МОДЕЛЮВАННЯ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ КОЛЬОРОВИХ ЗОБРАЖЕНЬ З ВЕРИФІКАЦІЄЮ ЦІЛІСНОСТІ КРИПТОГРАМ НА ОСНОВІ МАТРИЧНИХ МОДЕЛЕЙ ПЕРЕСТАНОВОК

Красиленко В.Г., Нікітович Д.В.
Вінницький інститут Університету "Україна"
krasilenko@mail.ru

Вступ. Розвиток телекомунікаційних мереж (ТКМ), електронних комунікацій, широке застосування інформаційних технологій (ІТ), постійне збільшення обсягів інформаційних потоків, їх значимості, конфіденційності, стійкості до потенційних загроз потребують, особливо для захищених ТКМ та автоматизованих систем управління, надійного та ефективного захисту цілісності інформаційних об'єктів (ІО), серед яких суттєво зросла доля специфічних текстово-графічних документів (ТГД) у вигляді цифрових, табличних даних, малюнків, графіків, діаграм, підписів, віз, резолюцій, тощо, які є по суті 2-D масивами (зображеннями) значної розмірності і які необхідно опрацьовувати та передавати. Багато з них містять інформацію з обмеженим чи закритим доступом, яку треба надавати як звітність у податкові та інші державні органи, засвідчувати їх цифровими підписами. Серед широкого спектру відомих методів та засобів захисту ІО віл несанкціонованого доступу особливе місце займають криптографічні методи, що, на відміну від інших, спираються лише на властивості самих ІО та не використовують властивості матеріальних носіїв ІО та особливості, характеристики пристроїв їх обробки, передачі та зберігання. Але більшість використовуваних методів та засобів криптографічних перетворень (КП) інформаційних масивів чи зображень та процедури і протоколи формування ключів та їх обміну орієнтовані на послідовну скалярну обробку блоків ТГД, перетворених у цифрові формати. Так, наприклад, навіть для широко 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 їх нових модифікацій, де ці довжини можуть обмежуватись 1К-2К бітами [1]. Програмні засоби реалізації КП у порівнянні з апаратними криптосистемами, хоч і мають ряд економічних та функціональних переваг, є ненадійними з точки зору можливих помилок при їх копіюваннях, «хакерських» зламуваннях чи завідомо введених, так званих «дирок», що уможливлює або їх контроль спецслужбами або слабкість до атак. Збільшення складності вирішуваних задач та об'ємів ІО, що переробляються в реальному часі, особливо в ядерній енергетиці, системах управління хімічними виробництвами, системах керування ракетними, супутниковими, військовими засобами обумовило створення високопродуктивних з підвищеною надійністю паралельних комп'ютерів, з вбудованими вузлами контролю та діагностики. Зростання швидкості виконання операцій та складності обчислювальних систем призводить до збільшення збоїв та помилок, що неминуче виникають у процесах обробки, зберігання та передачі даних, тому ще одним важливим завданням стає і контроль цілісності ІО, виявлення та виправлення помилок, розв'язання якого досягається введенням інформаційної надлишковості та спеціальних методів кодування. А поява паралельних алгоритмів, а особливо матричних багатопроцесорних засобів, потребує модифікацій відомих КП, з орієнтацією на ці нові засоби, та створення відповідних моделей матричного типу (МТ) [2-4]. Тому пошук нових матричних моделей (ММ) та засобів виконання КП ІО у вигляді ТГД чи зображень, орієнтованих на матричні, в тому числі особливо на оптичні, мікро-фотоелектронні, процесори з можливістю виявлення та верифікації цілісності зашифрованих ІО, є актуальним завданням.

Аналіз останніх досліджень і публікацій. У роботі [2] були продемонстровані можливості та переваги запропонованих раніше В.Г. Красиленком та досліджених матричних алгоритмів криптографічного захисту на основі більш узагальнених матричних афінних шифрів при

створенні сліпих цифрових підписів на ТГД. Ще більш узагальнені матричні афінно-перестановочні шифри були запропоновані та досліджені в [3], однією з основних складових яких є матричні моделі перестановок (ММ_П), які мають наочну простоту. Проте, як показано в [4], КП на їх основі без додаткових операцій не змінюють гістограми зображень чи ТГД, а запропоновані в ній модифіковані ММ_П з декомпозицією бітових зрізів усувають цей недолік, хоч і потребують у деяких випадках крім двох матричних ключів (МК) ще й двох векторних (ВК). В той же час всі вищезгадані моделі не дозволяють перевіряти (верифікувати) цілісність криптограми та наявність перекручувань інформації. У роботі [5] були розглянуті модифіковані матричні моделі КП з верифікацією цілісності криптограм лише для чорно-білих багато-градаційних зображень, тому є потреба розширити узагальнити ці моделі на випадок кольорових зображень, враховуючи специфіку їх форматів та розширень.

