ПОБІТОВІ ОПЕРАЦІЇ З ЕЛЕМЕНТАМИ АЛГОРИТМУ RSA В ШИФРУВАННІ-ДЕШИФРУВАННІ КОЛЬОРОВИХ ЗОБРАЖЕНЬ

Ковальчук А.М., старший викладач,
Пелех Ю.М.,канд.техн.наук, асистент,
Бубела Т.З., докт.техн.наук, професор
Національний університет «Львівська політехніка», Україна
e-mail: anatolii.m.kovalchuk@lpnu.ua

Анотація

Зображення як стохастичний сигнал є одною із найбільш уживаних форм інформації. Відповідно актуальною задачею є захист зображень від несанкціонованого доступу та використання. Це спричинює використання відомих класичних методів шифрування у випадку шифрування зображень. Але зображення є сигналом, який володіє, в додачу до типової інформативності, ще й візуальною інформативністю.
Така інформативність для сучасних методів обробки зображень дає можливість організації несанкціонованого доступу. Фактично створення атаки на зашифроване зображення можлива у двох варіантах: через традиційний злом методів шифрування, або через класичні методи візуальної обробки зображень (фільтрація, виокремлення контурів, тощо). 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 візуальної обробки зображень.
Алгоритм RSA є одним із найбільш уживаних промислових стандартів шифрування сигналів. На відміну від симетричного кодування у схемі кодування з відкритим ключем неможливо обчислити процедуру дешифрування, знаючи процедуру шифрування. А саме, час роботи алгоритму обчислення процедури дешифрування настільки великий, що його не можна реалізувати на будь-яких сучасних комп'ютерах, так само як і на комп'ютерах майбутнього. Такі схеми кодування називають асиметричними.
Тому актуальною задачею є реалізація такого використання алгоритму RSA, щоб при шифруванні зображення:
– не погіршилася криптографічна стійкість алгоритму RSA;
– було досягнуто повної зашумленості зображення для запобігання використанню методів візуальної обробки зображень.
Запропоновано алгоритм використання елементів алгоритму RSA, як найбільш стійкого до несанкціонованого дешифрування сигналів, і побітових операцій для сумісного поєднання при шифруванні – дешифруванні зображень. Шифрування – дешифрування проводиться без додаткового зашумлення. Запропонований алгоритм застосовано до зображень, в яких наявні строго виокремлені контури. Елементи алгоритму RSA використовуються для здійснення побітових операцій над величинами значень інтенсивностей пікселів кольорового зображення. Розроблений алгоритм має вищу криптографічну стійкість у порівнянні з алгоритмом RSA. Описано можливості використання елементів алгоритму RSA в побітових перетвореннях при шифруванні – дешифруванні зображень.
Наведено результати моделювання шифрування для криптографічних перетворень кольорових зображень заданої розмірності. Розроблено модифіковані моделі та алгоритмічні процедури процесів формування ключів, прямого та оберненого криптографічних перетворень, що зводяться до математичних поелементних операцій.

Ключові слова

Шифрування, кольорове зображення, побітові операції, контур, інтенсивність пікселя, дешифрування, матриця інтенсивностей пікселів.

1. Вступ

Необхідність вирішення теоретичних і практичних завдань інформаційної безпеки та досягнення необхідного рівня захисту інформації різного змісту зумовила в епоху інформаційних технологій та масових комунікацій і відповідний прискорений розвиток криптографії.
Зображення можна визначити як двовимірну функцію F(x, y), де x і y - координати в просторі (конкретно, на площині). Якщо величини x, y і F(x, y) приймають скінченне число дискретних значень, то кажуть про

