УДК 004.056.5

М.О.Козіна, В.Ю.Кремінський,
О.Б.Козін, С.-М.Нджикє Амугу

АЛГОРИТМ ПЕРЕВІРКИ ЦІЛІСНОСТІ ЦИФРОВОГО ЗОБРАЖЕННЯ

У роботі було розроблено алгоритм перевірки цілісності цифрового кольорового зображення-контейнеру з урахуванням можливості виходу за межі діапазону значення яскравості пікселя матриці зображення на етапі кодування. Проаналізовано розбиття матриці зображення на блоки різного розміру, обчислювання частотних коефіцієнтів дискретного косинус перетворення для блоків аналізованих розмірів. Отримано, що для блоків 2×2 ДКП та ДФП мають однакове формування частотних коефіцієнтів. Було розроблено програмний продукт, що реалізує розроблений алгоритм з окремими частинами для кодування та перевірки цілісності.

Ключові слова: дискретне косинус перетворення, цифрове зображення, цілісність контейнер, цілі частотні коефіцієнти.

Вступ і постановка задачі

У наше століття мережеві технології розвиваються з величезною швидкістю, росте пропускна здатність і обчислювальна потужність мережевих систем, винаходяться нові механізми їх взаємодії. Тому все гостріше стоїть питання захисту інформаційних об’єктів, що переміщуються або розміщуються у мережах. На жаль сьогодні дуже частим є несанкціоноване втручання у роботу мережевих систем, третіх осіб, які намагаються отримати доступ до конфіденційної інформації, що є інтелектуальною власністю компаній. Також дуже часто їх зусилля спрямовані на руйнування та спотворення вищезазначених об’єктів.

Таким чином, на наш погляд, сьогодні є дуже *актуальним* питання розробки нових сучасних комплексних методів і програмних продуктів захисту цифрової інформації. У відкритій мережі Інтернет були знайдені наукові статті цього напрямку, якими займаються автори. Так, у роботі [1] був запропонований метод вбудови інформації в область перетворення Фур'є для зображень в градаціях сірого, не порушуючи надійності сприйняття сформованого стеганоповідомлення з використанням блоків 2×2. Їх автентичність здійснюється шляхом вбудовування великого обсягу інформації в кожен блок розбиття. У роботі [2] автори запропонували поліноміальний комплексний метод виявлення областей клонування як фальсифікації цифрового зображення (ЦЗ), що дозволяє локалізувати клоновані ділянки з високою точністю.

Автори цих робіт, завдяки пошукам у області стеганографії [3,4] пропонують алгоритм перевірки цілісності, кольорових цифрових зображень, щодо несанкціонованих змін, зробленими третіми особами, з наміром зміни або руйнування цих цифрових об’єктів.

У відкритій пресі знайдено ефективні стеганографічні методи з використанням блоків малого розміру [1, 5]. У роботі [1] автори використовують блоки розміром 2×2 для вбудови інформації в область перетворення Фур'є (ДПФ), як було зазначено вище. У науковій роботі [6] автори використовують блоки розміром 2×2 для вбудови інформації у область перетворення Хартлі. У науковій роботі [5] запропонований стеганографічний метод, який заснований на вбудові конфіденційної інформації в частотну область контейнера, в якості якого виступає цифрове зображення в градаціях сірого. Перехід з просторової в частотну область і навпаки відбувається, використовуючи дискретне перетворення Фур'є. Матриця частотних коефіцієнтів будується для блоків розбиття вихідної матриці цифрового зображення розміром 2×2. За рахунок вибору блоку такого розміру не тільки збільшена пропускна здатність каналу зв’язку, в порівнянні зі стандартною розбивкою, але і отримано нульовою мнима частина частотних коефіцієнтів.

У проаналізованих вище роботах проводилися модифікації цифрових зображень у області перетворення, та обґрунтування області ДФП.

Метою даної роботи є розробка алгоритму перевірки порушення цілісності цифрового кольорового зображення-контейнера щодо несанкціонованих змін, з урахуванням можливості виходу за межі діапазону значення яскравості пікселя матриці зображення на етапі кодування.