Постановка задачі. Таким чином є необхідною і актуальною спроба подальшої модифікації та узагальнення відомих ММ_П з декомпозицією для КП саме кольорових зображень з метою їх спрощення, покращення та розширення їх функціональних можливостей, в тому числі, і 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 модифікація, моделювання у програмному середовищі Mathcad ММ_П з матричною R,G,B декомпозицією та надлишковою матричною хеш-функцією для КП кольорових зображень для забезпечення можливості перевірки їх цілісності, оцінювання стійкості моделей.

Виклад основного матеріалу та результатів дослідження. Спочатку ми зробимо короткий огляд існуючих ММ шифрів та алгоритмів КП зображень та розглянемо сутність запропонованих узагальнень ММ_П з матрично-бітовою декомпозицією (ММ_П МБД) та декомпозицією на спектральні R,G,B складові (ММ_П ДС). Сутність узагальненої моделі на основі ММ_П ДС полягає у

формуванні з явного кольорового зображення A_K, а саме з його трьох R,G,B складових (BZ1, BZ2, BZ3) додаткового зображення CONT, наприклад, згорнутого специфічним h – функціональним перетворенням, (у одному з наших експериментів це поелементне додавання за модулем 256 всіх BZ1, BZ2, BZ3), у застосуванні КП на основі ММ_П до кожного з них чи до спільного Pic_A, утвореного шляхом їх конкатенації. На рис. 1-6 зображені результати моделювання КП на основі модифікованих ММ_П ДС шляхом взаємно-однозначної заміни рівнів яскравості пікселів Pic_A на першому кроці зашифрування за допомогою матричного ключа (МК) KPM чи його α-степені (ключ KPMC) з утворенням C1_A та процедурою перемішування рядків та стовбців масиву C1_A на другому кроці зашифрування за допомогою двох ключів, що є різними степенями того ж базового ключа KPM, та утворення масиву C2_A у відповідності до формули:

$$\mathbf{C2\_A} := \mathbf{KPM}^{\eta \mathbf{xc}} \cdot (\mathbf{C1\_A}) \cdot \mathbf{KPM}^{\eta \mathbf{yc}} \tag{1}$$

