УДК 004.056.55

В.Г. КРАСИЛЕНКО
Вінницький соціально-економічний інститут університету "Україна"
В.М. ДУБЧАК
Вінницький національний аграрний університет

КРИПТОГРАФІЧНІ ПЕРЕТВОРЕННЯ ЗОБРАЖЕНЬ НА ОСНОВІ МАТРИЧНИХ МОДЕЛЕЙ ПЕРЕСТАНОВОК З МАТРИЧНО-БІТОВОЗРІЗОВОЮ ДЕКОМПОЗИЦІЄЮ ТА ЇХ МОДЕЛЮВАННЯ

*В роботі наводяться результати моделювання матричних моделей криптографічних перетворень зображень з декомпозицією на бітові зрізи та перемішуванням. Показані модельні експерименти зображень 128*128 та 340*610 елементів.*

Ключові слова: Криптографічні перетворення зображень, матричні моделі перестановок, матричний ключ, векторний ключ, матрична бітовозрізова декомпозиція, моделювання.

V.G.KRASILENKO
Vinnitsia Social and Economic Institute of the University " Ukraine "
V.M.DUBCHAK
Vinnytsia National Agrarian University

TRANSFORMATIONS OF IMAGES BASED ON OF MATRIX MODELS OF PERMUTATION WITH MATRIX BIT-PLANE DECOMPOSITION AND THEIR MODELING

Abstract- Designed matrix models of permutations for cryptographic transformations of images are proposed and in Mathcad programmed, monitored and evaluated.

*In the work are given results of modeling of matrix models of cryptographic transformations of images with matrix bit-plane decomposition and mixing. The simulating results for images with 128 * 128 and 340 * 610 pixels are shown.*

The developed matrix models of permutations based on matrix bit-plane decomposition for images cryptographic transformations are shown, that they have high entropic quality criteria, high performance for direct and inverse transformations.

Keywords : Cryptographic transformations, matrix-type model, matrix models of permutations, image, matrix key, vector key, decomposition, bit file cuts.

В епоху електронних комунікацій, інформаційних технологій суттєво зростає доля текстографічних документів (ТГД),що представляються у вигляді цифрових, табличних даних, малюнків, графіків, діаграм, підписів, віз, резолюцій і є по суті 2-D масивами (зображеннями). Часто існує необхідність опрацьовувати та передавати ТГД з конфіденційною чи з обмеженим доступом інформацію, надавати за допомогою електронних комунікацій звітність у податкові та інші державні органи, засвідчувати їх цифровим підписом, тощо. Для таких цілей використовується низка класичних алгоритмів, методів, моделей криптографічних перетворень (КП) інформаційних масивів, зображень та процедур і протоколів формування та обміну ключів [1]. Але більшість з них орієнтовані на послідовну скалярну обробку блоків ТГД, перетворених у цифрові формати. В той же час поява паралельних алгоритмів, а особливо матричних багатопроцесорних засобів, потребує створення і відповідних моделей матричного типу (МТ) [2]. Тому пошук нових матричних моделей та засобів виконання КП зображень є актуальним завданням.

У роботі [3] були розроблені, досліджені і промодельовані матричні алгоритми криптографічного захисту на основі більш узагальнених матричних афінних шифрів, а в [4] продемонстровані їх можливості та переваги при створенні сліпих цифрових підписів на ТГД. Ще більш узагальнені матричні афінно-перестановочні шифри були запропоновані та досліджені в [5]. Матричні моделі перестановок (ММ_П) мають наочну простоту, проте, як показано в [6], КП на їх основі без додаткових операцій не змінюють гістограми зображень чи ТГД. Тому в ній були запропоновані ММ_П з декомпозицією бітових зрізів. Проте вони мають недолік, що полягає в необхідності мати крім матричного ключа (МК) власне перемішування ще два векторних ключа.

Таким чином є необхідною і актуальною спроба подальшої модифікації відомих ММ перестановок для КП зображень з метою їх спрощення та покращення. А перевірка створених моделей шляхом їх моделювання для конкретних ТГД дозволить оцінити показники таких ММ_П та їх особливості і сфери застосувань.

