ISSN 2707-1898 (print)

Український журнал інформаційних технологій
Ukrainian Journal of Information Technology
http://science.lpnu.ua/uk/ujit
https://doi.org/10.23939/ujit2020.02.037
Article received 28.02.2020 p.
Article accepted 25.10.2020 p.
UDK 004.832.3:519.711.2

Correspondence author
A. M. Kovalchuk
akm805@ukr.net

А. М. Ковальчук

Національний університет "Львівська політехніка", м. Львів, Україна

БІНАРНІ ЛІНІЙНІ ПЕРЕТВОРЕННЯ В МОДИФІКАЦІЯХ АЛГОРИТМУ RSA ШИФРУВАННЯ ЗОБРАЖЕНЬ

Розглянуто бінарні лінійні перетворення в модифікаціях алгоритму RSA шифрування зображень, які побудовані так, що при малих значеннях ключа можна досягти якісного шифрування, але за умови, правильного підбору параметрів ключа шифрування, внаслідок чого досягається висока швидкість роботи алгоритму. Оскільки зображення є одними із найбільш уживаних видів інформації в сучасному інформаційному суспільстві, то актуальним завданням є його захист від несанкціонованого доступу та використання. Важливою характеристикою зображення є наявність в ньому контурів, завдання виділення якого вимагає використання операцій над сусідніми елементами, які є чутливими до змін і пригашають області постійних рівнів яскравості. Отже, контури – це ті області, де виникають зміни, стаючи світлими, тоді як інші частини зображення залишаються темними.

Математично – ідеальний контур представляє розрив просторової функції рівнів яскравості в площині зображення. Тому виокремлення контура означає пошук найбільш різких змін, тобто максимумів модуля вектора градієнта. Це є однією з причин, через що контури залишаються в зображенні при шифруванні в системі RSA, оскільки шифрування тут базується на піднесенні до степеня по модулю деякого натурального числа. При цьому, на контурі й на сусідніх до контура пікселах піднесення до степеня значення яскравостей дає ще більший розрив.

Проблема захисту від несанкціонованого доступу є складнішою порівняно з проблемою захисту використання. Основним базисом для організації захисту зображення є таке припущення: зображення – це стохастичний сигнал. Це спричинює перенесення класичних методів шифрування сигналів на випадок зображень. Але зображення є специфічним сигналом, який володіє, в додаток до типової інформативності (інформативності даних), ще й візуальною інформативністю. В зв'язку з цим до методів шифрування у випадку їх використання стосовно зображень висувається ще одна вимога – повна зашумленість зашифрованого зображення. Це потрібно для того, щоб унеможливити використання методів візуального оброблення зображень. Алгоритм RSA є одним із промислових стандартів шифрування сигналів. За відношенням до зображення існують певні проблеми його шифрування, а саме: частково зберігаються контури на різко флуктуаційних зображеннях. Тому актуальним завданням є розроблення модифікації методу RSA такої, щоб: зберегти стійкість до дешифрування; забезпечити повну зашумленість зображення, з метою унеможливити використання методів візуального оброблення зображень. Одним із шляхів вирішення цього завдання є використання бінарних афінних перетворень.

Ключові слова: шифрування, дешифрування, бінарне перетворення, зображення.

Вступ

З розвитком і поширенням інформаційних технологій зростає актуальність питання інформаційної безпеки. Розгляду цього питання присвячуються щорічні тематичні конференції і симпозіуми (напр. *RSA Conference*, Сан-Франціско, США). Поява нових мережевих технологій, "хмаркових" обчислень й ін., які дуже активно просуваються на ринок, спричинюють потребу розроблення нових стандартів безпеки і удосконалення методів персоніфікованого захисту даних.

Зображення є одними із найбільш вживаних видів інформації в сучасному інформаційному суспільстві. Відповідно актуальним завданням є захист зображень від несанкціонованого доступу та використання. Проблема несанкціонованого використання зображень на найнижчому рівні вирішується положеннями про авторське право, а на найвищому – методами стеганографії, поліграфічними сітками, тощо.

Проблема захисту від несанкціонованого доступу є складнішою порівняно з проблемою захисту використання. Основним базисом для організації захисту зображення є таке припущення: зображення – це стохастичний сигнал. Це спричинює перенесення класичних методів шифрування сигналів на випадок зображень. Але зображення є специфічним сигналом, який володіє, в додаток до типової інформативності (інформативності даних), ще й візуальною інформативністю [4], [10]. А остання привносить в питання захисту нові задачі.

