УДК 004.056.55
Красиленко В.Г., к.т.н., с.н.с., доцент, професор; Нікітович Д.В., науковий співробітник
Вінницький інститут Університету "Україна"

МОДЕЛЮВАННЯ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ КОЛЬОРОВИХ ЗОБРАЖЕНЬ НА ОСНОВІ МАТРИЧНИХ МОДЕЛЕЙ ПЕРЕСТАНОВОК ЗІ СПЕКТРАЛЬНОЮ ТА БІТОВО-ЗРІЗОВОЮ ДЕКОМПОЗИЦІЯМИ

Красиленко В.Г., Нікітович Д.В. Моделювання криптографічних перетворень кольорових зображень на основі матричних моделей перестановок зі спектральною та бітово-зрізовою декомпозиціями. В роботі представлені результати моделювання криптографічних перетворень кольорових зображень на основі їх декомпозиції на спектральні складові і матричні бітові зрізи і застосування модифікованих матричних моделей перестановок для перемішування елементів масивів і забезпечення можливості верифікації цілісності створених криптограм. Процеси прямого і зворотного криптографічних перетворень зводяться до матрично-матричних процедур. В якості матричних ключів використовуються одна або дві матриці перестановок або їх ступені. Показано як використання декомпозиції і конкатенації зображень дозволяє виконувати не тільки самі перетворення, але і контролювати цілісність криптограм. Експерименти в середовищі Mathcad з кольоровим зображенням (128*128 елементів) з метою їх зашифрування і розшифрування за допомогою запропонованих моделей підтвердили адекватність і переваги останніх.
Ключові слова: криптографічні перетворення зображень, матричні моделі, декомпозиція, конкатенація, матриця перестановок, ступінь матриці, матрично - матрична процедура, матрично- бітово-зрізове (bit-plane) кодування, криптограма, стійкість криптографічної системи, матричні ключі.

Красиленко В.Г., Никитович Д.В. Моделирование криптографических преобразований цветных изображений на основе матричных моделей перестановок со спектральной и битово-срезовой декомпозициями. В работе представлены результаты моделирования криптографических преобразований цветных изображений на основе их декомпозиции на спектральные составляющие и матричные битовые срезы и применения модифицированных матричных моделей перестановок для перемешивания элементов массивов и обеспечения возможности верификации целостности созданных криптограмм. Процессы прямого и обратного криптографических преобразований сводятся к матрично-матричным процедурам. В качестве матричных ключей используются одна или две матрицы перестановок или их степени. Показано как использование декомпозиции и конкатенации изображений позволяет выполнять не только сами преобразования, но и контролировать целостность криптограмм. Эксперименты в среде Mathcad с цветным изображением (128*128 элементов) с целью их шифрования и расшифровки с помощью предложенных моделей подтвердили адекватность и преимущества последних.
Ключевые слова: криптографические преобразования изображений, матричные модели, декомпозиция, конкатенация, матрица перестановок, степень матрицы, матрично-матричная процедура, матрично-битово-срезовое (bit-plane) кодирование, криптограмма, стойкость криптографической системы, матричные ключи.

Krasilenko V.G., Nikitovich D.V. Simulation of cryptographic transformations of color images based on matrix models of permutations with spectral and bit-plane decompositions. The results of the simulation of cryptographic transformations of color images on the basis of their decomposition into spectral and bit slices and use of modified permutation matrix models for mixing elements of arrays and enable verification of the integrity of the established cryptogram. The direct and inverse cryptographic transformations are reduced to the matrix-matrix procedure. As matrix keys used one or two of permutation matrix or their degree. It is shown how to use decomposition and concatenation of images allows you to perform not only the transformation, but also to control the integrity of cryptograms. Experiments in Mathcad with color multilevel images (128 * 128 elements) with a view to encrypt and decrypt using the proposed models have confirmed the relevance and benefits of the latter.
Keywords: cryptographic transformation of color images, matrix models, matrix key, decomposition, matrix-bit-slice (bit-plane) encoding, cryptogram, cryptographic system stability, a permutation matrix, the degree of the matrix, the matrix-matrix procedure.