Тому метою даної роботи є створення, моделювання матричних моделей перестановок з матричною бітовозрізовою декомпозицією для КП зображень у програмному середовищі Mathcad та їх верифікація і оцінювання.

Експериментальна частина

Розглянемо сутність математичної моделі з матрично-бітовою декомпозицією (МБД). На рис. 1,2 зображені результати моделювання ММ_П. Відмітимо, що без використання такої декомпозиції гістограми не змінюються, що є свідченням недостатньої криптостійкості, особливо для деяких видів зображень. На рис. 3,4 зображені: зображення А, його гістограма, формули та результати кодування А в бітові розрядні зрізи за допомогою АЦП матричного типу. Результати моделювання процесів криптографічних перетворень показані на рис. 5,6 і свідчать про коректну роботу запропонованого підходу на основі використання

матрично-бітової декомпозиції та матричних моделей перестановок. Експериментальні дані процедур створення необхідних ключів з урахуванням специфіки розглянутого підходу будуть розглянуті нами в подальших роботах.

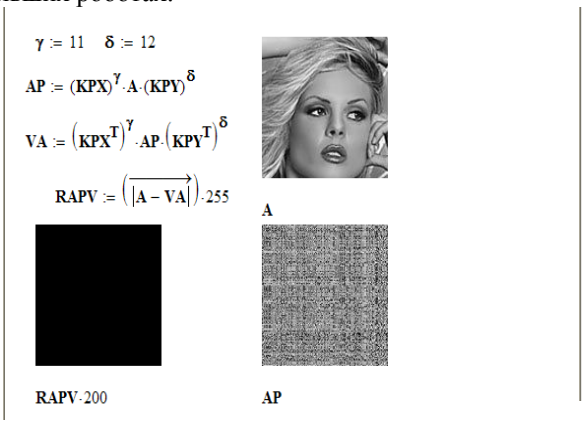


Рис.1. Матрична модель перетворень зображень перестановками (ММ_ПП) та результати моделювання (АР-криптограма, А та VA- явне і відновлене зображення)

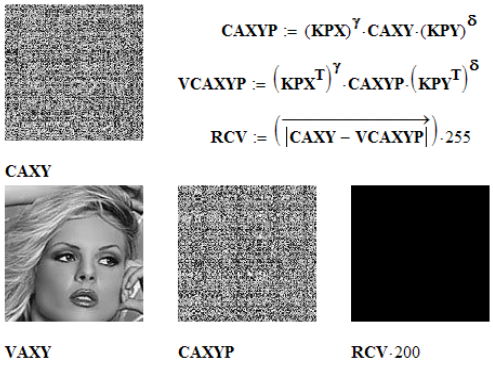


Рис.2. Матрична модель перетворень криптограм перестановками та результати моделювання (CAXYP-нова криптограма, CAXY та VCAXYP – явна і відновлена криптограми у вигляді зображень)

