СУЧАСНІ МЕТОДИ, ІНФОРМАЦІЙНЕ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ СИСТЕМ УПРАВЛІННЯ ОРГАНІЗАЦІЙНО-ТЕХНОЛОГІЧНИМИ КОМПЛЕКСАМИ

Збірник тез доповідей
всеукраїнської науково-практичної інтернет-конференції

11.05.2016

Луцьк
РВВ Луцького НТУ
2016

ЗМІСТ

Бойко Р.В., Катинський Т.В., Шолом П.С.
Налаштування поштового клієнта 1С8.х для роботи з Gmail через POP і SMTP 10

Бортник К.Я., Музичук В.Ю., Приходько О.С.
Технології web-дизайну 12

Данилюк О.А., Філіппова М.В.
Інформаційна система керування трудовими ресурсами на виробництві при впровадженні системи менеджменту якості 13

Довгаль А.О.
Побудова моделі загроз інформаційній безпеці мережі за допомогою регресіного аналізу 14

Дрейчан А.І., Соколовський Я.І., Семенюк В.Я.
Інформаційна система моніторингу успішності студентів 16

Дрючан В.І., Шолом П.С., Дудка О.М.
Web-сайт для самопідготовки учнів старших класів з курсу «Математика» на базі CMS Drupal 18

Єрмейчук С.Ю.
Аналіз алгоритмів пошуку 20

Желобицький Я.К., Максимович О.В., Багнюк Н.В., Мельник К.В.
Автоматичний терморегулятор фірми «OPAL» 22

Желобицький Я.К., Мельник В.М., Здолбіцька Н.В., Лавренчук С.В.
Web-ресурс для телерадіокомпанії з можливістю автоматичного запису ефірів і автонаповненням сайту з власного файлобмінника 24

Жигаревич О.К.
Розуміння екосистеми програмного забезпечення для розширеної технології навчання – тематичне дослідження 26

Завіша В.В.
Криптографічний захист інформації через фрактали 28

Іваніщук Р.В., Коцюба А.Ю., Христинець Н.А.
Вибір модулів та формування запитів Drupal Commerce для створення інтернет-магазину 29

Калінін Б.Ю., Федонюк А.А., Шолом П.С.
Судоку: японська гра на логіку засобами Java 32

Колодинський А.В., Христинець Н.А.
Застосування технології BDE при розробці програмного інтерфейсу в середовищі Delphi7 34

Котвицька А.Ю., Шолом П.С.
Програмно-методичний комплекс з дисципліни «Інженерія програмного забезпечення» засобами PHP 37

Коцюба А.Ю., Лавренчук С.В.
Про взаємодію середовищ C++ Builder та MS Office 39

Красиленко В.Г., Нікітович Д.В.
Криптографічні перетворення (КП) кольорових зображень на основі матричних моделей з операціями за модулем 41

Левчук Б.В., Здолбіцький А.П., Здолбіцька Н.В.
Світлодіодна лампа з електронним регулюванням яскравості 44

Лобода Р.В., Шолом П.С., Пасюк М.П.
CMS та CMF: порівняльний аналз засобів для побудови архітектури сайту 46

Лотоцький І.М., Мельник К.В.
Визначення складності алгоритму діагностування комп'ютерних систем на наявність вірусів в режимі сканера 47

Малярчук Р.А.
Основні характеристики програмного забезпечення різних типів 48

Мацюк С.М., Алексєєв О.М.
Ідентифікація і прогнозування показників процесу крупного дроблення руд 51

Мельник К.В., Мельник В.М., Сахнюк Н.В., Близнюк І.І.
Еволюційні моделі пошуку оптимального шляху 53

Мещеряков Л.І., Гулін О.О.
Комп'ютерне моделювання процесу дорожнього руху на основі клітинних автоматів 54

Міскевич О.І., Бортник К.Я., Ковальчук Р.Ю.
Організація інформаційних систем та технологій 56

Олида Н.В., Христинець Н.А.
Практика застосування компонентів DBS у розробках в середовищі Delphi 7 57

Ореховський В.І., Шолом П.С., Варакшина Н.В.
Android-додаток MeteoGov для перегляду прогрнозу погоди 59

Панасюк Н.Л.
Аналіз підходів щодо управління якістю підготовки майбутніх інженерів-педагогів в умовах магістратури технічного університету 62

Popov G.F., Savan S.I., Lazurik R.V., Pochynok A.V.
The Use of Semiempirical Models Into Computational Dosimetry of Electron Beams 65

