УДК 681.325

В.Г. Красиленко, Ю.А. Флавицька
Вінницький соціально-економічний інститут університету "Україна",
кафедра інформаційних технологій

МОДЕЛЮВАННЯ МАТРИЧНИХ АЛГОРИТМІВ КРИПТОГРАФІЧНОГО ЗАХИСТУ

Описано модифікований багатокроковий матричний афінний шифр для криптозастосувань з метою обробки двовимірних масивів та кольорових і некольорових зображень.

It's presented generalized multistep-by-step matrix affine cipher for encoding and decryption two-dimensional files, colour and not colour images.

Вступ. Існує багато криптографічних алгоритмів та протоколів, що використовуються для захисту інформації [1, 2], але більшість із них орієнтовані на послідовну обробку скалярних цифрових даних. Водночас в мережі Інтернет, в інших локальних та глобальних мережах, системах зв'язку, телекомунікацій поширені при передачі, обробці двовимірні масиви та зображення. Враховуючи, що при послідовній обробці та кодуванні чи шифруванні скалярних даних використовуються одні і ті самі ключі, це робить такі послідовні алгоритми не дуже стійкими. Тому доцільною є модифікація відомих алгоритмів та протоколів для криптозастосувань на матричний випадок, коли дані, що шифруються і дешифруються, представляються у вигляді багатовимірних, наприклад, матричних масивів.

Аналіз останніх досліджень, публікацій. Відомі результати моделювання модифікованого алгоритму створення 2-D ключа для криптографічних застосувань [3], в основу якого покладено протокол та математичні моделі протоколу Діффі–Хеллмана. Ці результати підтвердили, що можливо розширити функціональні можливості та стійкість такого матричного протоколу, при цьому всі обчислювальні процедури виконуються над матрицями. У симетричних системах шифрування двом користувачам, які бажають встановити безпечний обмін інформацією, необхідно спочатку на основі запропонованого модифікованого алгоритму встановити спільний безпечний ключ. Цей ключ, представлений у вигляді матриці, зображення або сукупності зображень чи тензора, можна використати для подальшого шифрування і дешифрування, оскільки обидві сторони отримують однаковий ключ. У роботі [4] розроблені нові алгоритми шифрування та приховування інформації при факсимільній передачі документів, які реалізовані у вигляді програмного забезпечення. Ці алгоритми є стійкими до впливу завад та різних спотворень, що виникають під час передачі документів факсом, та вирішують проблему декодування тексту з можливим великим рівнем шумів та геометричними спотвореннями. Запропонований у [5] модифікований матричний афінний багатокроковий шифр має порівняно з традиційним афінним асиметричним шифром переваги. Переваги та підтвердження роботи такого шифру показані у вищезгаданій роботі шляхом застосування двох програмних інструментів. Але детальніше моделювання та перевірку дії таких алгоритмів не здійснено.

Постановка задачі. Тому метою роботи є проведення ряду модельних експериментів у програмних середовищах Mathcad Professional та Microsoft Excel.

Теоретичні основи та результати. Суть узагальнених матричних афінних багатокрокових шифрів, що належать до асиметричних систем та алгоритмів, полягає у такому. Вибирають два матричні ключі A та S у вигляді матриць відповідної розмірності (див. рис. 1), елементи яких вибираються з діапазону 1÷(n-1), де n – просте велике число. Ці ключі використовуємо для