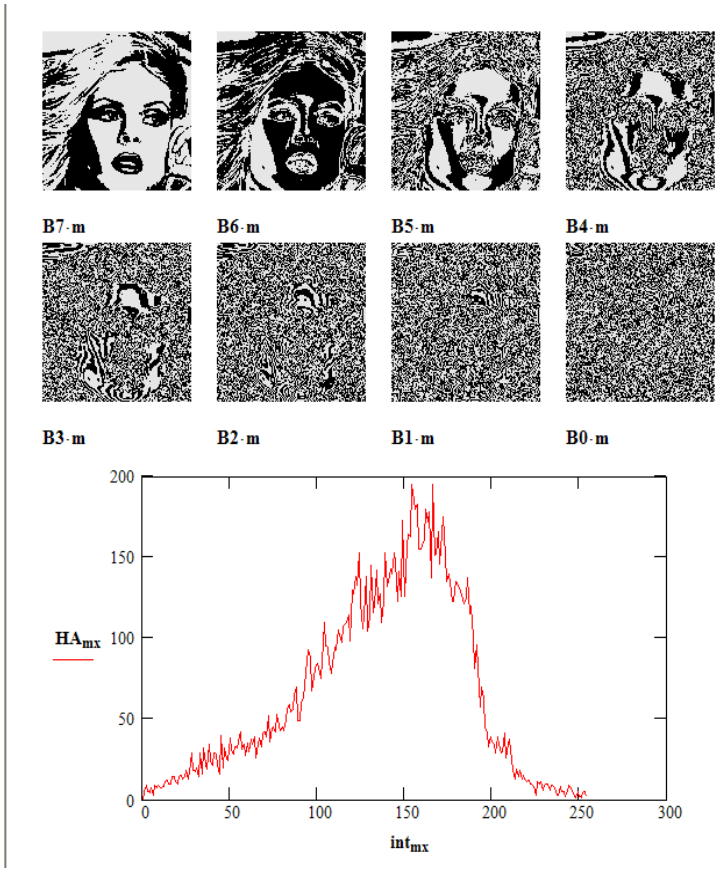


Рис.3. Бітові розрядні зрізи-матриці (B7-B0), утворені матричним АЦ-перетворенням зображення А і його гістограма

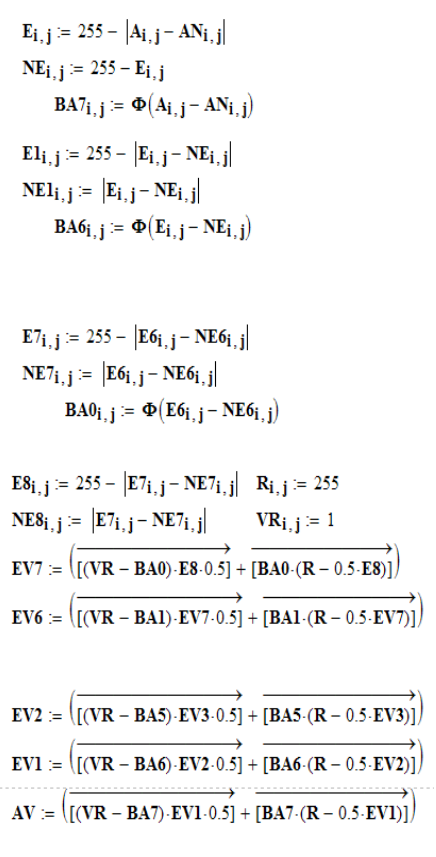


Рис.4. Формули, що використовувались для прямого АЦ та оберненого ЦА перетворень

Результати моделювання КП з МБД та перемішуванням рядків та стовбців матричними ключами, але для іншого зображення зі специфічною гістограмою показані на рис.7,8. Використовуючи як явне зображення А (128*128 ел.), формули для генерування МП - ключів KPX (128*128) та KPY (1024*1024), що показані на рис.7, вісім бітових матричних зрізів С7 – С0 матриці А, показаних на рис.8, та згрупованих у спільну матрицю ASB, ми за допомогою матричної процедури KPX*ASB*KPY формували матрицю C_ASB і новий набір зрізів SPXY7 – SPXY0, а з них криптограму CAXY (дивись рис.8). Матриці KPX та KPY можуть бути у відповідних ступенях. В нашому експерименті, результати якого показані на рис. 7,8, степінь матриці KPX була рівною 5 і визначалась одним додатковим параметром ключем η. За допомогою процедури KPXO*C_ASB*KPYO, де матриці KPXO та KPYO є оберненими (транспонованими KPX та KPY, по суті), з матриці C_ASB, що відповідала криптограмі CAXY, формувалась відновлена матриця ASB_V та VAXY.

$X := 128 \quad Y := 128$

$XP := 128 \quad YP := 128$

$KPX := \left| \begin{array}{l} E_{X-1,Y-1} \leftarrow 0 \\ \text{for } i \in 0..X-1 \\ \quad \left| \begin{array}{l} y \leftarrow \text{round}(\text{rnd}(Y-1)) \\ \text{while } \left(\text{mean}\left(E^{\langle y \rangle}\right) > 0\right) \\ \quad y \leftarrow \text{round}(\text{rnd}(Y-1)) \\ E_{i,y} \leftarrow 1 \end{array} \right. \\ E \end{array} \right.$

$KPY := \left| \begin{array}{l} E_{XP-1,YP-1} \leftarrow 0 \\ \text{for } j \in 0..YP-1 \\ \quad \left| \begin{array}{l} x \leftarrow \text{round}(\text{rnd}(XP-1)) \\ \text{while } \left[\text{mean}\left[\left(E^{T}\right)^{\langle x \rangle}\right] > 0\right] \\ \quad x \leftarrow \text{round}(\text{rnd}(XP-1)) \\ E_{x,j} \leftarrow 1 \end{array} \right. \\ E \end{array} \right.$

