УДК 004.056

ПІДХОДИ ТА МЕТОДИ ВИРІШЕННЯ ЗАДАЧІ ВИЯВЛЕННЯ ПОРУШЕНЬ ЦІЛІСНОСТІ ЦИФРОВОГО ЗОБРАЖЕННЯ

Зоріло В.В.[1)], Якименко І.З.[2)], Волощук О.М.[3)]

[1)] Одеський національний політехнічний університет, старший викладач
[2)] Тернопільський національний економічний університет, к.т.н., доцент
[3)] Тернопільський національний економічний університет, магістрант

I. Постановка задачі

Цифрове відео представляє собою послідовність кадрів, тобто аналіз цифрового відео на наявність фальсифікації може бути зведений до аналізу окремих кадрів відео послідовності (цифрових зображень). Тому для простоти викладання далі мова йтиме про цифрові зображення, але усі отримані результати можуть бути використані і для цифрових відео-послідовностей також.

Так як існує безліч способів зміни стану цифрового зображення (ЦЗ), що відрізняються за своєю суттю і спрямованістю, існує й безліч методів виявлення наслідків впливу на них чи порушення їх цілісності.

Дані обставини зумовлюють необхідність постійного розвитку та удосконалення методів захисту інформації.

II. Мета роботи

Метою дослідження є розробка методу виявлення клонування як фальсифікації цифрової інформації.

III. Класифікація методів захисту цифрових зображень

Усі методи захисту інформації можна розділити на методи активного захисту (МАЗІ), спрямовані на запобігання несанкціонованого доступу, витоку, зміни інформації, і методи пасивного захисту інформації (МПЗІ), призначені для того, щоб визначити, чи було зроблено навмисне порушення цілісності інформації [1] (таблиця 1).

МАЗІ за способом їх реалізації поділяють на програмні, криптографічні, технічні та організаційні.

МПЗІ в свою чергу поділяють за способом їх реалізації на методи експертної оцінки, програмно-технічні та програмні.

Таблиця 1

Класифікація методів захисту інформації

Методи захисту інформації						
Методи активного захисту інформації				Методи пасивного захисту інформації		
Програмні	Криптографічні	Технічні	Організаційні	Програмні	Програмно-технічні	Експертної оцінки

Програмно-технічні МПЗІ ґрунтуються на знаннях та аналізі специфічних особливостей пристроїв аудіо-, відео-або фото фіксації та (або) впливу будь-яких зовнішніх факторів на проведення запису.

Широке поширення сьогодні набули методи, засновані на аналізі EXIF-даних – додаткової інформації, що додається в медіафайли цифровою технікою безпосередньо при їх створенні [2]. За допомогою EXIF-даних можна встановити умови і способи отримання медіафайлу, авторство, координати місця зйомки (за наявності вбудованого приймача GPS) і т.д.

Недоліки цих методів полягають у тому, що, по-перше, існує програмне забезпечення для зміни EXIF-даних з метою виправлення автоматично зміненої в процесі обробки файлу інформації, по-друге, дані методи дозволяють зробити висновок про можливе редагуванні файлу, але не визначають

область і характер редагування, що не дає можливості використання їх для достовірного дослідження ЦЗ на предмет порушення цілісності.

Основним недоліком програмно-технічних методів захисту інформації є жорстка прив'язаність до технічного пристрою, його можливостей і властивостей або впливу оточуючих факторів на запис сигналу. Крім того в більшості випадків при виявленні фальсифікації дані методи не здатні локалізувати її область.

На відміну від програмно-технічних і експертних методів програмні методи не мають прив'язки до технічних пристроїв, за допомогою яких було отримано інформацію, а також не вимагають участі експерта в ідентифікації порушень її цілісності.

Неможливо гарантувати абсолютну успішність МАЗІ в будь-якій системі захисту інформації, що робить МПЗІ обов'язковою складовою частиною комплексної системи захисту інформації; крім того, якщо несанкціоновані зміни інформаційного контенту відбулися поза розглянутої інформаційної системи, вони принципово не можуть бути попереджені МАЗІ, а можуть бути виявлені тільки за допомогою МПЗІ, що визначає важливість, потребу і значимість цієї категорії методів в абсолютному значенні.