Вступ. Постійне збільшення обсягів та значимості інформаційних потоків з розвитком телекомунікаційних мереж, електронних комунікацій, широке застосування інформаційних технологій потребують, особливо для захищених систем управління, надійного та ефективного захисту цілісності інформаційних об'єктів (ІО) та стійкості до потенційних загроз. Суттєво зросла доля специфічних текстово-графічних документів (ТГД) у вигляді табличних даних, малюнків, діаграм, підписів, віз, резолюцій, тощо, які є зображеннями і які необхідно опрацьовувати та передавати каналами з обмеженим чи закритим доступом, засвідчувати їх цифровими підписами. Особливе місце серед відомих методів захисту ІО від несанкціонованого доступу займають криптографічні методи, що спираються на властивості самих ІО, а не матеріальних носіїв ІО та пристроїв їх обробки, передачі та зберігання. Більшість методів та засобів криптографічних перетворень (КП) ІО чи зображень, процедур і протоколів формування ключів та їх обміну орієнтовані на послідовну скалярну обробку блоків ТГД. Навіть для використовуваних найкращих симетричних алгоритмів (на основі діючого стандарту AES, IDEA, тощо) довжини блоків та ключів не перевищують 256 бітів, за винятком хіба-що FEAL, RC6 та інших нових, де ці довжини можуть обмежуватись 1К-2К бітами [1]. Програмні засоби реалізації КП у порівнянні з апаратними системами, хоч і мають ряд переваг, є ненадійними та слабкими до атак з точки зору їх «хакерських» зламувань чи завідомо введених вставок для контролю спецслужбами. Збільшення

складності задач та об'ємів ІО, що перероблюються в реальному часі, обумовило створення паралельних комп'ютерів, але зростання швидкості виконання операцій та складності процесорів призводить до збільшення збоїв та помилок, тому ще одним важливим завданням стає і контроль цілісності ІО, виявлення та виправлення помилок. Поява паралельних алгоритмів, а особливо матричних процесорів, потребує переорієнтації КП на ці засоби, та створення моделей матричного типу (МТ) [2-6]. Тому пошук нових матричних моделей (ММ) та засобів виконання КП ІО у вигляді ТГД (зображень), що краще відображаються на матричні процесори та забезпечують перевірку цілісності зашифрованих ІО, є актуальним завданням.

Аналіз останніх досліджень і публікацій. У роботі [2] були продемонстровані переваги КП матричними алгоритмами на основі більш узагальнених матричних афінних шифрів, в тому числі при створенні сліпих цифрових підписів на ТГД [3]. Ще більш узагальнені матричні афінно-перестановочні шифри були запропоновані та досліджені в [4], базовою операцією яких є матричні моделі перестановок (ММ_П), які мають наочну простоту. Проте, як показано в [6], КП на їх основі без додаткових операцій не змінюють гістограми зображень, а запропоновані в ній модифіковані моделі з декомпозицією бітових зрізів, хоч і усувають цей недолік, потребують у деяких випадках крім двох матричних ключів (МК) ще й двох векторних (ВК). В той же час всі вищезгадані моделі не дозволяють перевіряти цілісність криптограми та наявність перекручувань. У роботах [7,8] були розглянуті модифіковані матричні моделі КП з верифікацією цілісності криптограм лише для чорно-білих зображень, а в [9] хоч і розглядались КП кольорових, але без аспектів верифікації цілісності, тому є потреба розширити узагальнити ці моделі на випадок кольорових зображень, враховуючи специфіку їх форматів та розширень.

Постановка наукової проблеми. Таким чином є необхідною і актуальною спроба подальшої модифікації та узагальнення ММ для КП саме кольорових зображень з метою покращення їх характеристик і функціональних можливостей за рахунок верифікації цілісності. Моделювання та перевірка функціонування створених моделей на реальних ІО дозволить оцінити їх показники, можливості та особливості застосувань.

Тому метою даної роботи є узагальнення ММ_П на випадок КП кольорових зображень з перевіркою цілісності ІО та використанням спектральної та бітово-зрізової декомпозиції та надлишкового зрізу-підпису, їх моделювання у програмному середовищі Mathcad та оцінювання.