цифрове зображення. Цифровою обробкою зображень називають обробку цифрових зображень за допомогою комп'ютерів. Відмітимо, що цифрове зображення складається зі скінченного числа елементів, кожен з яких розташований в конкретному місці і набуває певного значення. Ці елементи називаються елементами зображення або пікселями.
Математично цифрове зображення відображається матрицею інтенсивностей пікселів розмірності n на m, де n – число рядків матриці зображення, m – число стобців.
Найбільш поширеним і стійким алгоритмом шифрування інформації є алгоритм RSA, який відноситься до найбільш вживаних асиметричних алгоритмів. Безпека алгоритму RSA базується на ресурсно затратній факторизації великих натуральних чисел. Використання алгоритму RSA, як найбільш стійкого до несанкціонованого дешифрування, стосовно зображень, у яких є чітко виокремлені контури, не завжди дає задовільні результати. Це означає, що на зашифрованому зображенні можливо розрізнити основні контури вхідного зображення – тобто має місце ефект неповного зашумлення [1, 2].
Виокремлення контура означає пошук максимумів модуля вектора градієнта [2, 3]. Це є однією з причин, через що контури залишаються в зображенні при шифруванні в системі RSA, оскільки шифрування в RSA базується на піднесенні до степеня по модулю деякого натурального числа .
Наявність в зображенні контурів є важливою характеристикою зображення. Задача виокремлення контура вимагає використання операцій над сусідніми елементами, які є чутливими до змін і пригашають величини рівнів яскравості, тобто, контури – це ті області, де виникають зміни, стаючи світлими, тоді як інші частини зображення залишаються темними [4, 5].
При цьому, на контурі і на сусідніх до контура пікселах піднесеня до степеня значення яскравостей дає ще більший розрив [6, 7, 10 - 15].
По відношенню до зображення існують певні проблеми його шифрування, а саме частково зберігаються контури на різко флуктуаційних зображеннях [16 - 20].
Надалі будемо використовувати наступне означення аффінного перетворення евклідового простору в декартових координатах: перетворення евклідового простору називають афінним, якщо це перетворення відображає кожну площину на площину.

2. Недоліки

Числовими експериментами [8, 9] встановлено, що існують значення простих чисел, що в області контурів на зображенні при шифруванні можуть виникати значні відхилення значень інтенсивностей пікселів, що унеможливлює розмивання цих контурів при цих значеннях вибраних простих чисел.

3. Мета роботи

По відношенню до зображення актуальною задачею є таке використання класичного алгоритму RSA щоб:
не знизити криптографічну стійкість алгоритму RSA;
забезпечити повну зашумленість зображення, з метою унеможливити використання методів візуальної обробки зображень [6].
Одним із шляхів створення такої модифікації є поєднання елементів алгоритму RSA і побітових операцій в програмній реалізації.

4. Методика шифрування

Елементами алгоритму RSA називають прості числа $\boldsymbol{P}$ і $\boldsymbol{Q}$ та числа $\boldsymbol{e}$ та $\boldsymbol{d}$, отримані з конгруенції $\boldsymbol{ed} \equiv \mathbf{1}\ (\mathbf{mod}\ \boldsymbol{\varphi}(\boldsymbol{N}))$, $\boldsymbol{N} = \boldsymbol{P} * \boldsymbol{Q}$, де $\boldsymbol{\varphi}(\boldsymbol{N})$ – функція Ейлера.
Нехай задано зображення $\boldsymbol{S}$ ширини $\boldsymbol{l}$ і висоти $\boldsymbol{h}$. Приймемо, що зображенню у відповідність ставиться матриця кольорів (матриця інтенсивностей пікселів) [**4, 6, 7**]

$$S = \begin{pmatrix} S_{1,1} & \dots & S_{1,l} \\ \dots & \dots & \dots \\ S_{h,1} & \dots & S_{h,l} \end{pmatrix},$$

де s_{ij} – значення інтенсивності піксела.
Задача виокремлення 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. Тому виокремлення контура означає пошук найбільш різких змін, тобто максимумів модуля вектора градієнта [3]. 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 і на сусідніх до контура пікселах піднесення до степеня значення яскравостей дає ще більший розрив.

Опис алгоритмів шифрування.

Шифрування по двох рядках матриці зображення.