шифрування. Крім того, вводиться параметр ß, який задає кількість кроків. Для знаходження двох матричних ключів AD, SD дешифрування, потрібно для кожного елемента $a_{i,j}$ матриці A знайти обернене за модулем n число $ad_{i,j}$ та для елемента $s_{i,j}$ обчислити значення елемента $sd_{i,j}$ матриці SDза таким виразом:

$$sd_{i,j}=(-a^{-1}_{i,j} * s_{i,j}) \bmod n. \quad (1)$$

Тоді процеси кодування та декодування для матричного повідомлення M та криптограми C виражаються такими матричними формулами:

$$C = (M\Theta A+S)^{\beta} \bmod N; \quad (2)$$

$$M = (C\Theta AD+SD)^{\beta} \bmod N, \quad (3)$$

де символ Θ означає поелементне множення матриць, а піднесення до степеня означає поелементне множення та додавання матриць β разів, а (mod N) означає поелементне взяття за модулем n всіх елементів матриці. Наведені вище формули спрощені, розгорнутий вигляд цих формул подано нижче:

$$C = \underbrace{(M\Theta A + S)\Theta A + S)\Theta A + S)... + S)}_{\beta} \bmod N; \quad (4)$$

$$M = \underbrace{(C\Theta AD + SD)\Theta AD + SD)\Theta AD + SD)... + SD)}_{\beta} \bmod N. \quad (5)$$

Ці формули легко перетворити, що дасть змогу звести та спростити відповідні обчислювальні процедури та виконувати їх покроково. Результати моделювання такого матричного шифру в Mathcad Professional показано на рис. 2. Для моделювання вибрано зображення розмірністю 128*128 пікселів, яке попередньо за динамічним діапазоном яскравостей зменшено вдвічі, хоча на рисунку зображено без динамічного перетворення (тобто нами вибрано n=127). Для моделювання ми вибрали ключ A та S у вигляді матриць з однаковими елементами, а тому у формулах, що використовувались, матриці множаться на скаляри. На рис. 2 показані матриці-криптограми, отримані відповідно після першого (C1), другого (C2) та третього (C3) кроків шифрувань при β=3, та матриці, (M3, M2, M1), отримані після першого, другого та третього кроків дешифрувань.