Романюк Р.Р., Здолбіцький А.П., Здолбіцька Н.В.
Портативний електронний алкотестер 67

Рябокінь Ю.М., Жигаревич О.К.
Дослідження онтології предметної області навчального програмного забезпечення 69

Сав'як В.О., Багнюк Н.В., Шолом П.С., Лавренчук С.В.
Android-додаток дистанційного перегляду розкладу занять університету 72

Сірець С.В., Коцюба А.Ю., Лавренчук С.В.
Автоматизоване робоче місце секретаря екзаменаційної комісії 74

Супрунюк В.В., Шолом П.С.
Тактильний пристрій на базі мікросхеми LM324N 77

Титаренко В.Л., Федотова-Півень І.М.
Мікроконтролерна система на платформі Freeduino для виявлення пошкодження підземного силового кабелю 78

Ткач О.В., Шкалуба В.І., Семенюк В.Я.
Використання OLE-технологій в навчанні 79

Чикірда Н.Л., Здолбіцький А.П.
Web-сервер на Raspberry Pi 2 під управляння Linux 80

Чирук Р.В., Коцюба А.Ю., Лавренчук С.В.
C++ Builder проект для формування розкладу викладача на основі його навантаження 81

Красиленко В.Г., Нікітович Д.В.
Вінницький інститут університету «Україна»

КРИПТОГРАФІЧНІ ПЕРЕТВОРЕННЯ (КП) КОЛЬОРОВИХ ЗОБРАЖЕНЬ НА ОСНОВІ МАТРИЧНИХ МОДЕЛЕЙ З ОПЕРАЦІЯМИ ЗА МОДУЛЕМ

Вступ, аналіз досліджень і публікацій. У роботі [1] були продемонстровані переваги шифрування кольорових зображень (КЗ) матричними алгоритмами на основі узагальнених матричних афінних шифрів, в тому числі при створенні сліпих цифрових підписів [2]. Базовими операціями ще більш узагальнених матричних афінно-перестановочних шифрів [3] є по-елементні множення, додавання за модулем матриць та матричні моделі перестановок (ММ_П) з процедурами множення матриць. Проте, як показано в [4], КП ММ_П для зміни гістограми зображень необхідні декомпозиція бітових зрізів у модифікованих моделях та крім двох матричних ключів (МК) ще й два векторних (ВК). Але вищезгадані моделі не дозволяють перевіряти цілісність (Ц) криптограм та наявність перекручувань, а моделі КП з верифікацією Ц були розглянуті в [5] лише для чорно-білих зображень. Таким чином є актуальною спроба подальшої модифікації ММ для КП саме (КЗ), враховуючи їх специфіку, з метою покращення їх характеристик і функціональних можливостей за рахунок верифікації, а моделювання та перевірка створених моделей на реальних ІО дозволить оцінити їх параметри та особливості застосувань.

Метою роботи є узагальнення ММ на випадок КП КЗ з перевіркою цілісності ІО та використанням спектральної декомпозиції та цифрового підпису, їх моделювання. **Виклад матеріалу та результатів дослідження.** Сутність запропонованих ММ зі спектральною декомпозицією та цифровим підписом (ЦП) (ММСДЦП) полягає у формуванні зі складових явного кольорового зображення ЦП та застосуванні до їх конкатенації (PIC256 на рис. 1) процедур матричного множення на відповідні МК (KeyC_b, KeyD_b) з використанням операцій множення та додавання за модулем. Як видно з рис. 2-5, результати моделювання на основі ММСДЦП процесів прямого та оберненого КП КЗ розмірністю 128*128 ел. підтвердили коректну роботу моделей при застосуванні правильних ключів (рис. 2, 4) так і неправильних (рис. 5). МК мали ієрархічну структуру, розмірність 256*256 і складались як блочна матриця з 16*16 блоків розмірністю 16*16 ел-тів, а кожен з блоків мав 4 під-блоки по 4*4 ел., три з яких показані у фрагментах KLC, KLD на рис. 1. Як блоки KLC, KLD так і повні ключі є взаємно оберненими матрицями при множенні їх за відповідним модулем. Суттєвою відмінністю пропонованих МК є те, що як самі блоки у цілій матриці, так і під-блоки, та й елементи в них можуть перемішуватись, тобто їх структури подібні матрицям перестановок. Таким чином криптографічна обробка блоків супроводжується одночасним перемішуванням як блоків так і під-блоків. При створенні криптограми C_G та її підпису C_A_PG з унесеними перекручуваннями (зміни інтенсивності точок спектральних складових та контрольної після розрахунків), дивись рис. 3, 4, навіть малі втручання виявляються.