Нехай P і Q - пара довільних простих чисел і $N = P*Q$, $\varphi(N) = (P - 1)(Q - 1)$. Шифрування відбувається поелементно з використанням наступного перетворення елементів матриці S інтенсивностей пікселів:

1. За алгоритмом **RSA** вибираються числа $e < \varphi(N)$, $d < \varphi(N)$, що виконується конгруенція $ed \equiv 1 (\mathrm{mod}\ \varphi(N))$.
2. Для i – ого рядка матриці, $1 \le i \le l$, вибирається число $m \equiv (i + P) \ (\mathrm{mod}\ 32)$, і будуються числа $A \equiv m^e \ (\mathrm{mod}\ N)$, $X = i*A*P$.
3. Для $i+1$ – ого рядка матриці, $1 \le i \le l$, вибирається число $n \equiv (i + Q) \ (\mathrm{mod}\ 32)$, і будуються числа $B \equiv n^d \ (\mathrm{mod}\ N)$, $Y = i*B*Q$.
4. З використанням бінарної операції ^ - порозрядного виключеного «**АБО**» - будуються числа $a = s_{i,j} \wedge X$ та $b = s_{i+1,j} \wedge Y$.
5. Виокремлюється кожний розряд a_i числа a за наступною схемою:

   a_1= a & 01; $a_2 = a$ & 02; $a_3 = a$ & 04; $a_4 = a$ & 010; $a_5 = a$ & 020; $a_6 = a$ & 040;
   $a_7 = a$ & 0100; $a_8 = a$ & 0200; $a_9 = a$ & 0400; $a_{10} = a$ & 01000; $a_{11} = a$ & 02000;
   $a_{12} = a$ & 04000; $a_{13} = a$ & 010000; $a_{14} = a$ & 020000; $a_{15} = a$ & 040000; $a_{16} = a$ & 0100000;
   $a_{17} = a$ & 0200000; $a_{18} = a$ & 0400000; $a_{19} = a$ & 01000000; $a_{20} = a$ & 02000000;
   $a_{21} = a$ & 04000000; $a_{22} = a$ & 010000000; $a_{23} = a$ & 020000000; $a_{24} = a$ & 040000000;
   $a_{25} = a$ & 0100000000; $a_{26} = a$ & 0200000000; $a_{27} = a$ & 0400000000; $a_{28} = a$ & 01000000000; $a_{29} = a$ & 02000000000; $a_{30} = a$ & 04000000000; $a_{31} = a$ & 010000000000;
   $a_{32} = a$ & 020000000000, де & - операція арифметичного «**І**».
6. Виконується циклічне заміщення $m + 1$ розрядів числа a за схемою:
   $k = a_{m+1}$, $a_{m+1} = a_m$, … , $a_2 = a_1$, $a_1 = k$.
7. Виокремлюється кожний розряд b_i числа b за наступною схемою:
   $b_1 = b$ & 01; $b_2 = b$ & 02; $b_3 = b$ & 04; $b_4 = b$ & 010; $b_5 = b$ & 020; $b_6 = b$ & 040; $b_7 = b$ & 0100;
   $b_8 = b$ & 0200; $b_9 = b$ & 0400; $b_{10} = b$ & 01000; $b_{11} = b$ & 02000; $b_{12} = b$ & 04000;
   $b_{13} = b$ & 010000; $b_{14} = b$ & 020000; $b_{15} = b$ & 040000; $b_{16} = b$ & 0100000; $b_{17} = b$ & 0200000;
   $b_{18} = b$ & 0400000; $b_{19} = b$ & 01000000; $b_{20} = b$ & 02000000; $b_{21} = b$ & 04000000;
   $b_{22} = b$ & 010000000; $b_{23} = b$ & 020000000; $b_{24} = b$ & 040000000; $b_{25} = b$ & 0100000000;
   $b_{26} = b$ & 0200000000; $b_{27} = b$ & 0400000000; $b_{28} = b$ & 01000000000; $b_{29} = b$ & 02000000000; $b_{30} = b$ & 04000000000; $b_{31} = b$ & 010000000000; $b_{32} = b$ & 020000000000,
   де & - операція арифметичного «**І**».
8. Виконується циклічне заміщення $n + 1$ розрядів числа b за схемою:
   $k = b_{n+1}$, $b_{n+1} = b_n$, … , $b_2 = b_1$, $b_1 = k$.
9. Зашифрованим є зображення після кроків 5 – 8.