Саме ця інформативність із дуже розвинутими сучасними методами оброблення зображень дає можливість для організації несанкціонованого доступу. Фактично організація хакерської атаки на зашифроване зображення можлива у двох варіантах: через традиційний взлом методів шифрування, або через методи візуального оброблення зображень (методи фільтрації, виділення контурів, тощо). Хоча останні не дають повного відтворення зашифрованого зображення, проте дають можливість отримати деяку інформацію із зображення. В зв'язку з цим до методів шифрування у випадку їх використання стосовно зображень висувається ще одне завдання – повна зашумленість зашифрованого зображення. Це потрібно для того, щоб унеможливити використання методів візуального оброблення зображень.

Алгоритм RSA є одним із найбільш уживаних промислових стандартів шифрування сигналів. За відношенням до зображення існують певні проблеми його шифрування, а саме частково зберігаються контури на різко флуктуаційних зображеннях [5], [8], [9].

Об'єкт дослідження – модифікаціях алгоритму RSA шифрування растрових зображень.

Предмет дослідження – методи і засоби модифікації алгоритму RSA шифрування растрових зображень з використанням бінарних афінних перетворень, що дасть змогу зберегти його стійкість до дешифрування зображень, забезпечить повну їх зашумленість, а також унеможливить використання методів їхнього візуального оброблення.

Мета роботи – розроблення підходу до модифікації алгоритму RSA з використанням бінарних афінних перетворень, що дасть змогу зберегти стійкість до дешифрування зображень, забезпечить повну їх зашумленість, унеможливить використання методів візуального оброблення зображень.

Для досягнення зазначеної мети визначено такі основні *завдання дослідження*:

- проаналізувати останні дослідження та публікації;
- навести основні характеристики зображення та їх математичне формулювання;
- проаналізувати лінійний афінний шифр та бінарне афінне перетворення;
- навести особливості шифрування q дешифрування рядками матриці зображення, а саме шифрування по одному рядку матриці зображення та за двома її рядками;
- здійснити програмну реалізацію автоматизованої системи оброблення растрових зображень підвищеного рівня функціональної безпеки.

Наукова новизна отриманих результатів дослідження – розроблено математичну модель, яка описує модифікацію алгоритму RSA шифрування растрових зображень з використанням бінарних афінних перетворень, що забезпечило його стійкість, повну зашумленість, а також унеможливило використання методів їхнього візуального оброблення.

Практична значущість результатів дослідження – розроблений програмний додаток реалізує модифікацію алгоритму RSA для шифрування растрових зображень з використанням бінарних афінних перетворень, що дало змогу зберегти його стійкість до дешифрування, забезпечило повну зашумленість зображення, а також унеможливило використання методів візуального оброблення зображень.

Аналіз останніх досліджень та публікацій. Як відомо [6], теоретична стійкість визначається за умови, що не існує тимчасових обмежень на несанкціоноване дешифрування, і, отже, це є відповіддю на питання, чи криптосистема не може бути розколота в принципі. Їх можна побудувати за допомогою випадкового рівноймовірного ключа шифрування, довжина якого не менша від довжини відкритого тексту. Зовсім стійкі системи надзвичайно дорогі в реалізації. Тому на практиці використовують системи, які в принципі можна розколоти, але за неприйнятний час [1], [2], [5], [10].

Проблеми розроблення інформаційних технологій підвищення надійності та безпеки зображень відображено в працях К. Шеннона, М. Діффі, М. Хеллмана, В. К. Задіраки, І. Д. Горбенка, В. Я. Чечельницького, М. П. Карпінського, Ю. М. Коростіля, О. А. Курченка. Серед наявної великої кількості криптографічних перетворень особливе місце займає асиметрична система криптографічного кодування RSA. При великих значеннях ключів кодування та декодування ця криптосистема визначає високий рівень безпеки будь-яких даних. Це привело до того, що алгоритм практичної реалізації криптосистеми став промисловим стандартом і визначає напрями розвитку інформаційних технологій забезпечення функціональної безпеки даних загалом і графічних растрових зображень зокрема.

У випадку використання криптографічного кодування растрових зображень на підставі стандарту RSA для виникає проблема, яка полягає у тому, що на закодованому зображенні можуть зберігатись контури (флуктуації функції інтенсивності). У цьому випадку атака на об'єкт захисту може полягати не у зламі самого алгоритму, а у використанні методів цифрового оброблення зображень (фільтрації, реконструкції) для отримання основної інформативності цього зображення [9].