На даний час активно розвивається галузь експертизи цифрових контентів, створюються нові та вдосконалюються існуючі програмні методи виявлення порушень цілісності ЦЗ, таких як клонування (заміна частини основного зображення замінюється частиною цього ж зображення) [1,2], колаж (комбінація частин різних зображень) [1], масштабування (зміна розмірів та (або) поворот частин ЦЗ) [7], корекція яскравості [4], пост обробка ЦЗ після його фальсифікації (ретуш, зміна різкості, регулювання контрасту, розмиття).

Активно протягом останнього десятиріччя розвиваються методи виявлення порушень цілісності цифрових зображень [1-6], засновані на загальному підході до аналізу стану та технології функціонування інформаційної системи (ЗПАІС), який у свою чергу базується на матричному аналізі та теорії збурень. Головні положення ЗПАІС у контексті ЦЗ коротко описані далі.

Оскільки будь-яка матриця однозначно визначається своїм сингулярним спектром – множиною сингулярних чисел (СНЧ) і набором сингулярних векторів (СНВ) спеціального виду, які отримуються за допомогою нормального сингулярного розкладання матриці (SVD) [26], то при вибраному матричному способі формалізації визначається сингулярним спектром (спектрами) і набором (наборами) СНВ відповідної йому матриці (матриць): СНЧ і СНВ несуть в собі всю інформацію про стан ЦЗ.

Активно протягом останнього десятиріччя розвиваються методи виявлення порушень цілісності цифрових зображень [8], засновані на загальному підході до аналізу стану та технології функціонування інформаційної системи (ЗПАІС), який у свою чергу базується на матричному аналізі та теорії збурень. Головні положення ЗПАІС у контексті ЦЗ коротко описані далі.

В якості математичної моделі цифрового зображення можна використовувати його матрицю (скінчену множину матриць) яскравості пікселів. Властивості ЦЗ, незалежно від його конкретного виду, будуть визначатися математичними властивостями відповідних матриць.

Оскільки будь-яка матриця однозначно визначається своїм сингулярним спектром – множиною сингулярних чисел (СНЧ) і набором сингулярних векторів (СНВ) спеціального виду, які отримуються за допомогою нормального сингулярного розкладання матриці (SVD) [4], то при вибраному матричному способі формалізації визначається сингулярним спектром (спектрами) і набором (наборами) СНВ відповідної йому матриці (матриць): СНЧ і СНВ несуть в собі всю інформацію про стан ЦЗ.

IV. Метод виявлення клонування як фальсифікації цифрової інформації

Виходячи із огляду літературних джерел стосовно вирішення задач виявлення порушень цілісності ЦЗ на даний момент найбільш перспективним є загальний підхід до аналізу стану та технології функціонування інформаційної системи (ЗПАІС).

У розробленому методі порівнюються суми СНЧу блоках (для клонованих блоків ці суми будуть рівні). Імовірність рівності сум СНЧ блоків, відмінних один від одного, дуже мала для ЦІ хорошої якості($Q \geq 8$). Збільшення ступеня стиснення ЦІ з погіршенням його якості призведе до появи помилок 2 роду, тобто до виникнення блоків ЦІ, хибно прийнятих клонованими, як буде показано нижче. Будемо вважати виявленими як клоновані ті блоки ЦІ, які мають рівні за значенням СНЧ. Так як при здійсненні фотомонтажу ймовірність збігу сіток розбиття на блоки ОІ та ЗО мала [97, 98], з метою виявлення об'єкта клонування розіб'ємо матрицю (матриці) ЦІ на пересічні блоки таким чином, щоб кожен блок відрізнявся від того який поруч стоїть на 1 стовпець (рядок). Будемо порівнювати між собою значення сум 4 найбільших СНЧ блоків матриць ЦІ, що не вплине на якість

виявлення фальсифікації, однак зменшить обчислювальну складність алгоритму методу виявлення клонування. Поставимо у відповідність ЦІ матрицю клонування (МК).