10. Всі отримані числа записуються в матрицю, яка є матрицею інтенсивностей пікселів зашифрованого зображення

$$V = \begin{pmatrix} v_{1,1} & \dots & v_{1,l} \\ \dots & \dots & \dots \\ v_{h,1} & \dots & v_{h,l} \end{pmatrix}$$

Дешифрування по двох рядках матриці зображення.

Дешифрування проводиться при заданих числах $e < \varphi(N)$ і d, $N = P*Q$, $\varphi(N) = (P - 1)(Q - 1)$.

1. Для i – ого рядка матриці V, $1 \le i \le l$, вибирається число $m \equiv (i + P) \ (\mathrm{mod}\ 32)$, і будуються числа $A \equiv m^e \ (\mathrm{mod}\ N)$, $X = i*A*P$.
2. Для $i+1$ – ого рядка матриці, $1 \le i \le l$, вибирається число $m \equiv (i + Q) \ (\mathrm{mod}\ 32)$, і будуються числа $B \equiv m^d \ (\mathrm{mod}\ N)$, $Y = i*B*Q$.
3. Виокремлюється кожний розряд a_i числа a за схемою:
   $a_1 = a$ & 01; $a_2 = a$ & 02; $a_3 = a$ & 04; $a_4 = a$ & 010; $a_5 = a$ & 020; $a_6 = a$ & 040;
   $a_7 = a$ & 0100; $a_8 = a$ & 0200; $a_9 = a$ & 0400; $a_{10} = a$ & 01000; $a_{11} = a$ & 02000;
   $a_{12} = a$ & 04000; $a_{13} = a$ & 010000; $a_{14} = a$ & 020000; $a_{15} = a$ & 040000; $a_{16} = a$ & 0100000;

$a_{17} = a$ & 0200000; $a_{18} = a$ & 0400000; $a_{19} = a$ & 01000000; $a_{20} = a$ & 02000000;
$a_{21} = a$ & 04000000; $a_{22} = a$ & 010000000; $a_{23} = a$ & 020000000; $a_{24} = a$ & 040000000;
$a_{25} = a$ & 0100000000; $a_{26} = a$ & 0200000000; $a_{27} = a$ & 0400000000; $a_{28} = a$ & 01000000000; $a_{29} = a$ & 02000000000; $a_{30} = a$ & 04000000000; $a_{31} = a$ & 010000000000;
$a_{32} = a$ & 020000000000, де & - операція арифметичного «**I**».

4. Виконується циклічне заміщення $m + 1$ розрядів числа a за схемою:
$k = a_{m+1}$, $a_{m+1} = a_m$, … , $a_2 = a_1$, $a_1 = k$.
5. З використанням бінарної операції ^ - порозрядного виключеного «**АБО**» будується число
$s_{i,j} = a \wedge X$.
6. Виокремлюється кожний розряд b_i числа b за наступною схемою:
$b_1 = b$ & 01; $b_2 = b$ & 02; $b_3 = b$ & 04; $b_4 = b$ & 010; $b_5 = b$ & 020; $b_6 = b$ & 040; $b_7 = b$ & 0100;
$b_8 = b$ & 0200; $b_9 = b$ & 0400; $b_{10} = b$ & 01000; $b_{11} = b$ & 02000; $b_{12} = b$ & 04000;
$b_{13} = b$ & 010000; $b_{14} = b$ & 020000; $b_{15} = b$ & 040000; $b_{16} = b$ & 0100000; $b_{17} = b$ & 0200000;
$b_{18} = b$ & 0400000; $b_{19} = b$ & 01000000; $b_{20} = b$ & 02000000; $b_{21} = b$ & 04000000;
$b_{22} = b$ & 010000000; $b_{23} = b$ & 020000000; $b_{24} = b$ & 040000000; $b_{25} = b$ & 0100000000;
$b_{26} = b$ & 0200000000; $b_{27} = b$ & 0400000000; $b_{28} = b$ & 01000000000; $b_{29} = b$ & 02000000000; $b_{30} = b$ & 04000000000; $b_{31} = b$ & 010000000000; $b_{32} = b$ & 020000000000,
де & - операція арифметичного «**I**».