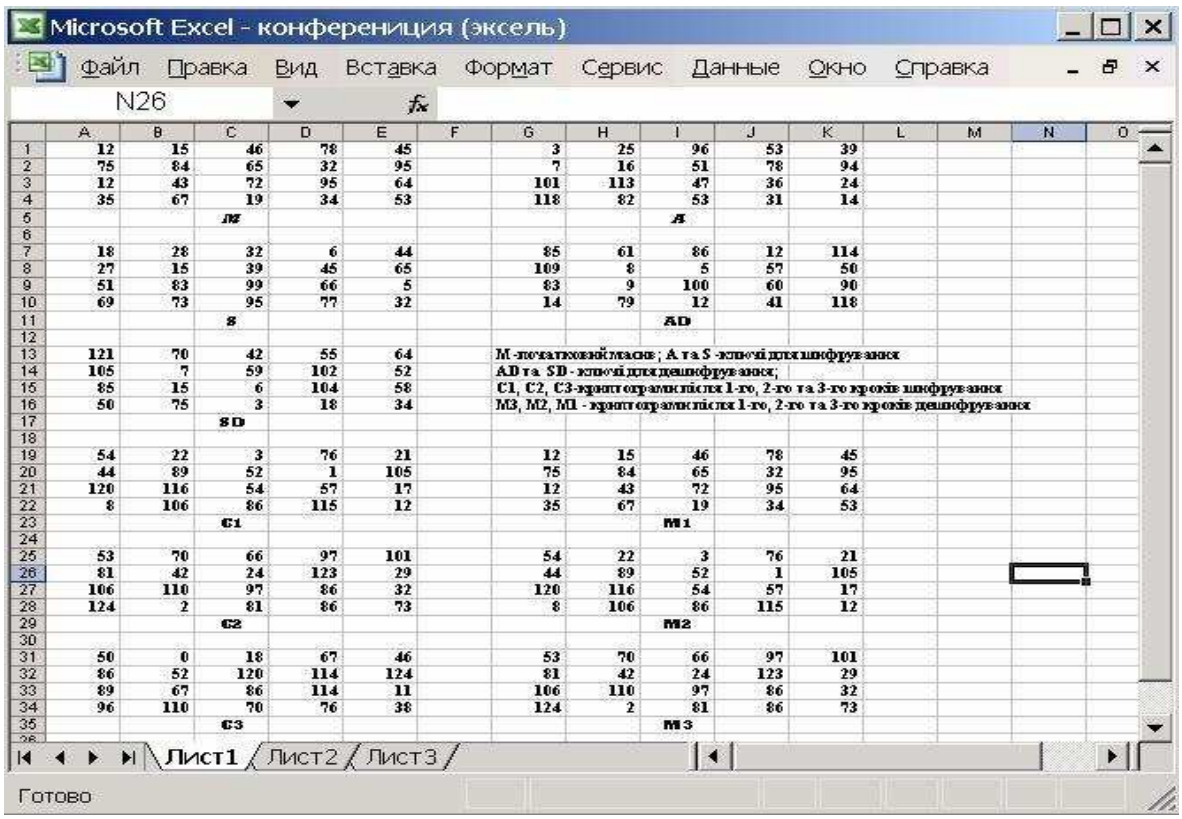

Рис. 1. Результати моделювання матричного афінного багатокрокового шифру в Microsoft Excel

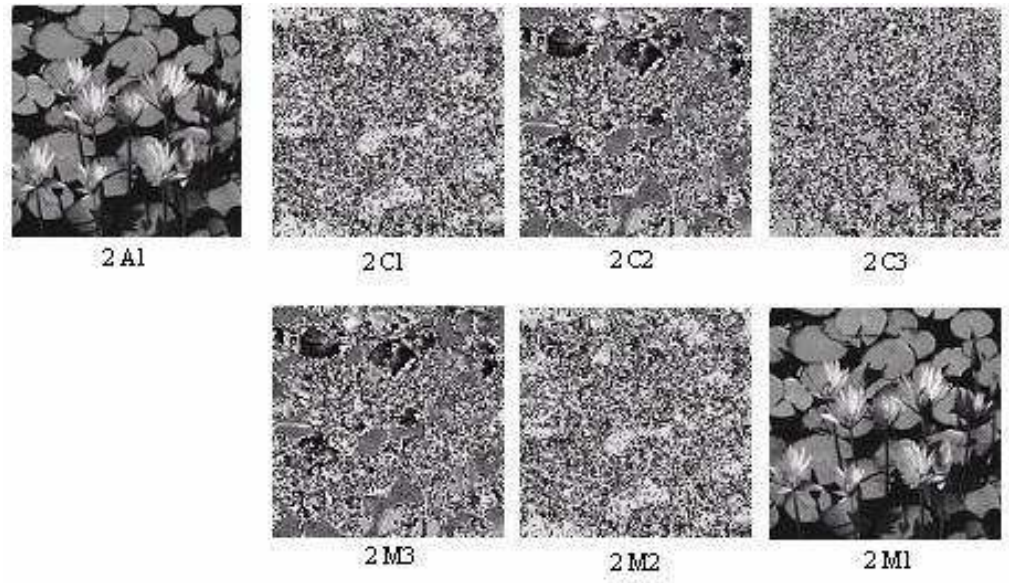

Рис. 2. Результати моделювання матричного афінного багатокрокового шифру в Mathcad

На рис. 3 наведено результати моделювання, що підтверджують обмеженість використання як ключів не матриць, а скалярів. Так, на цьому рисунку на вхідному зображенні показано секретне повідомлення, що після першого, другого та третього кроків шифрувань не приховується, а залишається відкритим для сприйняття.

Також видно, що при зворотньому дешифруванні ми повністю відновлюємо початкове зображення, але усі криптозображення після відповідних кроків зовсім не приховують секретних даних.

