УДК 004.932.2

К.О. Трифонова,
ОНПУ, пр. Шевченко 1, Одеса,

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ МЕТОДУ ВИЯВЛЕННЯ НЕСАНКЦІОНОВАНОГО ВТРУЧАННЯ «COPYPASTE» В ЦИФРОВЕ ЗОБРАЖЕННЯ

The way of increasing the efficiency of digital image detection and localization of unauthorized interference “copypaste” method based on analyzing the singular numbers of the corresponding matrix.

Keywords - falsification, localization, identification, quantification, singular number

Запропоновано спосіб підвищення ефективності методу виявлення та локалізації несанкціонованого втручання “copypaste”, заснованого на аналізі сингулярних чисел відповідної матриці.

Ключові слова – фальсифікація, локалізація, ідентифікація, квантування, сингулярні числа

Вступ

Процес впровадження нових інформаційних технологій в усі сфери життя суспільства неможливий без вирішення питання інформаційної безпеки. Складовою частиною якого є задача визначення автентичності цифрових зображень, створення методів для виявлення несанкціонованого втручання.

Важливість поданої задачі для сучасності примушує багатьох вчених шукати шляхи та методи її розв’язку, спираючись на техніку цифрових водяних знаків [1], техніку, основану на місцеположенні джерела світла при генерації цифрового зображення [2], ідентифікації цифрового пристрою, за допомогою якого було створено цифрове зображення [3,4] та ін. Методи, інформація про які доступна з відкритого друку, ніяк не пов’язані між собою, часто не мають строгого математичного обґрунтування отриманих результатів, не представляють цілісного апарату, що б ґрунтувався на єдиній математичній базі. Все це примусило шукати принципово нові математичні інструменти та підходи до розв’язку поставленої задачі в цілому, результатом чого став запропонований в [5,6] загальний матричний підхід визначення фальсифікації цифрового сигналу. Відповідно до даних основ, запропоновані математичні параметри, що несуть в собі інформацію про стан, а їх обурення - інформацію про зміну стану цифрового сигналу. Різні способи обурення (зокрема, різні способи несанкціонованого втручання) цифрового сигналу приводять до різних характерних збурень математичних параметрів, що сигналізують про відповідні збурюючи впливи.

Одним з найбільш поширених способів несанкціонованого втручання в цифровий сигнал є обурення, засноване на заміщенні, так зване «copypaste»: частина цифрового сигналу, замінюється частиною іншого цифрового сигналу - вклейкою.

Тому метою даної статті є підвищення ефективності методу визначення та локалізації несанкціонованого втручання «copypaste» в одному з найбільш поширених контентів – цифровому зображенні, на основі встановлених властивостей виділених математичних параметрів, що характеризують локалізацію обурюючого впливу (несанкціонованого втручання) на цифрове зображення.

Вплив стиску на сингулярні числа блоків матриці цифрового зображення

На даний час зберігання і передача цифрових сигналів по каналах комунікацій у зв'язку зі значним збільшенням обсягів інформації здійснюється в стислому стані з різними параметрами. Завдяки цьому обурення цифрового сигналу, засноване на заміщенні, розглянуто як обурення цифрового зображення вклейкою частини іншого цифрового зображення, що було стиснено з деякими параметрами.

На підставі загального підходу до виявлення фальсифікації цифрового сигналу [5,6] проведений обчислювальний експеримент для аналізу сингулярних чисел блоків цифрових зображень показав, що кількість нульових сингулярних чисел блоків є властивістю, яка надає можливість розрізняти, блоки цифрового сигналу вихідного і отриманого після стиснення часткового або повного відновлення [5,6].

При цьому аналіз частково відновленого зображення 100% демонструє результат впливу стиснення, на відміну від повністю відновленого, отриманого з частково відновленого завдяки округленню.

Тому для підвищення ефективності відділення блоків вихідного цифрового зображення від блоків зображення вклейки має сенс аналізувати матрицю відповідну частково відновленої.

Для вирішення поставленої задачі запропонований підхід, завдяки якому будується матриця квантованих частотних коефіцієнтів, зворотне ДКП якої відновить необхідну для проведення аналізу матрицю.

Також встановлено, що для матриці, побудованої таким чином, кількість нульових сингулярних чисел блоків представляє собою нормально розподілену випадкову величину.

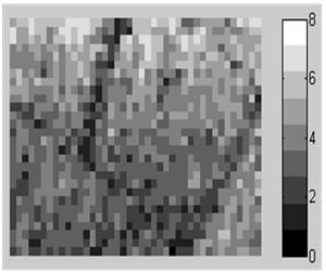
Метод виявлення обурення цифрового зображення, заснованого на заміщені

На основі отриманих результатів створено практичний метод виявлення та ідентифікації несанкціонованого втручання в цифрове зображення обуренням, заснованим на заміщенні.

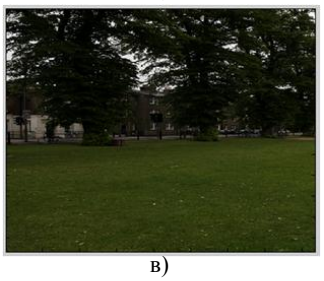
Вважаємо, що в нашому розпорядженні є цифрові зображення, отримані сучасними цифровими фотокамерами. Серед них як зображення, повністю відновлені після застосування різних реалізацій з різними параметрами процедур стиснення, так і збережені в форматі без втрат.