Виклад основного матеріалу та результатів дослідження.

Сутність запропонованих узагальнених ММ_П з одночасною спектральною та бітово-зрізовою декомпозиціями (ММ_П_СБЗД) полягає у формуванні з явного кольорового зображення, а саме з його трьох R,G,B складових (BZ1, BZ2, BZ3) шляхом матричних аналого-цифрових перетворень (АЦП) наборів М-розрядів-зрізів та додаткового зображення CON_S, наприклад, згорнутого специфічним h – функціональним перетворенням, (у експерименті це по-елементне додавання за модулем 2 всіх 24=3*8 зрізів), їх конкатенації та застосуванні КП до спільного масиву A_SC, шляхом множення його зліва і справа на матриці перестановок (МК чи його степені), що еквівалентно перемішуванню рядків та стовбців масиву. На рис. 1-5 зображені результати моделювання прямого та оберненого криптографічних перетворень кольорового зображення на основі ММ_П_СБЗД. Програмні модулі та формули для моделювання процесів створення ключів, зашифрування та розшифрування кольорових зображень на основі ММ_П_СБЗД з формуванням кольорової криптограми та матриці ознаки її цілісності показані на рис.1,2. Кожне спектральне складове спочатку перетворювалось у 8 бітових зрізів за допомогою формул на рис.1b, а потім всі 24 зрізи (матриці кодів Грея) конкатенувались з утвореним з них контрольним зрізом CON_S у масив A_SC за допомогою формул на рис.1c. З урахуванням обмежень на обсяг роботи та висвітлень в роботах [4-8] аспектів генерування ключів (матриць перестановок) та протоколів їх обміну [10] тут ми відмічаємо лише той позитивний факт, що в ММ_П_СБЗД достатньо одного матричного ключа (KPS), розмірність якого для експериментів була 640*640 відповідно до розмірів (128*128) взятого для перетворень зображення. За допомогою матричної процедури чи подібних їй при зміні степенів МК у відповідності до скалярних ключів η^{sl} та η^{sp}, (рис.2), формували масив C_ASC з об'єднаного масиву A_SC, а з нього результуючу кольорову криптограму (Ar, Ag, Ab) та її цифровий підпис C_CON (дивись рис.2, 3) шляхом обернених цифро-аналогових перетворень (ЦАП), формувань відповідних R,G,B спектральних складових кольорової криптограми та контрольного зрізу, що є по суті відповідним цифровим підписом (ЦП) криптограми.