А тому лише перехід на матричний випадок ключів (двох, а саме для шифрування KL та SL, та двох ключів KDL та SDL для дешифрування), що показані на рис. 4, дають змогу вхідне повідомлення з секретними даними (матриця ML) перетворити на криптограмму CL, в якій, як видно з отриманих зображень, можна приховати секретне повідомлення. На цьому рисунку також показані формули, які відтворюють один крок шифрування та дешифрування. У нижній частині рис. 4 зображено процес дешифрування у вигляді послідовності малюнків, які підтверджують, що з отриманої криптограми CL (зображення зліва) та двох ключів дешифрування у вигляді матриць KDL та SDL отримуємо зображення-матрицю VL, яка повністю відповідає вхідному масиву ML.

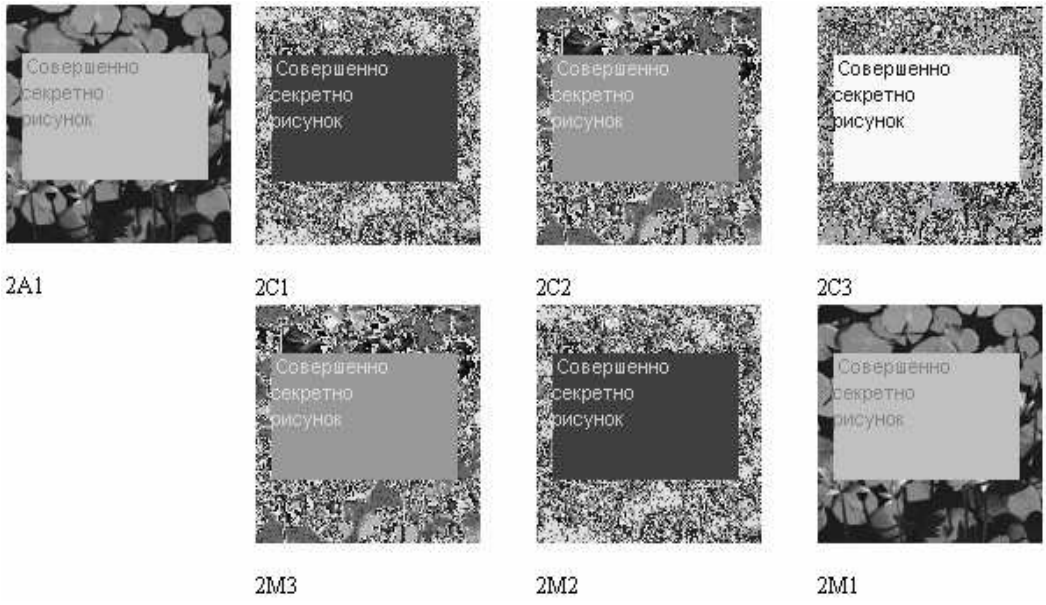

Рис. 3. Результати моделювання матричного афінного багатокрокового шифру з використанням скалярів як ключів

З наведених результатів видно, що навіть одного кроку шифрування і ключів, які мають деяку періодичну структуру, все-таки достатньо для приховування зображень з секретними текстовими фрагментами, що було неможливим при використанні як ключів скалярів.

Отже, результати модельних експериментів за допомогою двох програмних інструментів повністю підтверджують, що саме застосування повністю матричного типу ключів дає змогу приховувати інформацію незалежно від її вигляду та кількості градації яскровостей. Якщо використовувати як ключі випадкові згенеровані зображення, а не зображення з періодичною структурою, то стійкість таких багатокрокових матричних афінних шифрів зростає, і розширюються їх функціональні можливості. За відомими правилами та моделями в принципі відносно легко створити ключі для дешифрування. Оскільки множина можливих комбінацій ключів з багатоградаційними компонентами і значною розмірністю (128*128 пікселів) є доволі значною і оцінюється величиною для нашого випадку як $(127)^{128*128}$, то це забезпечує достатню стійкість до зламування, наприклад, простою брутальною атакою.