Даний підхід ефективний в умовах проведення фотомонтажу шляхом клонування однієї частини ЦЗ в іншу, а також в умовах симетричного клонування і при повороті об'єкта клонування в будь-якому напрямку на кут, кратний 90 градусам. Однак для СК і повороту на вказаний кут всередині ЗО можуть виявитися блоки, які не будуть виділені як фальсифікація. У разі малого розміру ЗО це може призвести до появи помилок 1 роду. На основі проведеного аналізу розроблено метод виявлення клонування (МВК) як фальсифікації ЦІ, основні кроки якого представлені нижче.

Розбити матрицю F ЦІ на 8×8 -блоки, які перетинаються $F_{ij}, i=1,2\ldots,(n-7), j=1,2\ldots,(m-7)$ так, щоб кожний блок відрізнявся від сусіднього на один стовбець (строку).

Побудувати матрицю S з елементами $s_{ij}=\sum_{k=1}^{4}\sigma_k$, $i=1,2\ldots,(n-7)$, $j=1,2\ldots,(m-7)$, де $\sigma_1,\sigma_2,\sigma_3,\sigma_4$ – найбільші СНЧ відповідного блоку $F_{ij}, i=1,2\ldots,(n-7), j=1,2\ldots,(m-7)$.

Побудувати матрицю клонування (МК) C з елементами c_{ij}, $i=1,2\ldots,(n-7)$, $j=1,2\ldots,(m-7)$; c_{ij} яка відповідає блоку F_{ij} ЦІ. Для визначення c_{ij} порівняти s_{ij} попарно з всімі елементами матриці S:

Якщо для s_{ij} знайдеться елемент $s_{kl}, k\neq i, l\neq j$, матриці S , що $\left|s_{ij}-s_{kl}\right|<\delta$

то $c_{ij}=1$, в іншому випадку $c_{ij}=0$.

Елементи $c_{ij}=1$ матриці C відповідають клонованим блокам ЦІ.

Для ілюстрації роботи даного методу доцільно провести фальсифікацію ЦІ, наступним способом: за допомогою штампа замаскуємо гілку в правій частині ЦІ. Для фальсифікованого зображення побудуємо МК.

Висновок

У роботі розроблено ефективний підхід в умовах проведення фотомонтажу шляхом клонування однієї частини ЦЗ в іншу, а також в умовах симетричного клонування і при повороті об'єкта клонування в будь-якому напрямку на кут, кратний 90 градусам.

Список використаних джерел

1. Pan, X. Region Duplication Detection Using Image Feature Matching / X. Pan, S. Lyu // IEEE Transactions on Information Forensics and Security. — 2010. — Vol. 5, No. 4. — PP.857–867.
2. Wang, J. Detection of image region duplication forgery using model with circle block / J. Wang, et al. // MINES'09 Proceedings of the 2009 International Conference on Multimedia Information Networking and Security, November 18–20. – 2009. – Vol. 1. — PP. 25–29.
3. Кобозева, А.А. Матричный анализ – основа общего подхода к обнаружению фальсификации цифрового сигнала / А.А. Кобозева, О.В. Рыбальский, Е.А. Трифонова // Вісник Східноукраїнського національного університету ім. В. Даля. — 2008. — №8(126), Ч.1. — С. 62–72.
4. Кобозева, А.А. Анализ информационной безопасности: монография / А.А. Кобозева, В.А. Хорошко. — К.: ГУИКТ, 2009. — 251 с.
5. Бобок, И.И. Адаптация стеганоаналитического метода, основанного на теории возмущений, для задачи выявления нарушения целостности цифрового изображения / И.И. Бобок, Е.В. Малахов // Інформатика та математичні методи в моделюванні. — 2012. — Том 2, №4. — С. 297–303.
6. Зорило, В.В. Метод выявления симметричного клонирования при фальсификации цифрового изображения / В.В.Зорило, А.А.Кобозева, Е.Ю.Лебедева // Інформатика та математичні методи в моделюванні. — 2013. — Том 3, №1. — С. 5-12.
7. Bay, H. SURF: Speeded Up Robust Features / H. Bay, et al. // Computer Vision and ImageUnderstanding. — 2008. — Vol. 110, No. 3. — PP. 346–359.
8. Lowe, D.G. Distinctive Image Features from Scale-Invariant Keypoints / D.G. Lowe // International Journal of Computer Vision. — 2004. — Vol. 60, Iss. 2. — PP. 91–110.