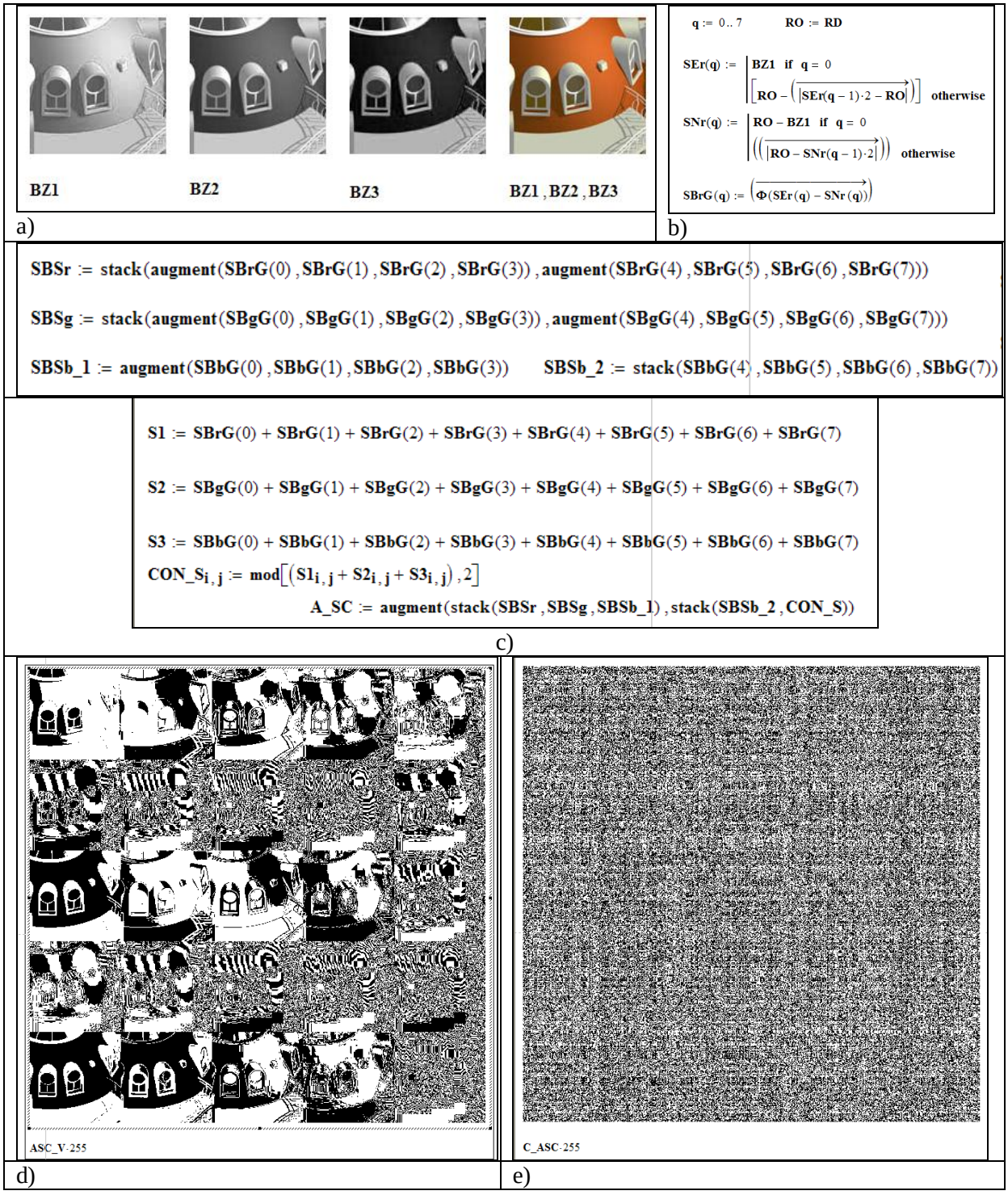

Рис. 1. Зображення та фрагменти вікон Mathcad, формули, що використовувались для моделювання:a) – R, G, B складові кольорового зображення (праворуч); b) - Формули, що використовувались для прямого АЦ (у бітові зрізи) та оберненого ЦА перетворень; c) – Формули для конкатенації всіх 24 зрізів та 25-го контрольного CON_S у масив A_SC; d) – Відновлений бітовий масив ASC_V, що є і масивом A_SC; e) – Криптограма з цифровим підписом C_CON у бітово-зрізовому представленні.

Процедури виділення бітових зрізів, їх перекодування з кодів Грея у двійкові зріз-коди для зворотної процедури формування трьох R, G, B складових результуючої кольорової криптограми (Ar, Ag, Ab) та її цифрового підпису C_CON (бітовий масив!) з масиву C_ASC (бітово-зрізове представлення криптограми та її ЦП !) здійснювались за допомогою формул на рис.2.

$\eta sl := 5 \quad \eta sln := 7 \quad KPSO := KPS^{T} \quad \eta sp := 9 \quad \eta spn := 3 \quad 128 \cdot 4 = 512$

$C\_ASC := KPS^{\eta sl} \cdot A\_SC \cdot KPS^{\eta sp} \quad 128 \cdot 5 = 640$

$ASC\_V := KPSO^{\eta sl} \cdot C\_ASC \cdot KPSO^{\eta sp}$

$Cr0 := submatrix(C\_ASC, 0, 127, 0, 127)$
$Cr1 := submatrix(C\_ASC, 0, 127, 128, 255)$
$Cr2 := submatrix(C\_ASC, 0, 127, 256, 383)$
$Cr3 := submatrix(C\_ASC, 0, 127, 384, 511)$
$Cb0 := submatrix(C\_ASC, 512, 639, 0, 127)$
$Cb1 := submatrix(C\_ASC, 512, 639, 128, 255)$
$Cb2 := submatrix(C\_ASC, 512, 639, 256, 383)$
$Cb3 := submatrix(C\_ASC, 512, 639, 384, 511)$