Отримані на сьогодні результати теоретичних і практичних досліджень надають можливість уникнути появи контурів на закодованих зображеннях при достатньо малих значеннях ключів. Проте, вони характеризується або високою обчислювальною складністю, або значними інформаційними втратами, які виникають в процесах забезпечення функціональної безпеки. Їх практичне використання є витратним з точки зору мінімізації ресурсів для забезпечення високого рівня функціональної безпеки.

Тому актуальним науковим завданням є розроблення підходу до модифікації алгоритму RSA з використанням бінарних афінних перетворень, що дасть змогу зберегти його стійкість до дешифрування зображень, забезпечить повну їх зашумленість, унеможливить використання методів їхнього візуального оброблення.

Результати дослідження та їх обговорення

Відомо, що растрове зображення є сіткою (растром) пікселів, зазвичай, прямокутною матрицею, відображених на моніторі, папері та інших відображувальних пристроях і матеріалах. Кількість пікселів, зазвичай, вказують кількість пікселів по ширині і висоті (наприклад, 1024×768, 1920×1080 і т.д.). Кількість використовуваних кольорів або глибина кольору (обсяг пам'яті в бітах, що використовуються для одного пікселя). Колірний простір – RGB, CMYK, XYZ, YCbCr та ін. Роздільна здатність – довідкова величина, яка вказує на рекомендований розмір зображення.

Характеристики зображення. Нехай задано рисунок P з ширини l і висоти h. Його можна розглядати як матрицю пікселів

$$< dtp_{ij} >_{1\le i\le n,\ 1\le j\le m}, \qquad (1)$$

де dtp_{ij} – піксел з координатами i та j, n і m – кількість точок по ширині l та висоті h.

В загальному випадку n і m є залежними від l та h, а тому більш коректним є запис

$$n = n(l) \ \text{ і } \ m = m(h). \qquad (2)$$

Матриці (1) у відповідність ставиться матриця кольорів

$$C=\begin{pmatrix} c_{1,1} & \dots & c_{1,m} \\ \dots & \dots & \dots \\ c_{n,1} & \dots & c_{n,m} \end{pmatrix}, \qquad (3)$$

де c_{ij} – значення інтенсивності у напівтонових зображень піксела dtp_{ij}. Тобто має місце така відповідність [7]

$$P = \mathrm{P}_{l,h} = \left[pxl_{ij} \right]_{1 \le i \le n(l), 1 \le j \le m(h)} \to \mathrm{C} = \left[c_{ij} \right]_{1 \le i \le n(l), 1 \le j \le m(h)}. \quad (4)$$

Під градацію яскравості звичайно приділяється 1 байт, причому 0 – чорний колір, а 255 – білий (максимальна інтенсивність). У випадку кольорового зображення виділяється по байту на градації яскравостей всіх трьох кольорів. Можливе кодування градацій яскравості іншим кількістю бітів (4, 12, або 24), але людське око здатне розрізняти тільки 8 біт градацій на кожний колір, хоча спеціальна апаратура може давати і більше точну передачу кольорів

У випадку кольорових зображень c_{ij} треба розглядати як вектор основних характеристик кольорової палітри. Наприклад, якщо задано зображення у 24-бітному форматі палітри *RGB*, то

$$\mathrm{c}_{i,j} = \{c_{i,j}^R, c_{i,j}^G, c_{i,j}^B\},$$

де $c_{i,j}^R, c_{i,j}^G, c_{i,j}^B$ – значення червоного, зеленого та синього кольорів піксела dtp_{ij} відповідно. Тоді наведений нижче алгоритм треба застосувати до кожної характеристики окремо.

Якщо, наприклад, по ширині ввести в розгляд такий вектор

$$\tilde{c}_j = \{c_{i,j} \mid i = \overline{1,n}\}, \quad (5)$$

то (3) можна записати у вигляді

$$\mathrm{C} = \left[\tilde{c}_j \right]_{j=\overline{1,m}}. \quad (6)$$

Важливою характеристикою зображення є наявність в зображенні контурів. Задача виділення контура вимагає використання операцій над сусідніми елементами, які є чутливими до змін і пригашають області постійних рівнів яскравості, тобто, контури – це ті області, де виникають зміни, стаючи світлими, тоді як інші частини зображення залишаються темними [1], [4].