7. Виконується циклічне заміщення $m + 1$ розрядів числа b за схемою:
$k = b_{m+1}$, $b_{m+1} = b_m$, … , $b_2 = b_1$, $b_1 = k$.
8. З використанням бінарної операції ^ - порозрядного виключеного «АБО» - будується число $s_{i+1,j} = b \wedge Y$.

Дешифрованим є зображення після кроків 5 – 8.

Результати наведені на Рис.1. – 3. при $P = 53, Q = 83$.

Рис.*1. Початкове зображення*

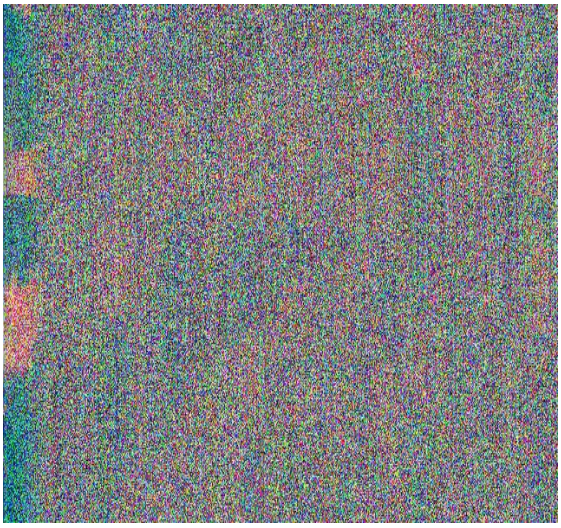

Рис.2. Зашифроване зображення

Рис.3. Дешифроване зображення

Шифрування по одному рядку матриці зображення.

Нехай P, Q - пара довільних простих чисел і $N = P * Q$, $\varphi(N) = (P - 1)(Q - 1)$. Шифрування відбувається поелементно з використанням наступного перетворення елементів матриці S інтенсивностей пікселів:

1. Випадково вибирається натуральне число $e < \varphi(N)$ і знаходиться таке натуральне d, що виконується конгруенція $ed \equiv 1 (\mathrm{mod}\ \varphi(N))$.
2. Якщо $i \equiv 0 (\mathrm{mod}\ 2)$, $1 \le i \le l$, то випадково вибирається число $m \equiv (i + P) (\mathrm{mod}\ 31)+1$, і будуються числа $B \equiv m^e (\mathrm{mod}\ N)$, $X = i*B*P$.
3. Якщо $i \equiv 1 (\mathrm{mod}\ 2)$, $1 \le i \le l$, то випадково вибирається число $m \equiv (i + Q) (\mathrm{mod}\ 31)+1$, і будуються числа $B \equiv m^d (\mathrm{mod}\ N)$, $X = i*B*Q$.
4. З використанням бінарної операції ^ - порозрядного виключеного «**АБО**» - будується число $a = s_{i,j} \wedge X$.
5. Виокремлюється кожний розряд a_i числа a за наступною схемою:

   a_1= a & 01; $a_2 = a$ & 02; $a_3 = a$ & 04; $a_4 = a$ & 010; $a_5 = a$ & 020; $a_6 = a$ & 040;
   $a_7 = a$ & 0100; $a_8 = a$ & 0200; $a_9 = a$ & 0400; $a_{10} = a$ & 01000; $a_{11} = a$ & 02000;
   $a_{12} = a$ & 04000; $a_{13} = a$ & 010000; $a_{14} = a$ & 020000; $a_{15} = a$ & 040000; $a_{16} = a$ & 0100000;
   $a_{17} = a$ & 0200000; $a_{18} = a$ & 0400000; $a_{19} = a$ & 01000000; $a_{20} = a$ & 02000000;
   $a_{21} = a$ & 04000000; $a_{22} = a$ & 010000000; $a_{23} = a$ & 020000000; $a_{24} = a$ & 040000000;
   $a_{25} = a$ & 0100000000; $a_{26} = a$ & 0200000000; $a_{27} = a$ & 0400000000; $a_{28} = a$ & 01000000000; $a_{29} = a$ & 02000000000; $a_{30} = a$ & 04000000000; $a_{31} = a$ & 010000000000;
   $a_{32} = a$ & 020000000000, де & - операція арифметичного «**І**».
6. Виконується циклічне заміщення $m + 1$ розрядів числа a за схемою:
   $k = a_{m+1}$, $a_{m+1} = a_m$, … , $a_2 = a_1$, $a_1 = k$.
7. Зашифрованим є зображення після 5 – го кроку.

8. Всі отримані числа записуються в матрицю, яка є матрицею інтенсивностей пікселів зашифрованого зображення

$$V = \begin{pmatrix} b_{1,1} & \dots & b_{1,l} \\ \dots & \dots & \dots \\ b_{h,1} & \dots & b_{h,l} \end{pmatrix}$$

Дешифрування по одному рядку матриці зображення.

Дешифрування проводиться при заданих числах $e < \varphi(N)$ і d, $N = P * Q$, $\varphi(N) = (P - 1)(Q - 1)$.

1. Якщо $i \equiv 0 (\mathrm{mod}\ 2)$, $1 \le i \le l$, то будується число $m \equiv B^d (\mathrm{mod}\ N)$ і число $X = i*B*P$.
2. Якщо $i \equiv 1 (\mathrm{mod}\ 2)$, $1 \le i \le l$, то будується число $m \equiv B^e (\mathrm{mod}\ N)$ і число $X = i*B*Q$.
3. Виокремлюється кожний розряд a_i числа a наступним чином:
   a_1= a & 01; $a_2 = a$ & 02; $a_3 = a$ & 04; $a_4 = a$ & 010; $a_5 = a$ & 020; $a_6 = a$ & 040;
   $a_7 = a$ & 0100; $a_8 = a$ & 0200; $a_9 = a$ & 0400; $a_{10} = a$ & 01000; $a_{11} = a$ & 02000;
   $a_{12} = a$ & 04000; $a_{13} = a$ & 010000; $a_{14} = a$ & 020000; $a_{15} = a$ & 040000; $a_{16} = a$ & 0100000;
   $a_{17} = a$ & 0200000; $a_{18} = a$ & 0400000; $a_{19} = a$ & 01000000; $a_{20} = a$ & 02000000;
   $a_{21} = a$ & 04000000; $a_{22} = a$ & 010000000; $a_{23} = a$ & 020000000; $a_{24} = a$ & 040000000;
   a_{25} = a & 0100000000; $a_{26} = a$ & 0200000000; $a_{27} = a$ & 0400000000; $a_{28} = a$ & 01000000000; $a_{29} = a$ & 02000000000; $a_{30} = a$ & 04000000000; $a_{31} = a$ & 010000000000;
   $a_{32} = a$ & 020000000000,
   де & - операція арифметичного «**І**».
4. Виконується циклічне заміщення $m + 1$ розрядів числа a за схемою:
   $k = a_{m+1}$, $a_{m+1} = a_m$, … , $a_2 = a_1$, $a_1 = k$.
5. З використанням бінарної операції ^ - порозрядного виключеного «**АБО**» - будується число $s_{i,j} = a \wedge X$.
6. Дешифрованим є зображення після 5 – го кроку.

Результати наведені на Рис.4 – 6 при $P = 127, Q = 53$.