$Cr4 := submatrix(C\_ASC, 128, 255, 0, 127)$
$Cr5 := submatrix(C\_ASC, 128, 255, 128, 255)$
$Cr6 := submatrix(C\_ASC, 128, 255, 256, 383)$
$Cr7 := submatrix(C\_ASC, 128, 255, 384, 511)$
$Cb4 := submatrix(C\_ASC, 0, 127, 512, 639)$
$Cb5 := submatrix(C\_ASC, 128, 255, 512, 639)$
$Cb6 := submatrix(C\_ASC, 256, 383, 512, 639)$
$Cb7 := submatrix(C\_ASC, 384, 511, 512, 639)$

$Br7 := Cr0 \quad Bg7 := Cg0 \quad Bb7 := Cb0$

$Br6 := (Br7 \oplus Cr1) \xrightarrow{} \quad Bg6 := (Bg7 \oplus Cg1) \xrightarrow{} \quad Bb6 := (Bb7 \oplus Cb1) \xrightarrow{}$

$Br5 := (Br6 \oplus Cr2) \xrightarrow{} \quad Bg5 := (Bg6 \oplus Cg2) \xrightarrow{} \quad Bb5 := (Bb6 \oplus Cb2) \xrightarrow{}$

$Br4 := (Br5 \oplus Cr3) \xrightarrow{} \quad Bg4 := (Bg5 \oplus Cg3) \xrightarrow{} \quad Bb4 := (Bb5 \oplus Cb3) \xrightarrow{}$

$Br3 := (Br4 \oplus Cr4) \xrightarrow{} \quad Bg3 := (Bg4 \oplus Cg4) \xrightarrow{} \quad Bb3 := (Bb4 \oplus Cb4) \xrightarrow{}$

$Br2 := (Br3 \oplus Cr5) \xrightarrow{} \quad Bg2 := (Bg3 \oplus Cg5) \xrightarrow{} \quad Bb2 := (Bb3 \oplus Cb5) \xrightarrow{}$

$Br1 := (Br2 \oplus Cr6) \xrightarrow{} \quad Bg1 := (Bg2 \oplus Cg6) \xrightarrow{} \quad Bb1 := (Bb2 \oplus Cb6) \xrightarrow{}$

$Br0 := (Br1 \oplus Cr7) \xrightarrow{} \quad Bg0 := (Bg1 \oplus Cg7) \xrightarrow{} \quad Bb0 := (Bb1 \oplus Cb7) \xrightarrow{}$

Рис.2. Формули, що використовувались для створення матриці перестановок KPS та оберненої до неї KPSO, скалярних ключів ηsl та ηsp, матричних процедур для реалізації моделей зашифрування (утворення криптограми C_ASC з об'єднаного масиву A_SC) та розшифрування (відновлення масиву ASC_V) та процедур виділення бітових зрізів, їх перекодуванні з кодів Грея у двійкові зріз-коди для зворотної процедури формування трьох R, G, B складових результуючої кольорової криптограми (Ar, Ag, Ab) та її цифрового підпису C_CON (бітовий масив!).