Математично – ідеальний контур це – розрив просторової функції рівнів яскравості в площині зображення. Тому виділення контура означає пошук найбільш різких змін, тобто максимумів модуля вектора градієнта [2], [4]. Це є однією з причин, через що контури залишаються в зображенні при шифруванні в системі RSA, оскільки шифрування тут базується на піднесенні до степеня по модулю деякого натурального числа. При цьому, на контурі й на сусідніх до контура пікселах піднесення до степеня значення яскравостей дає ще більший розрив.

Лінійний афінний шифр. Введемо означення бінарного аффінного перетворення евклідової площини в декартових координатах.

Перетворення евклідової площини називається афінним, якщо це перетворення відображає кожну пряму на пряму. Отже, лінійний афінний шифр – шифр афінної підстановки – має вигляд:

$$y = (ax + b) \bmod m. \quad (7)$$

У цьому виразі ключем є пара (a,b), $0 < a \le m-1$, $0 \le b \le m-1$, причому a повинно бути взаємно простим з m.

З виразу (7) одержуємо

$$x = (a'y + b') \bmod m, \quad (8)$$

де $a' = a^{-1} \bmod m$ – обернений до a елемент в кільці лишків за модулем m, $b' = -a'b$.

Рівність (8) має той самий вигляд, що й (7), отже шифрування й розшифрування здійснюються за цим самим алгоритмом, тільки з різними параметрами. Умова взаємної простоти a з m потрібна для того, щоб існував обернений елемент a^{-1} і рівняння (7) при фіксованому y мало єдиний розв'язок x, тобто можливо було однозначно розшифрувати. У протилежному випадку рівняння (8) має не єдиний розв'язок x або взагалі його не має.

Афінна підстановка легко піддається криптоаналізу, хоча кількість ключів в цьому шифрі $\varphi(m) \cdot m$, де $\varphi(m)$ – функція Ейлера (кількість менших за m і взаємно простих з ним чисел). Нехай y^* і y^{**} – перша і друга за частотою букви шифрованого тексту, x^* і x^{**} – відповідно найчастіша і наступна за нею букви алфавіту.

Природно припустити, що при шифруванні x^* перейде в y^*, а x^{**} – в y^{**}.

Складемо систему рівнянь:

$$\begin{cases} y^* = (ax^* + b) \bmod m; \\ y^{**} = (ax^{**} + b) \bmod m. \end{cases} \quad (9)$$

Відзначимо, що в цій системі невідомими є a і b, а x і y – відомі. З (9) маємо:

$$y^* - y^{**} = a\left(x^* - x^{**}\right) \bmod m. \quad (10)$$

Якщо пари $x^* \leftrightarrow y^*$, $x^{**} \leftrightarrow y^{**}$ підібрані вірно, то рівняння (9) має розв'язок a. Знаючи a, з (10) знаходимо b. Якщо ж ці пари не відповідають дійсності, то (9) або не має розв'язку, або при всіх розв'язках (10), розшифровуючи, одержимо беззмістовний текст.

Бінарне афінне перетворення. Бінарне афінне перетворення площини в декартових координатах має вигляд:

$$\begin{cases} x' = a_1 x + b_1 y + d_1, \\ y' = a_2 x + b_2 y + d_2, \end{cases} \quad (11)$$

де

$$\delta = \begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix} \ne 0. \quad (12)$$

Обернене до (11) перетворення також існує і тоді

$$x = \frac{\Delta_x}{\delta}, \; y = \frac{\Delta_y}{\delta}, \quad (13)$$

де

$$\Delta_x = \begin{vmatrix} x' - d_1 & b_1 \\ y' - d_2 & b_2 \end{vmatrix}, \; \Delta_y = \begin{vmatrix} a_1 & x' - d_1 \\ a_2 & y' - d_2 \end{vmatrix}. \quad (14)$$

Шифрування *q* дешифрування рядками матриці зображення

1. ***Шифрування по одному рядку матриці зображення.*** Нехай P, Q – довільні прості числа. Виберемо такі цілі числа [10]

$$N = PQ, \; \varphi(N) = (P-1)(Q-1),$$

$$ed \equiv 1 \left(\bmod \varphi(N) \right), \; e < \varphi(N), \; d < \varphi(N). \quad (15)$$