З урахуванням вище зазначеного огляду, теми і мети представлена робота є *актуальною*.

Основна частина

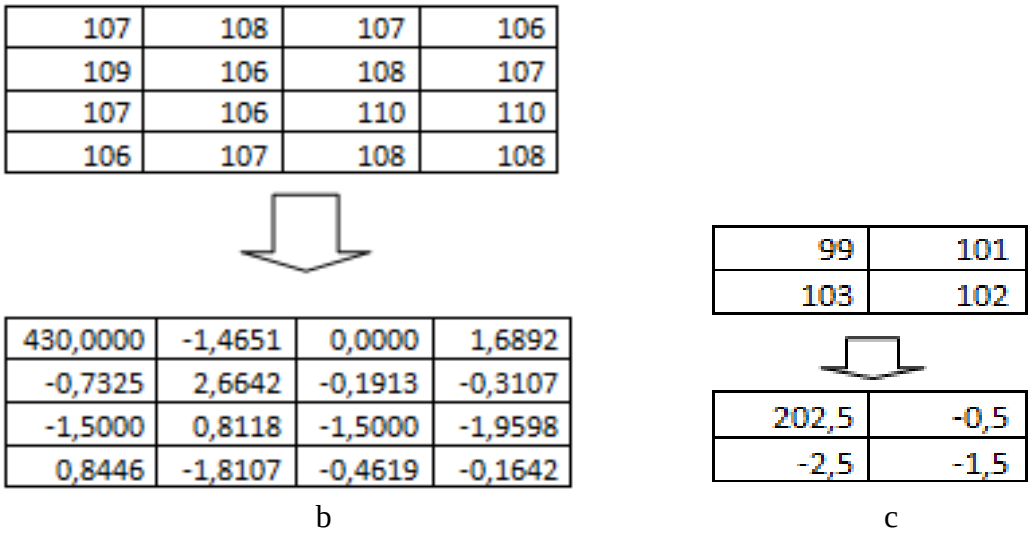
Перш за все, у даної роботі автори проаналізують дискретне косинус перетворення (ДКП), яке є ключовим кроком алгоритму стиснення, та різновидом перетворення Фур'є, і є також, не менш використовуваним при розробці сучасних методів та алгоритмів у області захисту інформації, ніж ДПФ. Крім того на базі вже отриманих результатів [4-6] пропонується алгоритм для перевірки цілісності контейнера, з програмною реалізацією, що виділяє область порушення цілісності блоків.

Важливим кроком для досягнення поставленої мети у роботі – є вибір розміру блоку розбиття матриці зображення. Для цього проводимо аналіз блоків різного розміру, які формуються після перетворення дискретно косинусного перетворення (ДКП), як стандартного 8×8 так і найменшого 2×2 (рис.1).

107	108	107	106	99	101	102	107
109	106	108	107	103	102	103	110
107	106	110	110	106	107	107	120
106	107	108	108	108	108	108	114
105	108	109	109	108	106	107	110
105	108	109	110	108	108	109	109
108	109	109	109	108	109	110	109
107	107	108	108	107	110	110	109

861,25	-3,09462	4,302372	-10,0126	2,75	-0,33337	2,547468	-2,43607
-7,54874	3,865634	5,626946	-5,89407	4,354338	-0,8037	2,638685	-1,31234
-5,59932	5,325041	2,207107	1,836577	-1,9038	2,501025	-1,11E-16	-0,96269
-5,17406	5,471604	-2,33263	0,457864	-2,60875	0,648556	-2,9587	-0,14931
-3,25	0,770863	-0,38268	1,201039	-1,75	-0,52472	-0,92388	-0,25088
2,11593	-1,38623	1,008855	0,25211	-0,80462	-0,47563	-0,12777	-0,79616
1,50752	-2,92313	3,33E-16	-2,02255	-0,02321	-0,03808	0,792893	-1,30467
1,420729	-0,20878	0,665015	-1,92853	0,58031	-0,35853	0,45099	-0,34787

а



107	108	107	106
109	106	108	107
107	106	110	110
106	107	108	108

430,0000	-1,4651	0,0000	1,6892
-0,7325	2,6642	-0,1913	-0,3107
-1,5000	0,8118	-1,5000	-1,9598
0,8446	-1,8107	-0,4619	-0,1642

99	101
103	102

202,5	-0,5
-2,5	-1,5

b c

Рис 1. ДКП для блоків різного розміру: a - 8×8, b - 4×4, c - 2×2.