$\text{mean}(KPX) \cdot X \cdot Y = 128$

$\text{mean}(KPY) \cdot XP \cdot YP = 128$

$SPXY7 := KPX^{KEYL_7} \cdot B7 \cdot KPY^{KEYP_7}$

$SPXY6 := KPX^{KEYL_6} \cdot B6 \cdot KPY^{KEYP_6}$

$SPXY5 := KPX^{KEYL_5} \cdot B5 \cdot KPY^{KEYP_5}$

$SPXY4 := KPX^{KEYL_4} \cdot B4 \cdot KPY^{KEYP_4}$

$SPXY3 := KPX^{KEYL_3} \cdot B3 \cdot KPY^{KEYP_3}$

$SPXY2 := KPX^{KEYL_2} \cdot B2 \cdot KPY^{KEYP_2}$

$SPXY1 := KPX^{KEYL_1} \cdot B1 \cdot KPY^{KEYP_1}$

$SPXY0 := KPX^{KEYL_0} \cdot B0 \cdot KPY^{KEYP_0}$

$consl := 7 \quad consp := 8 \quad d := 0..7$

$KEYL_d := consl + \text{round}(\text{rnd}(10), 0)$

$KEYP_d := consp + \text{round}(\text{rnd}(10), 0)$

$KEYL^T = (13 \quad 12 \quad 15 \quad 13 \quad 7 \quad 15 \quad 8 \quad 11)$

$KEYP^T = (9 \quad 8 \quad 12 \quad 10 \quad 15 \quad 12 \quad 16 \quad 11)$

$KPXO := KPX^T \quad KPYO := KPY^T$

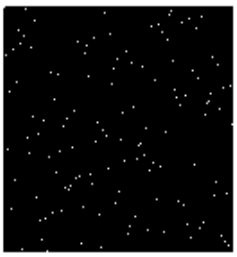
$CAXY := (128 \cdot SPXY7 + 64 \cdot SPXY6 + 32 \cdot SPXY5 + 16 \cdot SPXY4 + 8 \cdot SPXY3 + 4 \cdot SPXY2 + 2 \cdot SPXY1 + SI$

$SVXY7 := KPXO^{KEYL_7} \cdot SPXY7 \cdot KPYO^{KEYP_7}$

$SVXY6 := KPXO^{KEYL_6} \cdot SPXY6 \cdot KPYO^{KEYP_6}$

$SVXY5 := KPXO^{KEYL_5} \cdot SPXY5 \cdot KPYO^{KEYP_5}$

$SVXY4 := KPXO^{KEYL_4} \cdot SPXY4 \cdot KPYO^{KEYP_4}$



$250 \cdot KPXO \qquad 250 \cdot KPYO$

Рис. 5. Формули, що використовувались для створення матриць перестановок KPX (зліва) та KPY (справа), ключів KEYL та KEYP, та реалізації MM_ПП при порозрядній декомпозиції з шифруванням бітових зрізів (B7-B0) для створення проміжних бітових та результуючої криптограми CAXY