Шифрування відбувається з використанням елементів одного рядка за формулами (11), де

$$x = c_{i,j}, \; y = c_{i,j+1}, \; i = \overline{1,n}, \; j = \overline{1,m}. \quad (16)$$

Вибираються дві сусідні точки, так щоб в кожну пару кожна точка була вибрана тільки один раз. Коефіцієнти

$$\begin{cases} a_1 = b_2 = (P+Q)^e \bmod N; \\ b_1 = a_2 = (P \cdot Q)^d \bmod N, \end{cases} \quad (17)$$

є цілі числа,

$$d_1 = j \cdot j, \; d_2 = j \cdot j \cdot j, \; j = \overline{1,m}. \quad (18)$$

Дешифрування проводиться за формулами оберненого перетворення (13) з тими ж самими коефіцієнтами (17). Результати розрахунку наведено на рис. 1.

2. *Шифрування за двома рядками матриці зображення*. Шифрування відбувається з використанням елементів двох рядків за формулами (11), де

$$x = c_{i,j},\ y = c_{i+1,j},\ i = \overline{1,n},\ j = \overline{1,m}. \qquad (19)$$

Вибираються два значення з однаковими номерами, по одній з кожного рядка, так щоб в кожну пару кожне значення було вибрано тільки один раз.

Коефіцієнти, описані такою системою рівнянь

$$\begin{cases} a_1 = a_2 = (P+Q)^e \bmod N; \\ b_1 = b_2 = (P \cdot Q)^d \bmod N, \end{cases} \qquad (20)$$

є цілими числа, які можна визначити за такими формулами

$$d_1 = -j \cdot j,\ d_2 = -j \cdot j \cdot j,\ j = \overline{1,m}. \qquad (21)$$

Дешифрування відбувається за формулами оберненого перетворення (13) з тими ж самими коефіцієнтами a_1, a_2, b_1, b_2.

Внаслідое проведеного експерименту отримано результати розрахунку, які наведено на рис. 2.

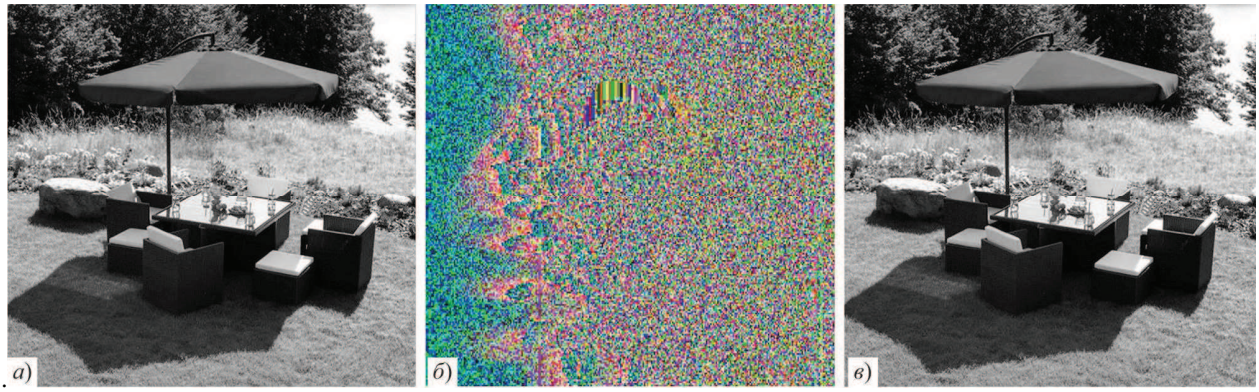

Рис. 1. Результати роботи з зображенням: *а*) початкове; *б*) зашифроване; *в*) дешифроване