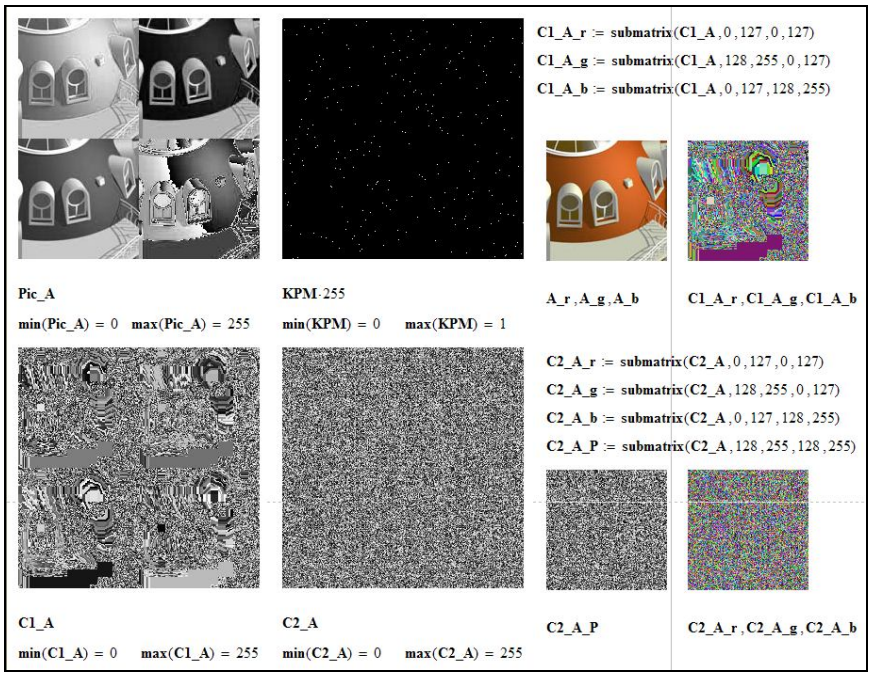

Рис. 1. Результати моделювання процесу зашифрування кольорових зображень

Використовуючи як явне зображення A (чи інші: A_K, A1, A2) розмірністю 128*128 ел. чи більше, аж до 512*512, його чорно-білу конкатеновану з R,G,B складових та хеш-матриці форму Pic_A (256*256 ел.), дивись на рис.1 а), програмні модулі зашифрування та розшифрування (рис.2, 3) та формули для генерування МП - ключів КРМ (256*256) та КРМС, один з яких (КРМ) показаний на рис.1, ми за допомогою матричної процедури (формула 1), чи подібних їй при зміні степенів МК у відповідності до скалярних ключів α , η_{xc} , η_{yc} (рис. 2, 3), формували матриці C1_A, C2_A на 1-ому та 2-ому кроках зашифрування, з яких були утворені результуюча кольорова криптограма C2_A_K (на рис. 1 у нижньому ряду четверта) та чорно-біле контрольне зображення C2_A_P (на рис. 1 у нижньому ряду третє). Процедурами за ф. (2), але вже за допомогою обернених перестановок пікселів на 1-ому кроці з використанням обернених ключів КРМО та аналогічних скалярних ключів відновлюється D2_A спочатку:

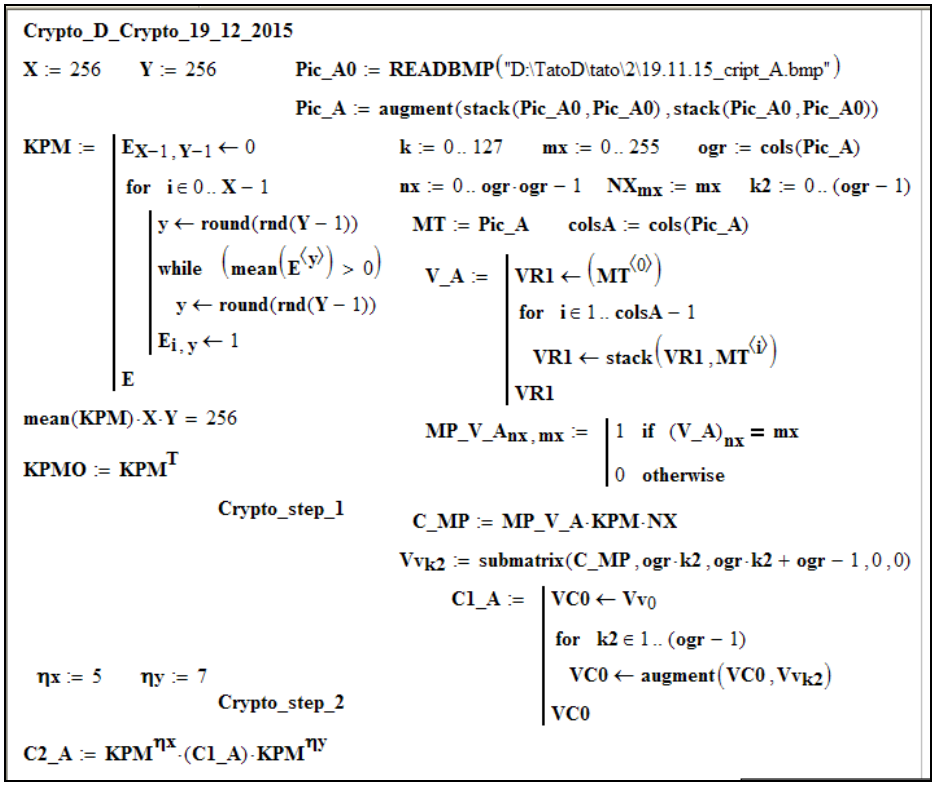

Рис. 2. Програмний модуль для моделювання процесу зашифрування кольорових зображень з формуванням на основі ММ_П ДС кольорової криптограми та матриці ознаки її цілісності