Рис.4. Початкове зображення

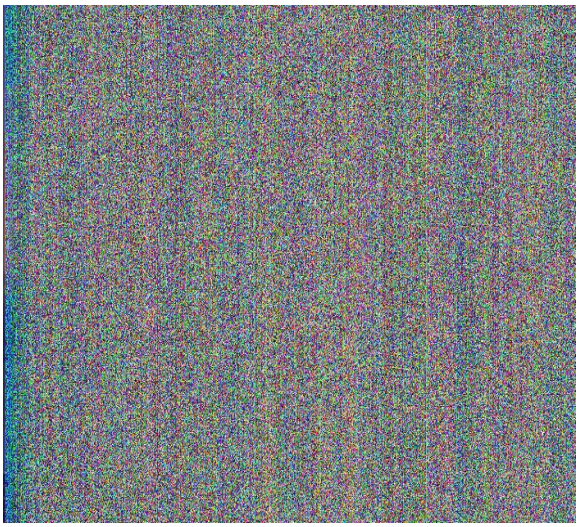

Рис.5. Зашифроване зображення

Рис.6. Дешифроване зображення

5. Висновки

Візуальним порівнянням зашифрованих зображень можна встановити, що шифрування з використанням матриці інтенсивностей пікселів зображення незначно відрізняються при різних значеннях простих чисел P і Q. Контури в обох зашифрованих зображеннях відсутні. Запропоновані модифікації застосовні до будь-якого типу зображень, але найбільші переваги досягаються при використанні зображень з чітко виокремленими контурами. Описаний алгоритм може бути використаний при необхідності передачі зашифрованих графічних зображень.

Візуально видно, що незначно відрізняються вхідні і дешифровані зображення, що означає, що використання запропонованого алгоритму не погіршує якості зображення. Але за ситуації існування певних вимог до критеріїв якості, зазвичай необхідне певне число спроб підбору таких простих чисел P і Q та чисел e і d у конгруенції $ed \equiv 1 \pmod{\varphi(N)}$, $N = P * Q$, щоб заданих критеріїв досягнення якості вхідного і дешифрованого зображення досягнути.

Числовими експериментами з різними кольоровими зображеннями встановлено, що запропонована модифікація має перевагу – підвищує криптографічну стійкість алгоритму RSA .

Література

[1] Michael Vollmer, Klaus-Peter Mollmann, Fundamentals of Infrared Thermal Imaging, Infrared Thermal Imaging, 10.1002 9783527693306, (1-106), (2017), https://www.wiley.com/enus/Infrared+Thermal+Imaging:+Fundamentals,+Research+and+Applications,+2nd+Edition-p-9783527413515