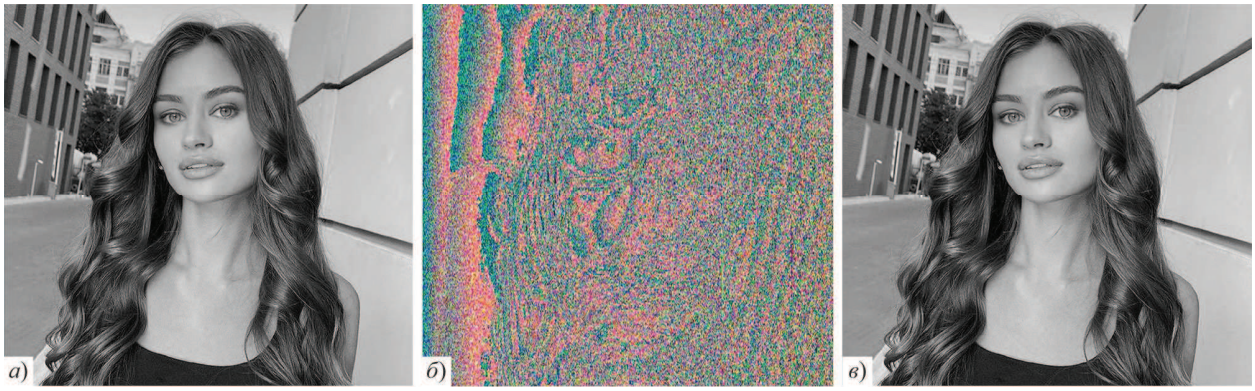

Рис. 2. Результати роботи з зображенням: а) початкове; б) зашифроване; в) дешифроване

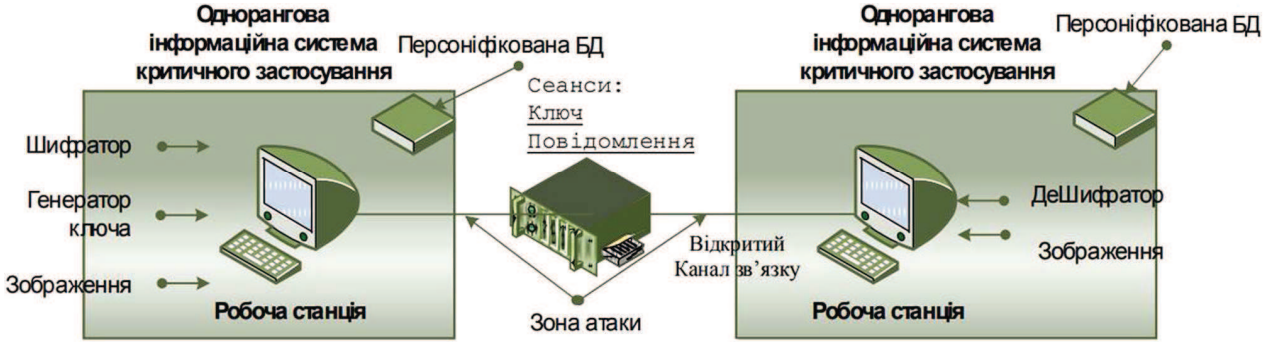

Рис. 3. Схема реалізації технології захисту растрових зображень в одноранговій мережевій автоматизованій системі

Отже, внаслідок виконання дослідження вирішено актуальну науково-прикладну задачу, яка полягає у розробленні підходу до модифікації алгоритму RSA з використанням бінарних афінних перетворень, що дає змогу зберегти його стійкість до дешифрування зображень, забезпечить повну їх зашумленість, а також унеможливить використання методів їхнього візуального оброблення.

3. *Програмна реалізація автоматизованої системи оброблення растрових зображень підвищеного рівня функціональної безпеки*. Розроблене у вигляді мережевого прикладного застосунку з використанням технології plug-ins програмне рішення призначене для організації:

- персоніфікованого захисту растрових зображень;
- захищеного обміну зображення в телекомунікаційних сеансах передачі даних.

Використання формату динамічної бібліотеки надає нам можливість застосовувати програмну реалізацію криптографічних алгоритмів у процесах розроблення та

експлуатації складних обчислювальних структур, а саме автоматизованих систем управління й, передусім, критичного призначення.

Підсистема захисту растрових зображень є складовою усіх сучасних автоматизованих систем. Проте, у випадку використання телекомунікаційних сеансів небезпека несанкціонованого витоку інформації зростає завдяки можливості хаккерських атак у процесах мережевих транзакцій. Відповідно зростає актуальність завдання забезпечення безпеки процесу функціонування мережевих автоматизованих систем.

На рис. 3 наведено схему реалізації технології захисту растрових зображень в автоматизованій системі без виділеного сервера. Типовим прикладом таких систем є медичні інофрмаційно-управляючі системи реалізовані в межах технології Smart House. Визначальним в архітектурі таких систем є їх автономне функціонування без зовнішніх виділених управляючих систем. Мережеві транзакції в таких системах здійснюються тільки у випадках виклику зовнішніх дій, синтезу зворотних реакцій та при виконанні синхронізаційних дій.