Так як формули отримання частотних коефіцієнтів ДФП і отримані результати (рис.1) для розміру блока розбиття 2×2 у даній роботі та у роботі [5] мають однакове формування частотних коефіцієнтів, то саме їх використовуємо у алгоритмі, що розроблюється.

У якості контейнера виступає кольорове цифрове зображення. Вибране зображення можливо представити у вигляді розкладання трьох матриць кольорової моделі RGB: червоної (Red), зеленої (Green), блакитної (Blue). Нехай B - матриця, розміром $M\times N$ — одна з кольорових складових цифрового зображення - контейнера довільного формату, для зберігання якого використана модель RGB. Далі всі наступні перетворення цифрового зображення формально будуть представлятися як перетворення *B*.

Розіб'ємо матрицю *B* на неперетинні блоки, розміром 2×2.

Для отримання цілих частотних коефіцієнтів, які на етапі перевірки цілісності цифрового зображення дадуть змогу отримати область перевірки цілісності, треба врахувати коефіцієнт ½, який з'являється при формуванні частотних коефіцієнтів саме блоків розміром 2×2 [5]. Для цього у роботах [3,5,7, 8] запропоновано декілька способів урахування цього. У даній науковій роботі запропоновано вираховувати суму коефіцієнтів для блоку розбиття (*bl*) у просторовій області. Якщо результат суми (S) є непарним (використовуємо функцію залишку при діленні на число 2 - mod), то потрібно вдатися до корегування одного з коефіцієнтів просторової області блоку, що аналізується. У разі отримання парного числа – корегування блоку не потрібно.

S=sum (bl);
if mod(S, 2) ~ =0
Потрібне коригування
Else
Не потрібне коригування

Якщо потрібно корегування одного з коефіцієнтів блоку для врахування коефіцієнту ½ достатньо змінити його на 1 одиницю. При зміні просторового коефіцієнту необхідно враховувати те, що значення яскравості пікселя матриці зображення знаходиться у границях [0; 255]. І щоб уникнути виходу за ці границі діапазону запропоновано наступне корегування [7,8]:

```
if   bl (i,j)>254;
bl (i,j)=bl(i,j)-1 ;
else
bl (i,j)=bl(i,j)+1;
```

Завдяки вибору розміру блоку розбиття матриці зображення, а також попереднього коригування значень елементів яскравості для блоку в просторової області отримуємо цілі значення частотних коефіцієнтів ДКП, зазначені властивості яких при декодуванні будуть використані для перевірки цілісності контейнера.

Проведений практичний аналіз на зображеннях різного жанру, кольоровості, взяті з власного архіву та з бази тестових зображень (200 цифрових зображень) показав, що довільні зображення мають дуже малу кількість блоків, а саме менше 1%, у більшості не мають зовсім, де просторові коефіцієнти цього блоку належать множині цілих чисел.

На етапі декодування (перевірки цілісності) для кожного отриманого коефіцієнта блоку, що аналізується, потрібна перевірка на належність множині цілих чисел:

```
for i=1:2
for j=1:2
if mod(bl1(i,j)*10,10) ~= 0
Цілісність блоку порушена;
break;
else
Цілісність блоку не порушена
end
end
end
```

Для зручності користувача, у разі порушення цілісності блоку при реалізації програмного продукту, коригуються усі коефіцієнти блоку, що аналізується, змінюючись на 0. Ця задумка робиться для того, щоб той, хто аналізує отримане зображення, бачив на ньому області, які не пройшли перевірку цілісності.