Висновки. Моделювання КП зображень на основі ММСДЦП свідчать про їх коректну роботу, зручність (всього 1 матрична процедура та 1 МК!),

адаптованість до форматів, багатофункціональність (поєднання операцій матричних блокових замін з перестановками, можливість визначати факти порушень цілісності ІО) та ефективність (орієнтація на матричні процесори). Розглянуті аспекти матричних алгебраїчних процедур і операцій за модулем та створення МК.

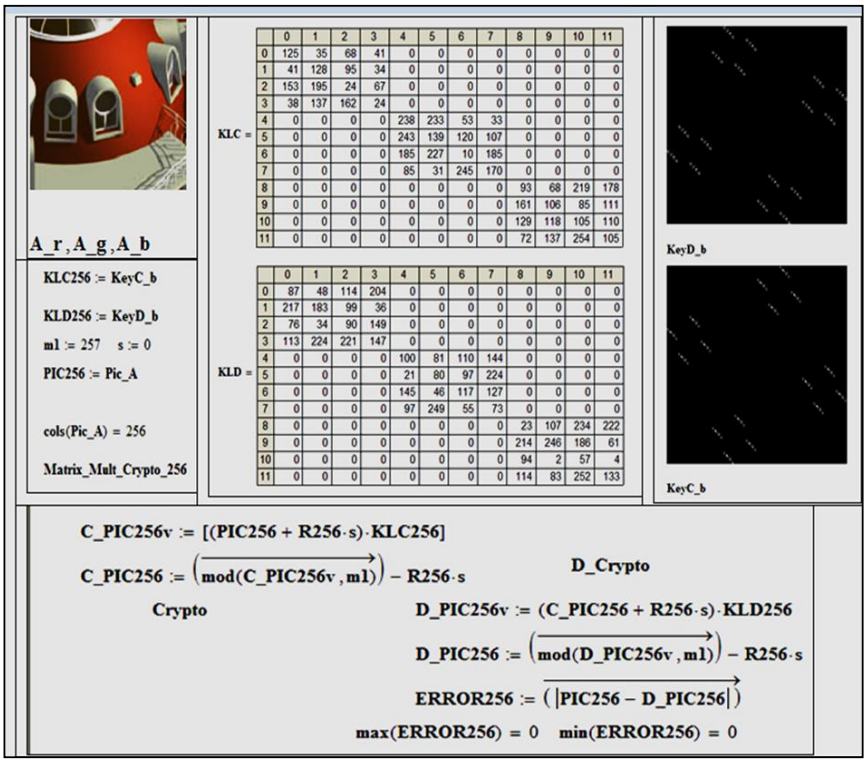

Рис. 1. Початкове КЗ, вигляд ключів, їх фрагментів та формули (фрагменти Mathcad) для моделювання КП КЗ запропонованими ММ з операціями множень матриць за модулем.

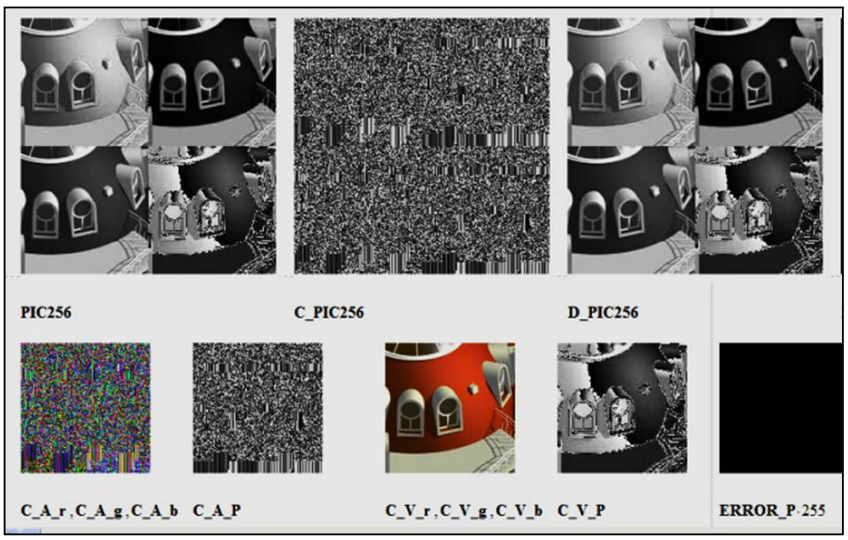

Рис. 2. Результати моделювання (вікно Mathcad) процесів КП кольорового зображення з верифікацією цілісності на основі матричних моделей зі спектральною декомпозицією: верхній ряд – конкатеновані складові початкового (PIC256), зашифрованого (C_PIC256), розшифрованого (D_PIC256) зображень; нижній ряд, зліва направо – кольорова криптограма, її підпис (C_A_P), розшифроване, контрольне (C_V_P) та різницеве зображення.