Автономність функціонування автономних однорангових систем визначає наявність персональних БД на кожному обчислювальному пристрої. Відповідно до цього стає актуальним завданням персоніфікованого захисту растрових зображень (наприклад, зображень людини для віддаленого діагностування та визначення критичних ситуацій) на окремому комп'ютері. Таке завдання, передусім, вирішується засобами авторизації локальної БД. Водночас, використання засобів криптографічного кодування дає змогу істотно посилити цей захист, оскільки у файлах з БД будуть зберігатися закодовані зображення. У випадку, якщо локальна БД не використовується як система із авторизованим доступом, то криптографічне кодування даних залишається єдиним способом їх захисту від несанкціонованого витоку. На рис. 3 персоніфікований захист растрових зображень відображено тільки позначенням "Персоніфікована БД".

Більшість сучасних однорангових автоматизованих системи з різних причин використовують мережеві комунікаційні засоби. Серед цих причин, насамперед, може бути потреба використання зовнішніх систем:

- віддаленого глибокого інтелектуального аналізу;
- протоколювання й трекінгу;
- управління та прийняття рішень.

У випадку використання таких зовнішніх систем захисту інформації неминуче виникає завдання передавання растрового зображення. Оскільки існує тільки комунікаційний канал, то, зазвичай, мережеві транзакції здійснюються відкритими каналами. Відповідно криптографічне кодування таких зображень залишається єдиним засобом їхнього захисту від мережевого перехоплення конфіденційної інформації.

Розроблений нами програмний застосунок разом із бібліотекою захисту є прототипом саме однорангових автоматизованих систем. Бібліотека функцій захисту растрових зображень може бути використана для розроблення програмного модуля мережевого захисту інформації шляхом кодування усіх повідомлень, що передаватимуться в комунікаційні порти.

Особливістю цього підходу є відокремленість агента від самої системи захисту. Це має свої переваги, оскільки такий модуль є стійким до збоїв самої системи і забезпечує захист растрових зображень для будь-яких комунікаційних сеансів.

Недоліком відокремленого програмного модуля є складність забезпечення персоніфікованого захисту растрових зображень в локальній БД системи. Тому потрібно криптографічний програмний модуль імплементувати в саму систему захисту і відокремлювати від решти завдань, в т. ч. й мережевих. Такий підхід забезпечуватиме максимальну незалежність роботи модуля, а також можливість оновлення алгоритмів захисту без потреби перебудови системи загалом.

Висновки

Запропоновані модифікації алгоритму шифрування даних призначені для шифрування зображень в градаціях сірого і ґрунтуються на використанні ідей базового алгоритму RSA. Запропоновані модифікації алгоритму можна використати стосовно будь-якого типу растрового зображення, але найбільші переваги досягаються у випадку використання зображень, які дають змогу чітко виокремити контури.

Обидва типи модифікацій алгоритму без жодних застережень можна використати й стосовно шифрування кольорових зображень. Однак, незалежно від типу зображення, пропорційно до розмірності вхідного зображення, може зрости розмір шифрованого зображення.

Модифіковані методи шифрування растрових зображень побудовані так, що при малих значеннях ключа також можна досягти якісного шифрування, але за умови правильного підбору параметрів шифрування. При цьому досягається висока швидкість роботи алгоритму.

Окрім цього, підвищується стійкість процедури шифрування, оскільки для шифрування й дешифрування зображень використовують довільні прості числа, які можуть бути досить великими. А від цього залежить стійкість криптографічного алгоритму шифрування.

Розроблене на підставі отриманих теоретичних результатів дослідження програмне рішення забезпечує збереження растрового зображення не тільки при передаванні його комунікаційними каналами зв'язку, а й у випадку організації стійкого персоніфікованого захисту.

References

[1] Gryciuk, Yu., & Grytsyuk, P. (2015). Perfecting of the matrix Affine cryptosystem information security. *Computer Science and Information Technologies: Proceedings of Xth International Scientific and Technical Conferenc*e (CSIT'2015), 14–17 September, 2015. pp. 67–69. https://doi.org/10.1109/stc-csit.2015.7325433

[2] Gryciuk, Yu. I., & Grytsyuk, P. Yu. (2015). Mathematical Foundations of the generation of keys using a permutation cipher Cardano. *Scientific Bulletin of UNFU*, 25(10), 311–323. https://doi.org/10.15421/40251048

[3] Hrytsiuk, Yu., & Grytsyuk, P, Dyak, T., & Hrynyk, H. (2019). Software Development Risk Modeling. *IEEE 2019 14th International Scientific and Technical Conference on Computer Sciences and Information Technologies* (CSIT 2019), (Vol. 2, pp. 134–137), 17–20 September, 2019. https://doi.org/10.1109/stc-csit.2019.8929778

[4] Iane, B. (2007). Tcifrovaia obrabotka izobrazhenii. Moscow: Tekhnosfera. 583 p. [In Russian].