У зв’язку з тим, що реалізація стеганографічного алгоритму потребує багато математичних обчислень, зручно використовувати інтерактивне середовище для програмування, чисельних розрахунків і візуалізації результатів при цьому мову програмування. У зв’язку з цим був обраний MATLAB – пакет прикладних програм для вирішення задач технічних обчислень і однойменна мова програмування, що використовується в цьому пакеті. За допомогою MATLAB можна аналізувати дані, розробляти алгоритми, створювати моделі і додатки. Реалізація інтерфейсу була розроблена за допомогою середовища GUIDE. Середовище GUIDE входить до складу пакету MATLAB і служить для створення додатків з графічним інтерфейсом користувача.

Для того, щоб розпочати роботу з програмним продуктом необхідно запустити відповідний m-файл (start.m). Після запуску на екрані з’явиться стартова сторінка програмного продукту, на якій буде запропоновано обрати необхідну функцію “Кодування” чи «Перевірка цілісності» (рис. 2).

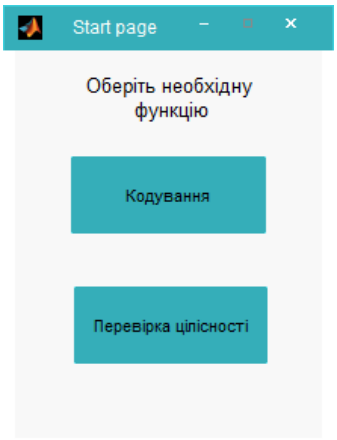


Рис. 2 – Стартова сторінка

Заздалегідь, для демонстрації роботи програмного продукту, ми попередньо змінили за допомогою одного з відомих графічних редакторів зображень певну інформацію на цьому зображенні. А саме – вихідні реквізити для відправлення грошей. Нижче наведено приклад роботи з формою (рис. 3).

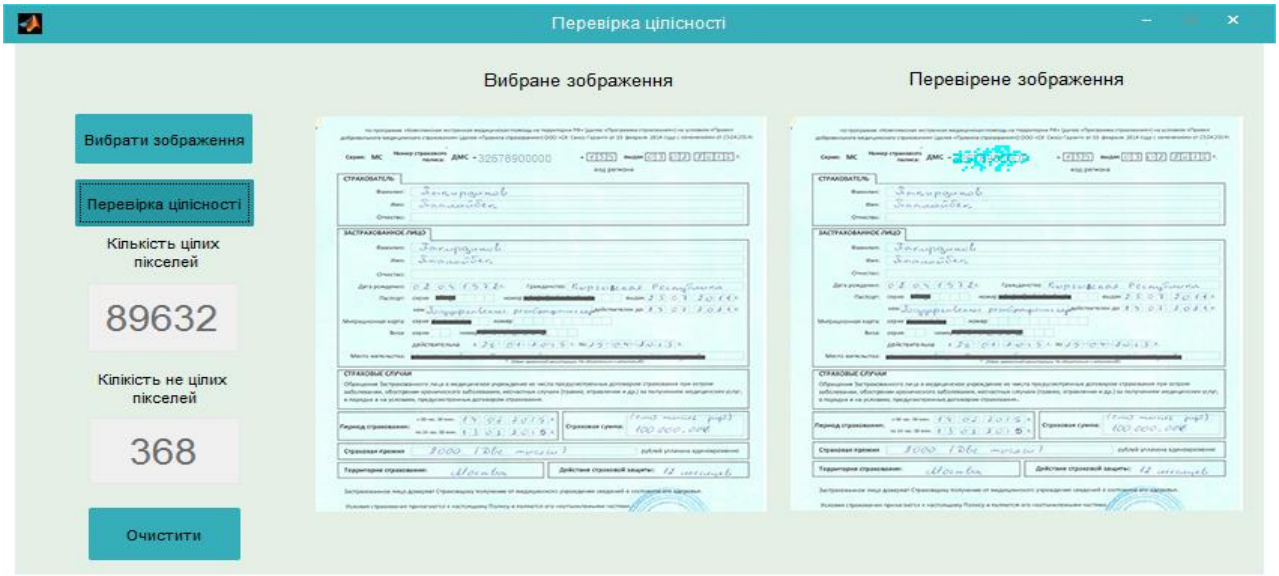


Рисунок 3 – Перевірка порушення цілісності зображення

Запропонована програмна реалізація алгоритму може допомогти при розробці комплексної системи захисту інформації на підприємстві. Вона допоможе зрозуміти, яку інформацію треба запросити ще раз, а на яку потрібно не зважати уваги.