Нехай частина основного зображення (ОЗ), замінюється деякою іншою областю (ЗО), передбачається, що ЗО менше половини ОЗ (для

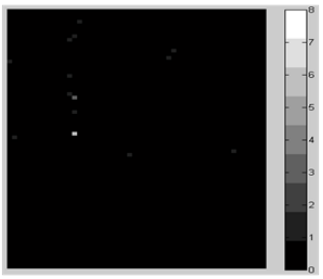
а)



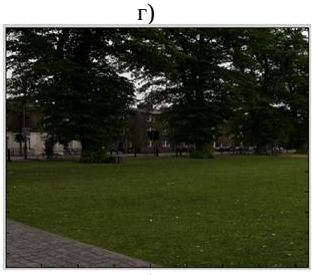
б)



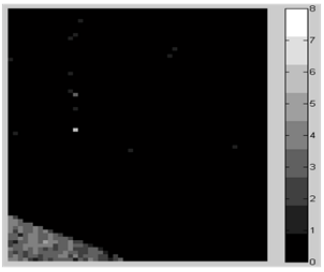
в)



г)



д)



е)

Рис. 1 а) ЗО в) ОЗ д) цифрове зображення, отримане в результаті «copypaste» б) МНСЧБ ЗО г) МНСЧБ ОЗ е) МНСЧБ цифрового зображення отриманого в результаті «copypaste»

більшої наочності одержуваних нижче висновків ніяка подальша обробка зображення не виконується).

Таке обурення цифрового зображення, засноване на заміщенні, приклади якого на основі зображень (рис. 1а, 1б), демонструють «copyraste», представлені на (рис. 1в) зберігаються без втрат.

При побудові матриці нульових сингулярних чисел блоків отриманого цифрового зображення частини, що відповідають ОЗ і ЗО, будуть відрізнятися:

- підобласть матриця нульових сингулярних чисел блоків, яка відповідає області, що зберігалася без втрат, буде, як випливає з вищесказаного, містити велику кількість нулів;
- підобласть матриці нульових сингулярних чисел блоків відповідна області, яка була піддана певній мірі стиснення, буде складатися з нормально розподілених ненульових значень з відповідним значенням математичного очікування і середньоквадратичним відхиленням.

Графічне представлення матриці нульових сингулярних чисел блоків результуючих цифрових зображень наочно демонструє відповідні підобласті (рис. 1е).

Таким чином, якщо ОЗ відрізняється від ЗО ступенем стиснення, причому результуючий сигнал збережений без втрат, то основні кроки запронованого методу, виявлення обурення цифрового сигналу, заснованого на заміщення, будуть наступними:

1. Побудова матриці цифрового зображення.
2. Розбиття отриманої матриці стандартним чином на блоки 8x8.
3. Побудова матриці I , що відповідає частково відновленої.
4. Побудова для I матриці нульових сингулярних чисел блоків M .
5. Виявлення: виділення в M областей, необов'язково прямокутних, що становлять менше половини розглянутого цифрового сигналу, таких що:
   a. $O_1, O_2, ..., O_m$ більшість елементів яких мають нульове значення;
   b. $O_1, O_2, ..., O_m$ більшість елементів яких мають ненульове значення.
6. Ідентифікація:
   a. $O_1, O_2, ..., O_m$ - є результатом «copyraste» з цифрового сигналу в форматі без втрат;
   b. області з $Z_1, Z_2, ..., Z_p$, для яких підтверджується гіпотеза про нормальну функцію розподілу для кількості нульових сингулярних чисел блоків цифрового сигналу, є результатом «copyraste» з цифрового сигналу для якого застосовувалося стиснення.

Висновок

Використовуючи отримані результати розроблений метод є більш ефективним при виявленні і локалізації несанкціонованого втручання в цифрове зображення, ніж метод отриманий раніше [5].

1. Fridrich J. Invertible authentication. / J.Fridrich, M. Goljan, R.Du.// Proc. SPIE Photonics West, Security and Watermarking of Multimedia Contents III. – 2001. – Vol.3971. – P.197 – 208.

2. Johnson M.K. Exposing digital forgeries by detecting inconsistencies in lighting. / M.K Johnson, H. Farid // Proc. ACM Multimedia and Security Workshop. – 2005. – P.1– 10.

3. Fridrich J. Determining image origin and integrity using sensor noise // M. Chen, J. Fridrich, M. Goljan , J. Lukas// IEEE Transactions on Information Forensics and Security. – 2008. – Vol. 3. – P.74 – 90.

4. Fridrich J. Detecting digital image forgeries using sensor pattern noise. // J. Lukas, J. Fridrich, M Goljan // Proc. SPIE, Electronic Imaging, Security, Steganography and Watermarking of Multimedia Contents VIII. – 2006. –Vol.6072. - P.1-11.

5. Кобозева А.А. Матричний аналіз - основа загального підходу до виявлення фальсифікації цифрового сигналу / А.А. Кобозева, О.В. Рибальський, Е.А. Трифонова / / Вісник Східноукраїнського національного університету ім. В. Даля. - 2008. - № 8 (126), ч.1. - С.62-71.

6. Кобозева А.А. Комплексний підхід до експертизи автентичності матеріалів цифрового звукозапису / А.А. Кобозева, О.В. Рибальський, Е.А. Трифонова [и др.] / / Вісник Східноукраїнського національного університету ім. В. Даля. - 2009. - № 6 (136), ч.1. - С.75-78.