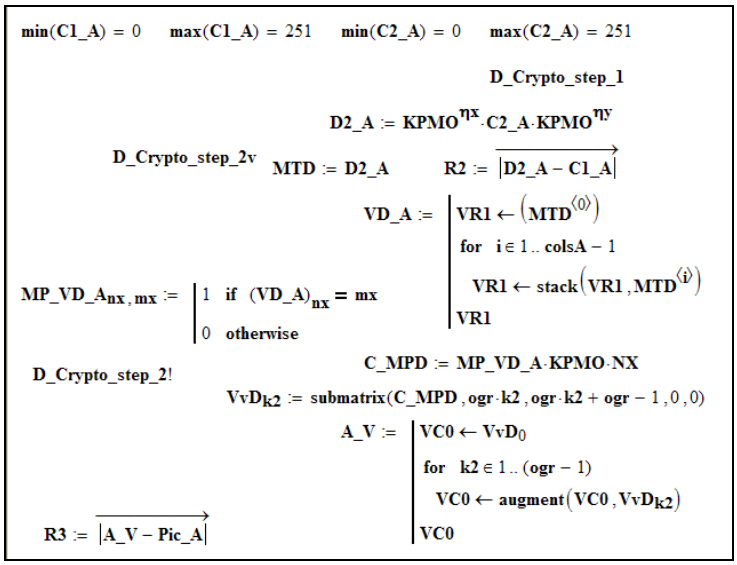

Рис. 3. Програмний модуль для моделювання процесу розшифрування кольорових зображень з перевіркою точності відновлення явного та верифікацією цілісності криптограми

$$\mathbf{D2\_A := KPMO^{\eta xd} \cdot C2\_A \cdot KPMO^{\eta yd}} \quad (2),$$

а потім на другому кроці з нього шляхом оберненого перетворення градацій пікселів формується розшифроване зображення A_V. Отримані результати моделювання процесу розшифрування при використанні правильних ключів, що на рис.4, свідчать про коректність моделей та правильне відтворення кольорового та всіх проміжних зображень на різних кроках перетворень.

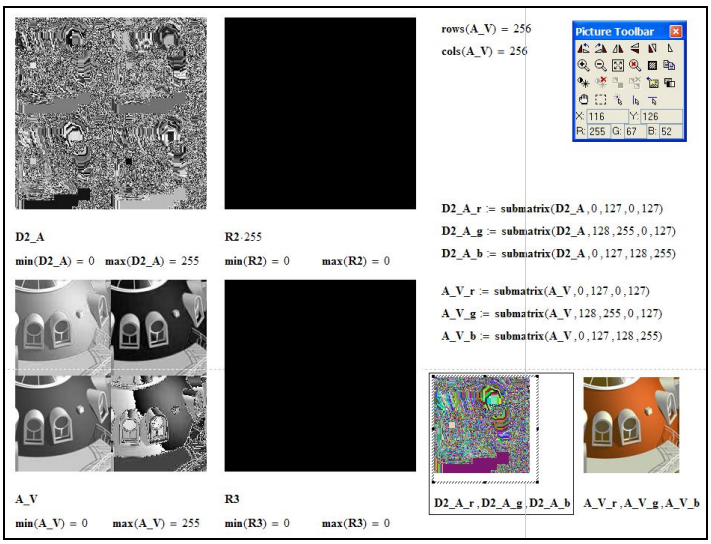

Рис. 4. Результати моделювання процесу розшифрування кольорових зображень при використанні правильних ключів

Результати аналогічного моделювання (рис. 5) при використанні неправильних ключів свідчать про неможливість без знання ключів відтворити початкове зображення. Розшифровані на 1-ому та 2-ому кроках відповідні кольорові зображення є подібними до завад. У випадку внесення природних чи штучних цілеспрямованих спотворень неможливо без знання ключів приховати сам факт втручання.

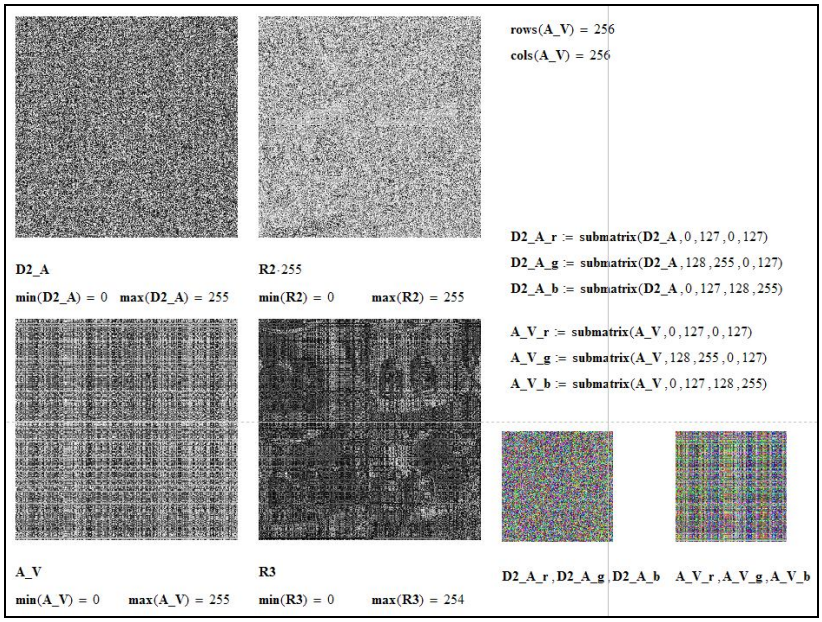

Рис. 5. Результати моделювання процесу розшифрування кольорових зображень при використанні неправильних ключів

Результати розшифрування (рис.6) при наявних втручаннях і їх виявленні при знанні особою ключів показують, що можна визначити наявність втручань і з великою ймовірністю зрозуміти ІО, а шляхом порівнянь апріорного та розшифрованого зображень навіть взнати вид спотворень та усунути їх.