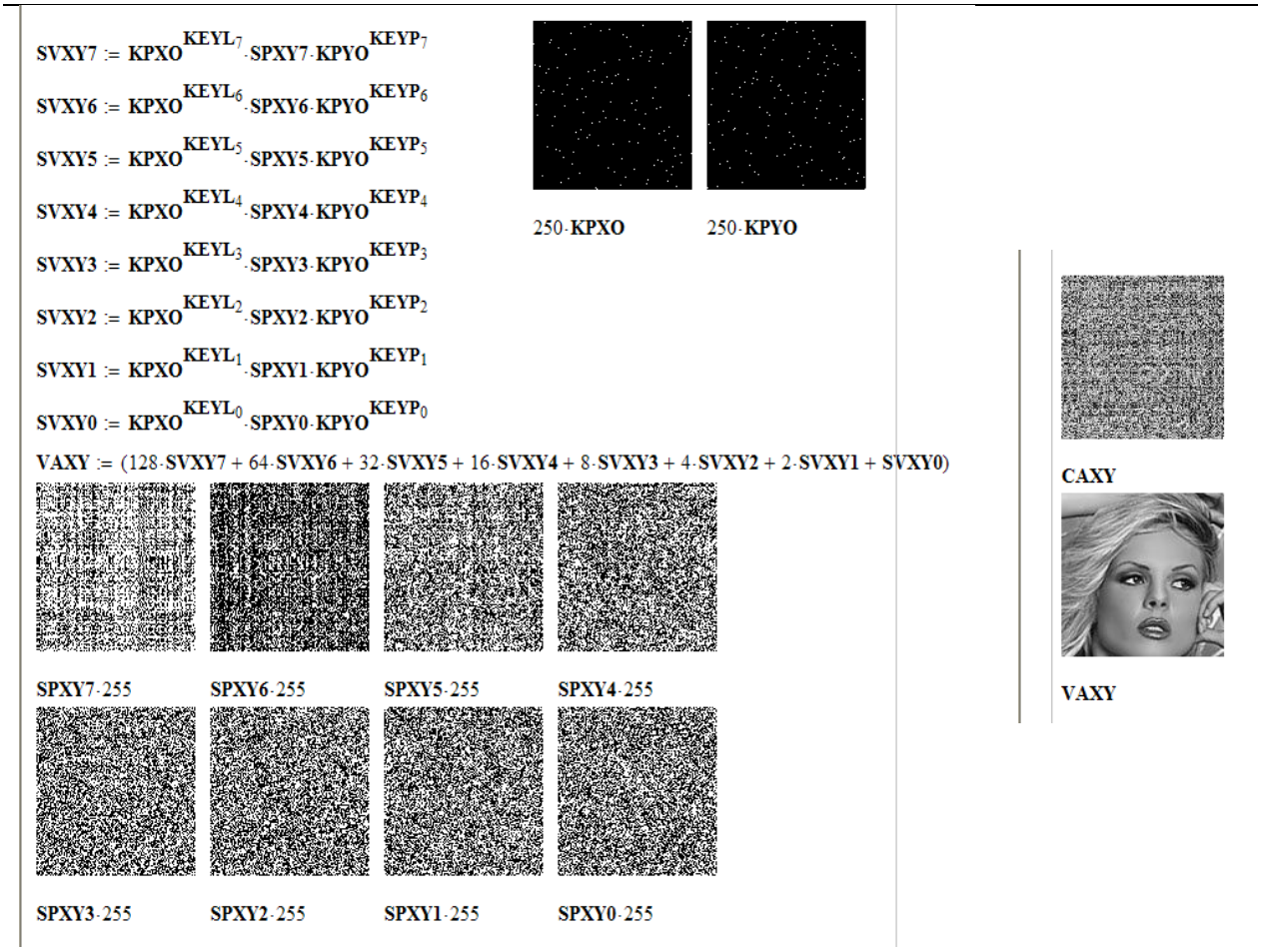


Рис.6. Формули, що використовувались для реалізації ММ_ПП при порозрядній декомпозиції та зворотній процедурі розшифрування бітових зрізів-шифрограм (SPXY7-SPXY0) для створення з відновлених бітових зрізів (SVXY7-SVXY0) відновленого зображення VAXY (з крипи CAXY)

Аналогічно можливо цей же чи подібний йому другий додатковий параметр-ключ використати для піднесення у відповідну степінь і матрицю KPY. Цей другий експеримент відрізняється від першого також тим, що в першому перестановки чи перемішування відбувалося лише для пікселів всередині кожного зрізу, крім того, для таких перестановок для кожного зрізу формувалася своя матриця перестановок, а саме як відповідна степінь базових матриць KPXO та KPYO, при цьому степені визначалися компонентами додаткових векторних ключів KEYL та KEYP. У другому експерименті перемішування здійснювалося для пікселів всієї загальної бітової картини, що була спільною композицією всіх бітових зрізів, тобто перестановки були по суті і між зрізами поряд з внутрішніми перестановками у самих зрізах. Це потребує збільшення розмірності МП-ключів, наприклад, одного із них у 8 разів, зате відпадає необхідність у додаткових векторних ключах, оскільки для збільшення криптостійкості та функціональності для такої модифікації моделі необхідно додатково до матричних ключів лише два скалярних ключі. Ці таємні ключі (скаляри) визначають степені МП-ключів у моделі. Там же на рис. 8 показана відновлена аналогічною процедурою матриця VAXY, що співпадає з A. Це свідчить про коректну роботу запропонованих моделей та їх модифікацій.