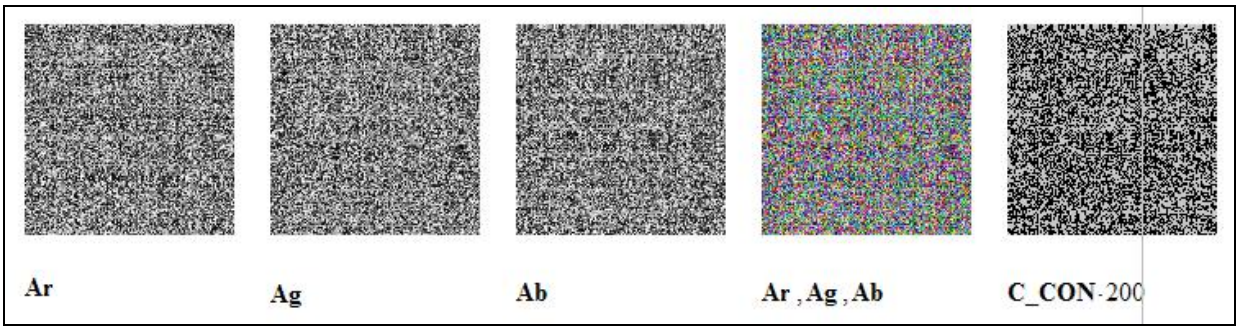

Рис.3. Утворені зашифруванням три R (Ar), G (Ag), B (Ab) складові результуючої кольорової криптограми (Ar, Ag, Ab) та її цифровий підпис C_CON (бітовий масив!).

Аналогічними процедурами, але вже за допомогою обернених перестановок з використанням ключа KPSO та аналогічних скалярних ключів відновлюється масив ASC_V, а з нього формуються відновлені (розшифроване) зображення та його контрольний підпис для верифікації. Отримані

результати моделювання процесу розшифрування при використанні правильних ключів, що на рис.5, свідчать про коректність моделей та правильне відтворення кольорового та всіх проміжних зображень на різних кроках перетворень. Результати моделювання процесу розшифрування при використанні неправильних ключів чи наявних втручаннях, що будуть наводитись у доповіді також засвідчили адекватність та стійкість моделей. Гістограми, що на рис.4, та їх аналіз також підтверджують якісну роботу моделей.