[5] Kovalchuk, A., Izonin, I., Strauss, C., & Kustra, N. (2019). Image encryption and decryption schemes using linear and quadratic fractal algorithms and their systems. *1-st Internati-*

onal Workshop on Digital Content and Smart Multimedia, DCSMart, 2019. Lviv, Ukraine.
[6] Netravali, A. N., & Limb, D. O. (1980). Kodirovanie izobrazhenii: obzor. *TIIER, 68*(3), 76–117. [In Russian].
[7] Pavlidis, T. (1986). *Algoritmy mashinoi grafiki i obrabotki izobrazhenii*. Moscow: Radio i sviaz. [In Russian].
[8] Rashkevych, Y., Kovalchuk, A., Peleshko, D., & Kupchak, M. (2009). Stream Modification of RSA algorithm for image coding with precize contour extraction. *Proceedings of the X-th International Conference CADSM, 2009*. Lviv-Polyana, Ukraine.
[9] Rashkevych, Yu. M., Peleshko, D. D., Kovalchuk, A. M., & Peleshko, M. Z. (2008). Modyfikatsiia alhorytmu RSA dlia deiakykh klasiv zobrazhen. *Tekhnichni visti, 1*(27), *2*(28), 59–62. [In Ukrainian].
[10] Shnaier, B. (2003). *Prikladnaia kriptografiia*. Moscow: Triumf. 815 p. [In Russian].

A. M. Kovalchuk
Lviv Polytechnic National University, Lviv, Ukraine

BINARY LINEAR TRANSFORMATIONS IN MODIFICATIONS OF RSA ALGORITHM OF IMAGES

The images are one of the most used kinds of the information in modern information company. Therefore actual problems is the organization of protection from unauthorized access and usage. An important characteristic of the image is the presence of contours in the image. The task of contour selection requires the use of operations on adjacent elements that are sensitive to change and suppress areas of constant levels of brightness, that is, contours are those areas where changes occur, becoming light, while other parts of the image remain dark. Mathematically, the ideal outline is to break the spatial function of the brightness levels in the image plane. Therefore, contour selection means finding the most dramatic changes, that is, the maxima of the gradient vector module. This is one of the reasons that the contours remain in the image when encrypted in the RSA system, since the encryption here is based on a modular elevation of some natural number. At the same time, on the contour and on the neighboring contours of the peak villages, the elevation of the brightness value gives an even bigger gap.

Problem protect from unauthorized access is by more composite in matching with a problem protect from usage. Basis for organization of protection is the interpretation of the image as stochastic signal. It stipulates carry of methods of encoding of signals on a case of the images. But the images are a specific signal, which one in possesses, is padding to representative selfless creativeness, also by visual selfless creativeness. Therefore to methods of encoding, in case of their usage concerning the images, one more requirement – full noise of the coded image is put forward. It is necessary to make to impossible usage of methods of visual image processing. The algorithm RSA is one of the most used production specifications of encoding of signals. In attitude of the images there are some problems of its encoding, the contours on the coded image are in particular saved. Therefore actual problem is the mining of modification to a method RSA such, that: to supply stability to decoding; to supply full noise of the images. One solution of this problem is usage of affine transformations.

Keywords: encryption, decryption, binary transformation, image.

Інформація про автора:

Ковальчук Анатолій Михайлович, ст. викладач, кафедра інформаційних технологій видавничої справи.
Email: akm0519@gmail.com; http://orcid.org/0000-0001-5910-4734; https://publons.com/researcher/R-3495-2017

Цитування за ДСТУ: Ковальчук А. М. Бінарні лінійні перетворення в модифікаціях алгоритму RSA шифрування зображень. *Український журнал інформаційних технологій*. 2020, т. 2, № 1. С. 37–42.

Citation APA: Kovalchuk, A. M. (2020). Binary linear transformations in modifications of RSA algorithm of images. *Ukrainian Journal of Information Technology, 2*(1), 37–42. https://doi.org/10.23939/ujit2020.02.037