Нами був проведений також модельний експеримент, в якому було перевірено дію запропонованого криптографічного алгоритму при шифруванні та дешифруванні кольорових зображень. В експерименті використовувалось кольорове зображення розмірністю 128 x 128 пікселів з 3-байтним представленням кольору в кожному пікселі (див. рис. 5 a). Для шифрування кольорове зображення розбивається на три основні кольорові складові (R, G, B), до кожної з яких застосовується матричний афінний шифр. У нашому випадку до всіх складових застосовувався один і той самий матричний ключ, хоча може бути використано три різних ключі для кожної складової.

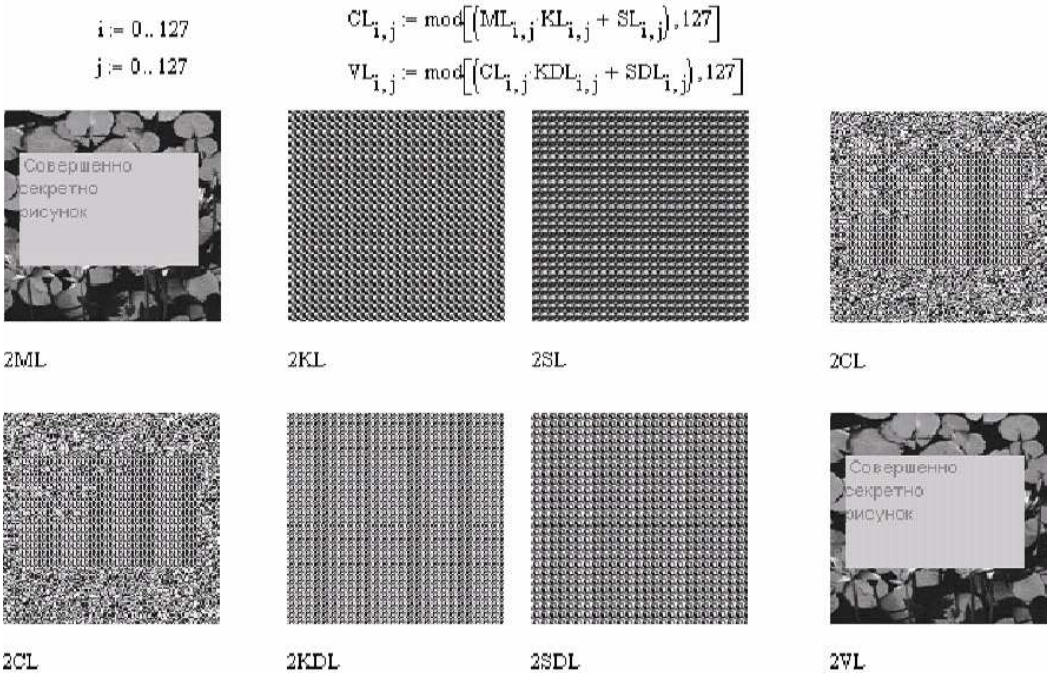

Рис. 4. Моделювання матричного узагальненого багатокрокового афінного шифру за допомогою матриць-ключів

Ми використовували ті самі ключі, що і в попередньому експерименті при роботі з некольоровими зображеннями, а саме матриці KL та SL для шифрування та матриці KDL та SDL для дешифрування. Три відповідних кольорові складові (див. рис. 6, c) отриманої криптограмми в кольоровому форматі (див. рис. 5, b) дають змогу після їх дешифрування покомпонентно отримати відновлені всі три кольорові складові, що показані на рис. 6, d, з яких ми отримуємо дешифроване кольорове зображення, показане на рис. 5, c. Кольорові зображення на рис. 5 при відтворенні статті, що публікується, будуть чорно-білими.