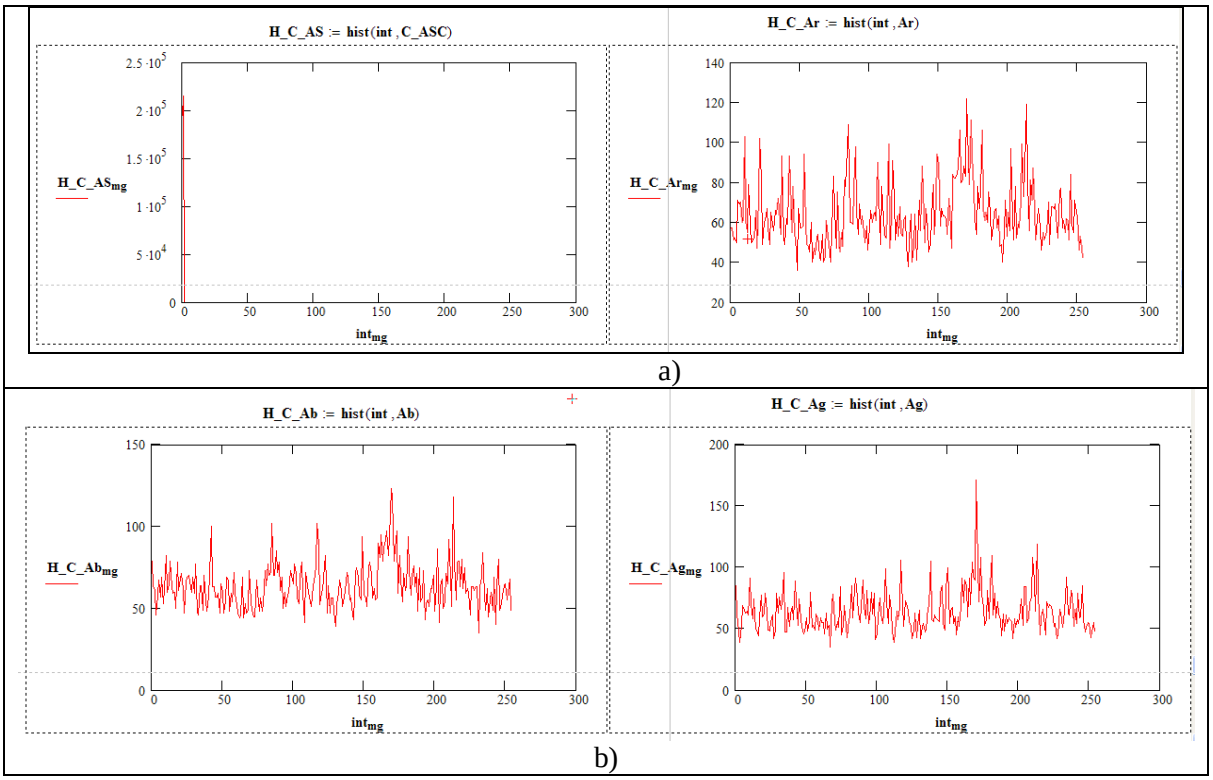

Рис.4. Гістограми криптограми C_ASC (вона ж - масиву A_SC) у бітово-зрізовому вигляді та утворених трьох R (Ar), G (Ag), B (Ab) спектральних складових результуючої кольорової криптограми (Ar, Ag, Ab).

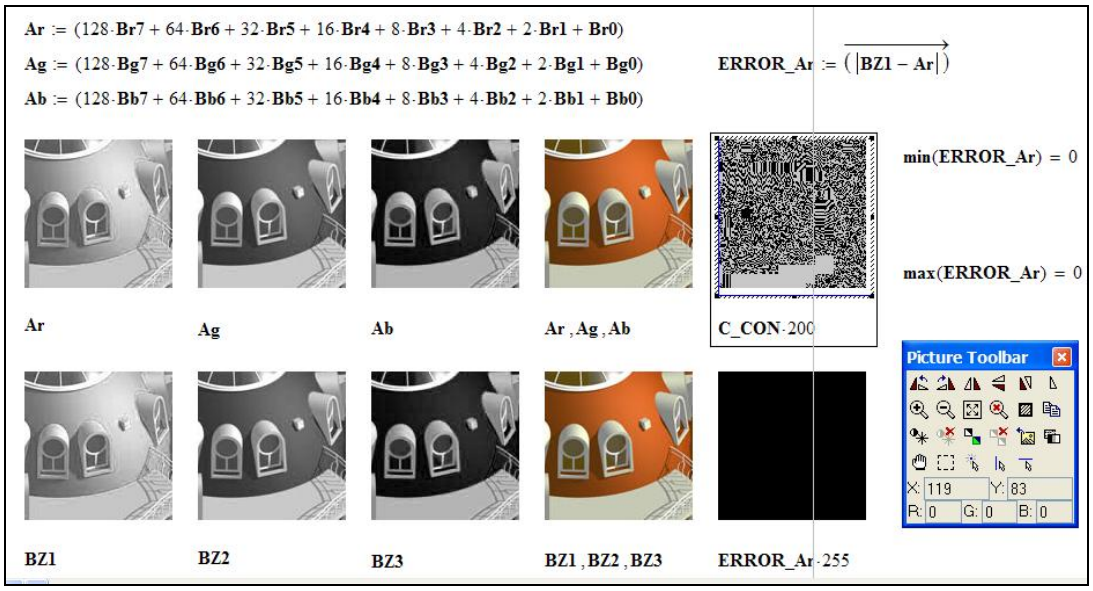

Рис.5. Відновлені розшифруванням та ЦА перетвореннями (формули вгорі!) зображення (верхній ряд) та початкові (спектральні складові та кольорове у нижньому ряду) для порівняння та верифікації точності моделей криптографічних перетворень та їх цілісності.

У роботах [3-6] було показано можливість збільшення ентропії криптограм на основі подібних моделей практично аж до 7,5-7,8 біт на точку чорно-білого зображення. Результати моделювання свідчать про неможливість без знання ключів відтворити початкове зображення. У випадку внесення спотворень при знанні особою ключів можна визначити наявність втручань, а порівнянням апріорного та розшифрованого зображень навіть усунути їх. Стосовно крипостійкості розглянутих моделей, то зазначимо, що, як було показано в [3], з урахуванням сьогоднішніх методів та засобів пошуку ключа гарантована стійкість аналогічних по суті базових моделей на основі матриць перестановок, яка залежить від потужності множини ключів (вона пропорційна n!, де n – розмірність матричних ключів), забезпечується уже при розмірності, рівній 32*32, а в нас матричні ключі розмірністю щонайменше 640*640, тобто відповідна потужність (640!) ще на багато порядків створює запас стійкості.