Результати моделювання процесів прямого та оберненого криптографічних перетворень у програмному середовищі Mathcad з іншими зображеннями та при використанні різних ключів показані на рис. 9,10,11. Вони свідчать про коректну роботу запропонованого підходу на основі використання матрично-бітової декомпозиції та матричних моделей перестановок. Час шифрування не перевищує хвилин навіть для ТГД формату А4.

Висновки

Проведена серія модельних експериментів розроблених матричних моделей перестановок з матричною бітовозрізовою декомпозицією для криптографічних перетворень зображень та підтверджені ефективність та зручність нових моделей. Розроблені модифікації моделей мають високі ентропійні критерії якості криптоперетворень, підтверджені гістограмним аналізом, високу швидкодію при прямому та оберненому перетвореннях, зручно відображаються та реалізуються матричними процесорами та легко адаптуються при необхідності обробки різноформатних та кольорових зображень.

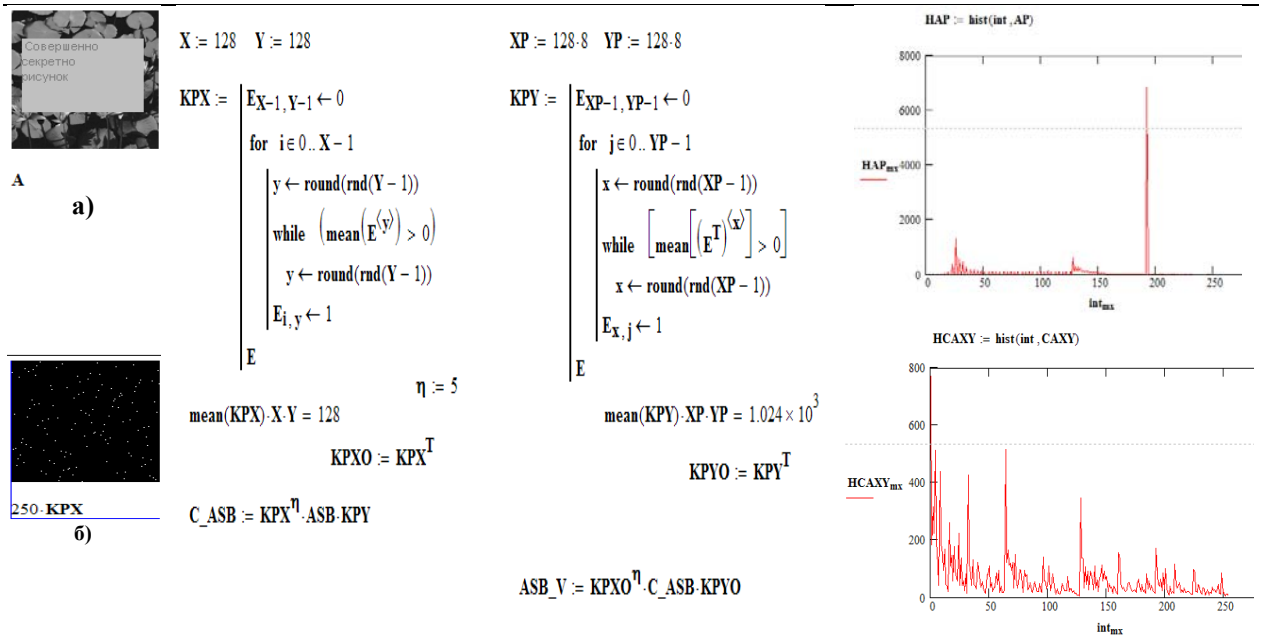


Рис. 7. а) явне зображення A, його гістограма – праворуч зверху, посередині – формули для генерування МП-ключів KPX та KPY, б) зображення ключа KPX, гістограма криптограми CAXY (праворуч знизу).