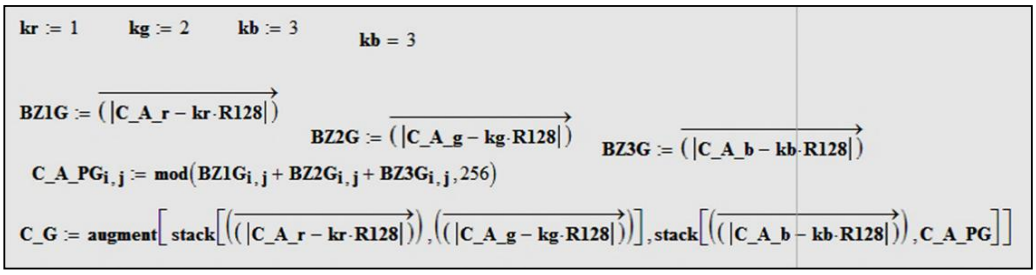

Рис. 3. Формули (фрагмент вікна Mathcad) для створення криптограми C_G та її підпису C_A_PG з унесеними, закамуфльованими перекручуваннями (зміни інтенсивності пікселів спектральних складових та контрольної після розрахунків)

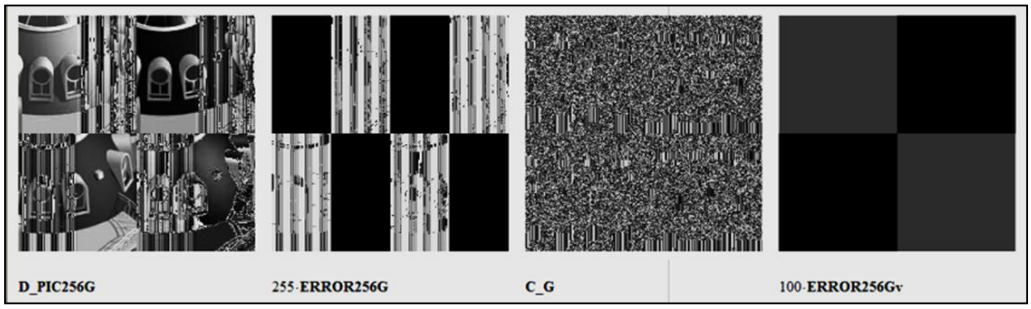

Рис. 4. Результати розшифрування за наявності втручань при правильних ключах

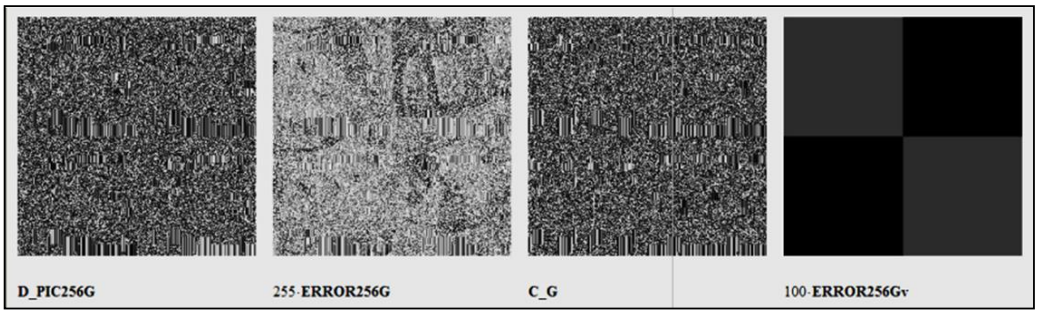

Рис. 5. Результати розшифрування при використанні неправильних ключів.

Список використаних джерел:

1. 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.

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 криптографічних перетворень кольорових зображень з верифікацією цілісності криптограм на основі матричних моделей перестановок / В.Г. Красиленко, Д.В. Нікітович // Матеріали НПК «Проблеми моделювання та розроблення інформаційних систем». – Дрогобич: ДДПУ ім. І. Франка, 2016. – С. 128-136. Режим доступу: http://ddpu.drohobych.net/wp-content/uploads/2016/04/material_konf.pdf