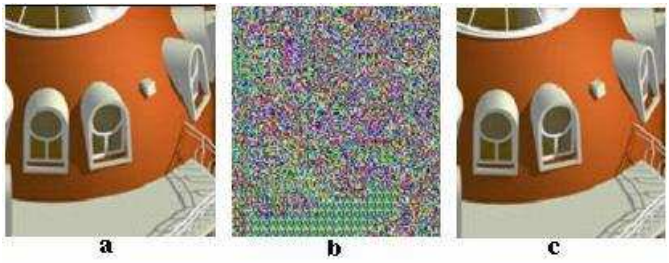

Рис. 5. Результати моделювання матричного алгоритму на кольорових зображеннях: а – вхідне зображення, що шифрується; б – утворена алгоритмом криптограма у вигляді кольорового зображення; с – відновлене з криптограми кольорове зображення

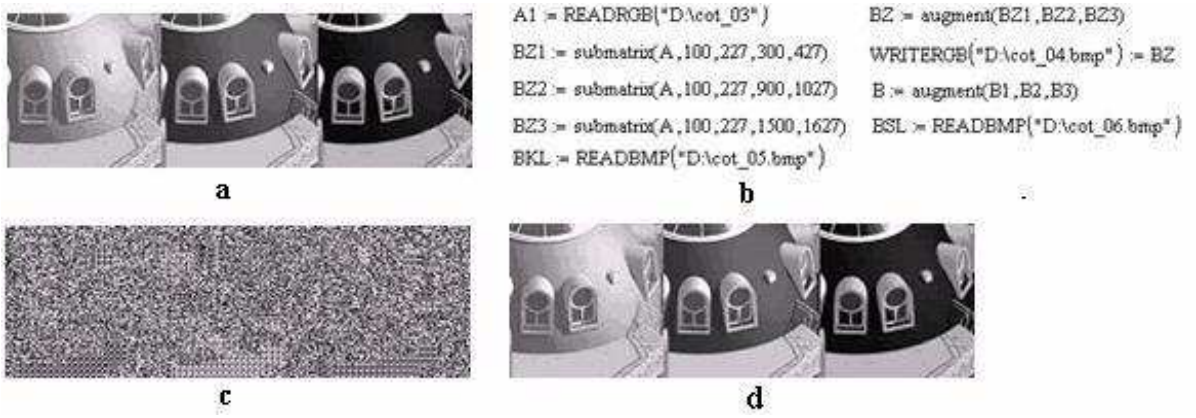

Рис. 6. Пояснення процесів моделювання: а – зображення трьох основних складових (R, G, B) кольорового зображення; b – формули, що були використані для моделювання; с – зображення трьох основних складових криптограми; d – зображення складових (R, G, B) відновленого дешифрованого зображення

Результати моделювання повністю підтвердили правильність гіпотез і переваги модифікованого матричного узагальненого багатокрокового алгоритму.

Висновки. Запропонований модифікований багатокроковий матричний афінний шифр дає змогу використовувати його для криптографічних застосувань при обробці двовимірних масивів та зображень і є стійкішим порівняно з традиційним афінним асиметричним шифром.

1. Ємець В., Мельник А., Попович Р. Сучасна криптографія: Основні поняття. – Л.: БаК, 2003. – 144 с. 2. Хорошко В. О., Чектов А. О. Методи і засоби захисту інформації: Навч. посібник. – К.: Юніор, 2003. – 502 с. 3/ Красиленко В. Г., Нікольський О. І., Лазарєв О.О. Моделювання модифікованого алгоритму створення 2-D ключа в криптографічних застосуваннях // Науково-методичний збірник науково-практичної конференції «Наука і навчальний процес». – Вінниця, 2008. – С. 107–109. 4. Красиленко В.Г., Лазарєв О.О, Огородник К.В. Захист інформації при факсимільному передаванні документів // Збірник наукових праць науково-практичної конференції «Прогресивні інформаційні технології в науці та освіті». – Вінниця, 2007. – С. 167–170. 5 Красиленко В.Г., Бозняк Ю.А, Потєй Ю.А. Матричні алгоритми криптографічного захисту // Науково-методичний збірник науково-практичної конференції "Наука і навчальний процес". – Вінниця, 2008. – С. 99–101.