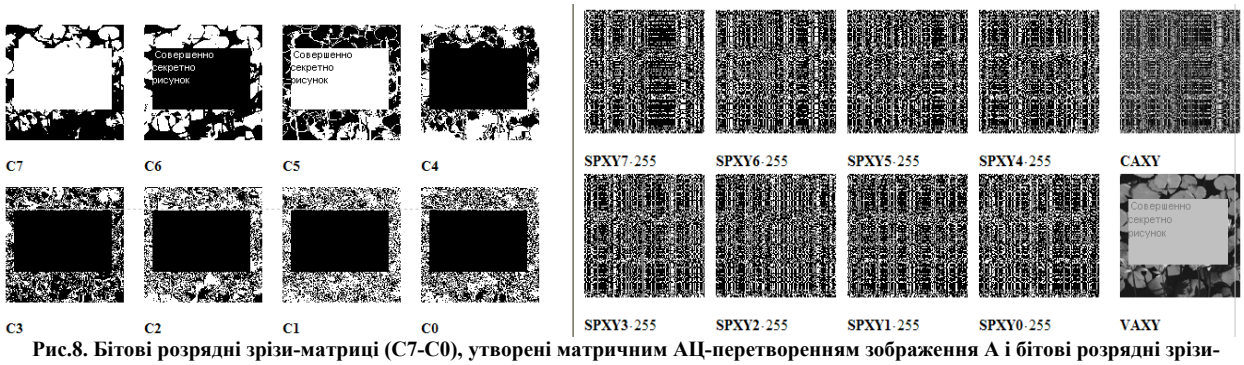


Рис.8. Бітові розрядні зрізи-матриці (C7-C0), утворені матричним АЦ-перетворенням зображення A і бітові розрядні зрізи-матриці SPXY7 – SPXY0 криптограми CAXY

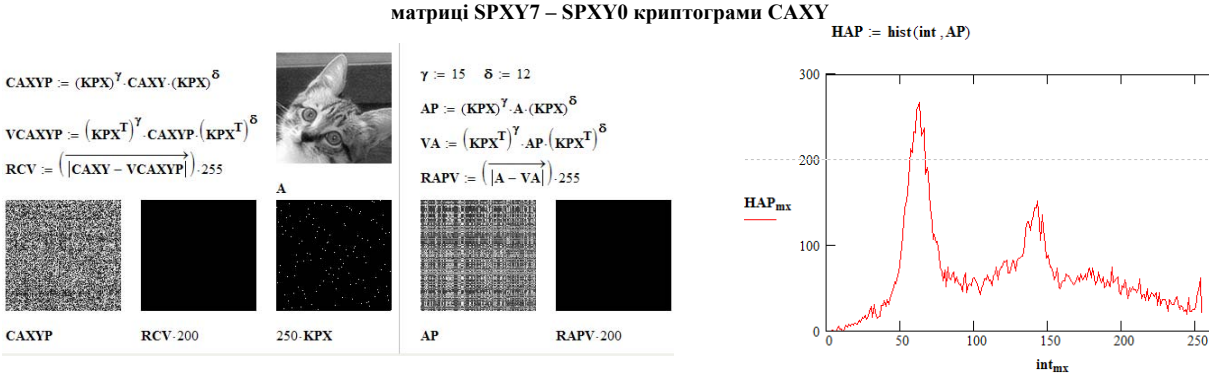
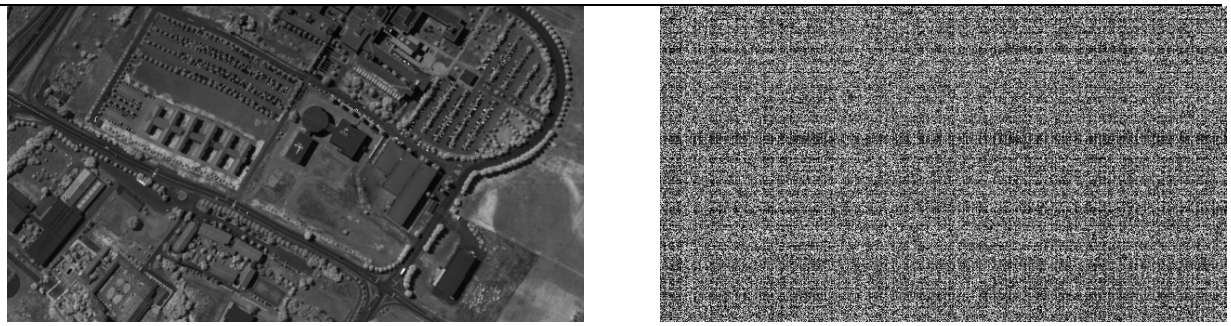