[2] B. Usmonov, O. Evsutin, A. Iskhakov, A. Shelupanov, A. Iskhakova, R. Meshcheryakov, (2017, November). The cybersecurity in development of IoT embedded technologies. In 2017 International Conference on Information Science and Communications Technologies (ICISCT) IEEE, pp. 1-4. DOI: 10.1109/ICISCT.2017.8188589.
[3] D. Wagh, H. Fadewar, & G. Shinde, (2020). Biometric Finger Vein Recognition Methods for Authentication. In Computing in Engineering and Technology pp. 45-53. DOI: 10.1007/978-981-32-9515-5-5.
[4] P. Chanukya, T. Thivakaran, (2020). Multimodal biometric cryptosystem for human authentication using fingerprint and ear. Multimedia Tools and Applications, 79(1-2), pp. 659-673. DOI: 10.1007/s11042-019-08123-w.
[5] L.Valechha, H. Valecha, V. Ahuja, T. Chawla, & S. Sengupta, (2020). Orisyncrasy - An Ear Biometrics on the Fly Using Gabor Filter. In Advances in Data Sciences, Security and Applications, pp. 457-466. DOI: 10.1007/978-981-15-0372-6-37.
[6] J. Yang, L. Liu, T. Jiang, Y. Fan, (2003). A modified Gabor filter design method for fingerprint image enhancement. Pattern Recognition Letters, 24(12), pp. 1805-1817. DOI: 10.1016/S0167-8655(03)00005-9.
[7] Majid Rabbani, Rajan Joshi. "*An overview of the JPEG2000 still image compression standard*" , Eastman Kodak Company, Rochester, NY 14650, USA, Signal Processing: Image Communication. – 2002. – Vol. 17. – P. 3–48, https://scirp.org/reference/referencespapers.aspx?referenceid=727652
[8] A. Kovalchuk, I. Izonin, C. Strauss, M. Podavalkina, N. Lotoshynska, N. Kustra. "*Image encryption and decryption schemes using linear and quadratic fractal algorithms and their systems*", CEUR Workshop Proceedings, Vol. 2533, 2019, pp. 139-150. https://doi.org/10.23939/istcmtm2020.04.025
[9] A. Kovalchuk, I. Izonin, Gregush Ml, M., N. Lotoshyiiska, "*An approach towards image encryption and decryption using quaternary fractional-linear operations*", Procedia Computer Science, Vol. 160, 2019, pp. 491-496. Conference Paper (Open Access), DOI : 10.1016 /j.procs. 2019.11.059.
[10] S. X. Liao and M. Pawlak *On image analysis by moments* , IEEE Transaction on Pattern Analysis and Machine Intelligence. – 1996. – 18, No 3. – P. 254–266, https://ieeexplore.ieee.org/document/485554
[11] E. M. Haacke, R.W. Brown, M.R. Thompson and R. Vencatesan. *Magnetic Resonanse Imagin: Physical Principles and Sequence Design.* John Wiley & Sons, New York, 1999, https://www.wiley.com/ensg/Magnetic+Resonance+Imaging:+Physical+Principles+and+Sequence+Design,+2nd+Edition-p-9780471720850
[12] J. T. Kajiya. The rendering equation. *Computer Graphics,* 20: 143-150, 1986, https://dl.acm.org/doi/10.1145/15886.15902
[13] M. Sarfraz. *Introductory Chapter: On Digital Image Processing*. 2020, DOI: 10.5772 intechopen.92060, https://www.intechopen.com/chapters/71817
[14] Ehsan Samei, Donald J Peck, Projection X-ray Imaging, Hendee's Physics of Medical Imaging, 10.1002 9781118671016, (217-242), (2019), https://onlinelibrary.wiley.com/doi/10.1002/9781118671016.ch6
[15] B. Schneier. *Applied Cryptography: Protocols, Algorithms and Source Code in C*, M.: Triumf, 2003, 815c. https://www.amazon.com/Applied-Cryptography-Protocols-Algorithms-Source/dp
[16] B. Jane. *Digital Image Processing*. Springer–Verlag Berlin Heidelberg, 2005, pp.583, https://www.amazon.com/Digital-Image-Processing-Algorithms-Applications/dp/3540592989
[17] R. C. Gonzales and R.E. Woods. *Digital image processing.* Prentice Hall, Upper Saddle River, NJ, 2ndedn,2002. https://www.amazon.com/Digital-Image-Processing-Algorithms-Applications/dp
[18] I. Tsmots, O. Riznyk, V. Rabyk, Y. Kynash, N. Kustra, M. Logoid, (2020) Implementation of FPGA-Based Barker's-Like Codes. In: Lytvynenko V., Babichev S., Wójcik W., Vynokurova O., Vyshemyrskaya S.,Radetskaya S. (eds) "*Lecture Notes in Computational Intelligence and Decision Making*". ISDMCI 2019. Advances in Intelligent Systems and Computing, vol 1020. Springer, Cham. DOI: 10.1007/978-3-030-26474-1_15.
[19] Rafael C. Gonzalez, Richard E. Woods, "*Digital Image Processing*", published by Pearson Education,Inc,Publishing as Prentice Hall, 2002, http://sdeuoc.ac.in /sites/default /files/sde_videos /Digital%20Image%20Processing%203rd%20ed.%20-%20R.%20Gonzalez%2C%20R.%20Woods-ilovepdf-compressed.pdf
[20] B. Girod "*The information theoretical significance of spatial and temporal masking in video signals*", Proc. of the SPIE Symposium on Electronic Imaging.1989.–Vol. 1077.– P.178–187, https://typeset.io/papers/the-information-theoretical-significance-of-spatial-and-2bas6i0mgw.