У роботі були визначені помилки 1-роду. Помилкою 1-роду вважається вірогідність виявлення порушення цілісності у кодованому цифровому зображенні, з яким нічого не відбулося. Помилки 1-роду могли виникнути за рахунок випаду значень яскравості пікселів за границі діапазону, що було враховано у розробленому алгоритмі. При перевірці порушення цілісності зображення у нашому прикладі отримана вірогідність дорівнює 0%.

Висновки

У представленій науковій роботи для досягнення поставленої мети була обрана область перетворення ДКП. Проаналізовано розбиття матриці зображення на блоки різного розміру та обчислювання частотних коефіцієнтів дискретно косинусного перетворення для блоків отриманих розмірів. Отримано, що для блоків 2×2 ДКП та ДФП мають однакове формування частотних коефіцієнтів.

Для перевірки цілісності цифрового кольорового зображення-контейнеру від несанкціонованих змін було розроблено алгоритм та програмний продукт, що його реалізує. Алгоритм враховує можливість виходу за межі діапазону значення яскравості пікселя матриці зображення на етапі кодування. Програмна реалізація алгоритму виявляє несанкціоновані зміни навіть в один піксель, Крім того, з її допомогою також буде виявлено блок розміром 2×2, у якому ця зміна відбулася. Похибки 1-роду відсутні.

Література

1. Nabin Ghoshal. Image Authentication Technique in Frequency Domain based on Discrete Fourier Transformation (IATFDDFT) / Nabin Ghoshal , J. K. Mandal - Proceedings of ICCS - 2010, November 19, 2010 - November 20, 2010. –P.144-150.

2. Зорило В.В. Комплексный метод выявления и локализации областей клонирования в цифровых изображениях/ В.В. Зорило, Е.Ю. Лебедева// Праці Одеського політехнічного університету. – 2015. – Вип.1. – С.101-106.

3. Кобозева, А.А. Стеганографический метод, обеспечивающий проверку целостности и аутентичности передаваемых данных / А.А. Кобозева, М.А. Козина // Проблемы региональной энергетики. Электронный журнал Академии наук Республики Молдова. – 2014. – №3 (26). – С. 93-106.

4. Козина, М.А. Стеганографический метод организации скрытого канала связи, осуществляющий проверку целостности передаваемой информации / М.А. Козина // Сучасна спеціальна техніка. – 2014. – №4 (39). – С. 98-106.

5. Kozina M.O. Discrete Fourier transform as a basis for steganography method / M. O. Kozina // Праці Одеського політехнічного університету. – 2014. – Вип.2(44). – С.118-126.

6. Kozin A. Steganography method using Hartley transform / A. Kozin, O. Papkovskaya, M. Kozina // Сучасні проблеми радіоелектроніки, телекомунікацій, комп'ютерної інженерії: матеріали XIII Міжнар. конф., 23.02–26.02.2016 р., Львів, Славське, Україна / Нац. ун-т "Львів. політехніка". – Л. : Вид-во Львів. політехніки, 2016. – С. 473-475.

7. Кремінський В.Ю. Стеганоалгоритм перевірки цілісності цифрового контейнеру / В.Ю.Кремінський, Софі Маріан Нджикє Амугу, М.О.Козіна / 13 Всеукраїнська конференція студентів і молодих науковців «Інформатика, інформаційні системи», 8 квітня 2016р. – Одеса, 2016. –С.59-60.

8. Kreminskiy V. Steganography algorithm checking the integrity of the digital image / V. Kreminskiy // 53 Konferencja Studenckich Kół Naukowych pionu hutniczego Akademii Górniczo-Hutnicza im. Stanisława Staszica w Krakowie, 12 maja 2016.- Kraków, 2016. - C. 247.

Надійшла 28.11.2016 р. Рецензент: д.т.н., проф. Єрохін В.Ф.