Гістограмний аналіз криптограм також підтверджує якісну роботу запропонованих моделей. У роботах [2-4] було показано можливість збільшення міри невизначеності (ентропії) на основі подібних моделей практично аж до 7,5-7,8 біт на точку чорно-білого зображення. 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 МК), забезпечується уже при розмірності, рівній 32*32, а в нас матричні ключі розмірністю щонайменше 256*256, тобто відповідна потужність (256!) ще на багато порядків створює запас стійкості.

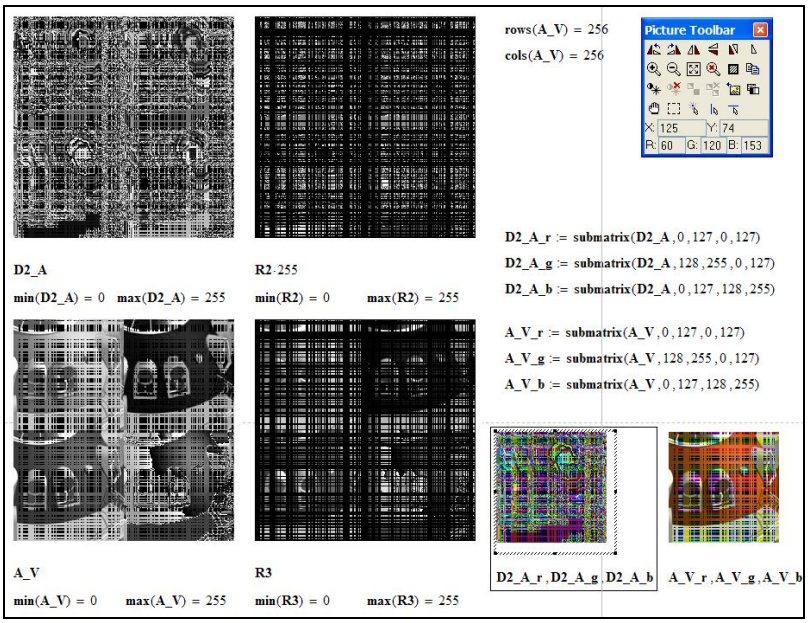

Рис. 6. Результати моделювання процесу розшифрування кольорових зображень при наявних втручаннях та спотвореннях і їх виявлення при використанні правильних ключів

Висновки: Моделювання КП на основі ММ_П ДС підтверджують можливість визначати не лише факти втручань та порушення цілісності ІО, але і знаходити та усувати ці зміни. Моделі ускладнюють здійснення прихованих атак та внесення перекручувань. Результати моделювання прямого та оберненого КП свідчать про коректну роботу запропонованих моделей, їх адаптованість до різних форматів, зручність та ефективність. Розглянуті процедури створення необхідних МК, матриць перестановок та їх обміну.

Список використаних джерел:

1. Ємець В. Сучасна криптографія. Основні поняття / В. Ємець, А. Мельник, Р. Попович. – Львів: БаК, 2003. – 144 с.

2. 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.

3. 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.

4. 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.

5. Красиленко В.Г. Моделювання модифікованих матричних моделей криптографічних перетворень зображень з верифікацією цілісності криптограм / В.Г. Красиленко, Д.В. Нікітович // Матеріали ІІ міжнародної науково-практичної Інтернет-конференції «Інформаційні технології: теорія, інновації, практика». – Полтава: ПолтНТУ, 2015. – С. 86-89.

СИСТЕМА АВТОМАТИЗАЦІЇ ДІЯЛЬНОСТІ ГОТЕЛЮ

Лехович О.А.

Дрогобицький державний педагогічний університет імені Івана Франка

lehovicho@mail.ru

Автоматизація готелю повинна дозволити її працівникам позбутися великої кількості зайвих процесів, що спричинило б досить швидку і якісну роботу готелю пов’язану із додаванням внесенням та редагуванням інформації.

Аналіз предметної області

Готель надає номери клієнтам на певний термін. Кожен номер характеризується місткістю, комфортністю (президентський, люкс, напів-люкс,