Рис.9. Результати моделювання та гістограма явного зображення

Рис.10. Результати моделювання та гістограма зашифрованого зображення



A **CAXY**

Рис.11. Явне зображення A (340*610*8) та його криптограма CAXY

Література

1. Ємець В. Сучасна криптографія. Основні поняття [Текст] / В. Ємець, А. Мельник, Р. Попович. – Львів: БаК, 2003. – 144 с.
2. Красиленко В.Г. Моделювання сліпих електронних цифрових підписів матричного типу на конфіденційну текстографічну документацію [Текст] / В.Г. Красиленко, Р. О. Яцковська, С. К. Грабовляк, // І Міжнародна науково-методична конференція Вінниця: ВНАУ, 2012. – С. 103-107.
3. Красиленко В.Г. Моделювання матричних алгоритмів криптографічного захисту [Текст] / В.Г. Красиленко, Ю.А. Флавицька // Вісник НУ «Львівська політехніка» «Комп'ютерні системи та мережі». - № 658. – С. 59-63.
4. Красиленко В.Г. Матричні афінні шифри для створення цифрових сліпих підписів на текстографічні документи [Текст] / В.Г. Красиленко, С.К. Грабовляк // Системи обробки інформації. – Х.: ХУПС, 2011. – Вип. 7(97**). –** С. 60 – 63.
5. Красиленко В.Г. Матричні афінно-перестановочні шифри для шифрування та дешифрування зображень [Текст] / В.Г. Красиленко, С.К. Грабовляк // Системи обробки інформації. - Х.: ХУПС, 2012. – Вип. 3(101).-т. 2. **–** С.53-61.
6. Красиленко В.Г. Матричні моделі перестановок з матрично-бітовою декомпозицією для криптографічних перетворень зображень та їх моделювання [Текст] / В.Г. Красиленко, В.М.Дубчак, О.В.Красиленко // Наука і навчальний процес: науково-методичний збірник матеріалів НПК ВСЕІ Університету «Україна». – Вінниця: Вінницький соціально-економічний інститут Університету «Україна», 2013. - С. 90 – 92.

References

1. Yemets W. , Miller A., Popovich R. Modern Cryptography . Basic Concepts. Lviv. Buck , 2003. - 144 p.
2. Krasilenko V.G., Yatskovsky R.O., Grabovlyak S.K. Modeling of blind digital signatures matrix type tekstohraficconfidential documents . The International Scientific Conference Vinnitsa. VNAU, 2012. P. 103-107.
3. Krasilenko V.G. , Flavitskaya Y.A. Modeling of matrix encryption algorithms. Vestnik "Lviv Polytechnic Computer systems and networks". № 658. - P. 59-63 .
4. Krasilenko V.G., Grabovlyak S.K. Matrix affine ciphers for blind digital signatures on tekstohrafic documents. Information processing systems. HUPS , 2011. - Vol. 7 (97). P. 60 - 63.
5. Krasilenko V.G. , Grabovlyak S.K. Matrix affine- permutation ciphers to encrypt and decrypt images. Information processing systems. HUPS , 2012. - Issue 3 (101). Part 2 P.5361 .
6. Krasilenko V.G. , Dubchak V.M., Krasilenko O.V. Matrix models permutations of matrix- bit cryptographic decomposition for image and modeling. Research and Training Process: Research and Methodological Proceedings of NPK VSEI University " Ukraine ". Kiev. Vinnitsa Institute of Social and Economic University " Ukraine ", 2013. - S. 90 - 92.

Рецензія/Peer review : 23.1.2014 р. Надрукована/Printed :6.2.2014 р.
Рецензент: д.т.н.,проф., завідувач кафедрою ПКТА
Вінницького Національного технічного університету Філинюк М.А.