis of multimedia data. Kyiv: "Centerfor Educational Literature".[In Ukrainian]

[8] The Decree of the President on the Regulations on the Procedure for Cryptographic Protection of Information in Ukraine" dated May 22, 1998, No. 505/98. [In Ukrainian] https://ips.ligazakon.net/document/u505_98?an=1&ed=1999_09_27

[9] Lakhno, V. A. (2016). Lecture Notes on the Discipline 'Fundamentals of Cryptographic Information Protection.' Kyiv. [In Ukrainian]

[10] CCNA Cyber Ops (Version 1.1) – Chapter 9: Cryptography and the Public Key Infrastructure. (2019). Вилучено з https://itexamanswers.net/ccna-cyber-ops-version-1-1-chapter-9-cryptography-and-the-public-key-infrastructure.html

[11] Tarnavsky, Yu. A. (2018). Information Security Technologies (pp. 107-108). Kyiv: Igor Sikorsky Kyiv Polytechnic Institute. [In Ukrainian]

[12] Kuznetsov, O. O., Poluyanenko, M. O., & Kuznetsova, T. Yu. (2019). Data hiding in the spatial domain of still images by modifying the least significant bit. Kharkiv: V. N. Karazin Kharkiv National University.[In Ukrainian]

Submitted November 17, 2023; Revised December 18, 2023; Accepted December 25, 2023

Authors:
Bodnia Mykyta, CSD Student, V.N. Karazin Kharkiv National University, Ukraine.
E-mail:bodnia2020kb12@student.karazin.ua
Yesina Maryna, Ph.D., Associate Professor, Department of Security of Information Systems and Technologies, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine; research associate-consultantof JSC"IIT", Kharkiv, Ukraine.
E-mail:m.v.yesina@karazin.ua
ORCID: https://orcid.org/0000-0002-1252-7606
Ponomar Volodymyr, Ph.D., researcherof Security of Information Systems and Technologies, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine; design engineerof JSC"IIT", Kharkiv, Ukraine.
E-mail:Laedaa@gmail.com
ORCID:https://orcid.org/0000-0001-5271-2251

Researching the possibilities of using steganographic and cryptographic algorithms for information hiding.

Abstract. The organization of information security has always been a relevant task, especially after the emergence of information and communication systems. The fundamental directions in the field of information security, dating back to ancient times, include cryptography and steganography. Cryptography implements information protection by transforming it into an unreadable form. Steganography allows the concealment of information in various containers (such as images, texts, audio recordings), keeping the presence of information unnoticed by casual observers. The article discusses approaches to cryptography and steganography, the concept of hybrid application of cryptographic and steganographic methods to provide a dual-layer data protection, and the overall architecture of cryptographic and steganographic systems. Traditional cryptographic systems applied in modern information security systems include symmetric and asymmetric cryptosystems. Although symmetric systems have evolved with the appearance of new mathematical transformations, they have a significant drawback. It consists of the need for an additional transfer of the secret key to the recipient. Such a strategy requires the use of a protected communication channel equipped with technical protection systems. At the same time, there is a risk of unauthorized access, which can cause the secret key to be compromised. Based on the above problems of symmetric cryptosystems, preference is given to asymmetric algorithms when developing protection mechanisms. An analysis of the RSA cryptosystem, based on an asymmetric encryption approach, has been conducted. This system is used in contemporary authentication protocols and ensures confidentiality in information systems and the Internet. The performance of software modules for key pair generation, encryption, and decryption for the RSA system was investigated by modifying the algorithm's general parameters (transform module, source data size). The results of time measurements are presented in a table, based on which dependencies of time on specific parameter modifications are built. The steganographic algorithm of modification of the least significant bit (LSB), which is used to hide data in images, is studied. Currently, there is a wide range of steganographic algorithms developed based on the characteristics of human sensory systems (such as vision or hearing). The article discusses the properties of the human visual system (HVS) utilized in steganography.

Keywords: *Cryptography, Steganography, Key, Information Message, Asymmetric Cryptosystem, Symmetric Cryptosystem, Ciphertext, Steganogram.*