Висновки

Результати моделювання прямого та оберненого КП на основі ММ_П_СБЗД свідчать про коректну роботу цих моделей, їх адаптованість до різних форматів, зручність (всього один МК та його степені!), функціональність (можливість визначати факти втручань та порушень цілісності ІО, знаходити їх та усувати) та ефективність (орієнтація на матричні процесори). Розглянуті процедури створення необхідних МК, матриць перестановок та їх обміну, оцінена крипостійкість. Моделі ускладнюють здійснення прихованих атак та внесення перекручувань.

1. Ємець В. Сучасна криптографія. Основні поняття / В. Ємець, А. Мельник, Р. Попович. – Львів: БаК, 2003. – 144 с.
2. Красиленко В.Г. Моделювання матричних алгоритмів криптографічного захисту / В.Г. Красиленко, Ю.А. Флавицька // Вісник НУ «Львівська політехніка» «Комп'ютерні системи та мережі». - № 658. – С. 59-63.
3. Красиленко В.Г., Матричні афінні шифри для створення цифрових сліпих підписів на текстографічні документи / В.Г. Красиленко, С.К. Грабовляк // Системи обробки інформації. – Х.: ХУПС, 2011. – Вип. 7(97**). –** С. 60 – 63.
4. Красиленко В.Г. Матричні афінно-перестановочні шифри для шифрування та дешифрування зображень / В.Г. Красиленко, С.К. Грабовляк // Системи обробки інформації. - Х.: ХУПС, 2012. – Вип. 3 (101).-т. 2. **–** С. 53-62.
5. Красиленко В.Г. Матричні моделі криптографічних перетворень зображень з матрично-бітово-зрізовою декомпозицією і перемішуванням та їх моделювання / В. Г. Красиленко, Д.В. Нікітович //Матеріали 68 НТК «Сучасні інформаційні системи і технології. Інформаційна безпека», ч. 3, секції 3-4. – Одеса, ОНАЗ ім.. О.С.Попова, 2013. – С.139-143.
6. Красиленко В.Г. Криптографічні перетворення зображень на основі матричних моделей перестановок з матрично-бітовозрізовою декомпозицією та їх моделювання / В. Г. Красиленко, В. М. Дубчак // Вісник Хмельницького національного університету. Технічні науки. - 2014. - № 1. - С. 74-79.
7. Красиленко В.Г. Моделювання модифікованих матричних моделей криптографічних перетворень зображень з верифікацією цілісності криптограм / В.Г. Красиленко, Д.В. Нікітович // Матеріали II міжнародної науково-практичної Інтернет-конференції «Інформаційні технології: теорія, інновації, практика». – Полтава: ПолтНТУ, 2015. – С. 86-89.
8. Красиленко В.Г. Моделювання криптографічних перетворень зображень на основі їх матрично-бітовозрізової декомпозиції та матричних моделей перестановок з верифікацією цілісності / В.Г. Красиленко, Д.В. Нікітович // Всеукраїнська науково-практична конференція молодих вчених та студентів «Перспективні напрямки сучасної електроніки, інформаційних і комп'ютерних систем» (MEICS-2015). – Дніпропетровськ: Дніпропетровський національний університет ім. Олеся Гончара, 2015. - С. 32-34.
9. Красиленко, В.Г. Моделювання матричних афінних алгоритмів для шифрування кольорових зображень / В. Г. Красиленко, К. В. Огородник, Ю.А.Флавицька // Комп'ютерні технології: наука і освіта: тези доповідей V Всеукр. наук.-пр. конф. – К., 2010. – С.120-124.
10. Красиленко В. Г. Алгоритми формування двовимірних ключів для матричних алгоритмів криптографічних перетворень зображень та їх моделювання / В. Г. Красиленко, В. І. Яцковський, Р. О. Яцковська // Системи обробки інформації. - 2012. - Вип. 8. - С. 107-110.