DOI 10.15276/imms.v12.no1-2.46
УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 12 (2022), No. 1-2, pp. 46-52

ВИЯВЛЕННЯ ЧАСТИН ЦИФРОВОГО ЗОБРАЖЕННЯ, ЗМЕНШЕНИХ ПІСЛЯ ФАЛЬСИФІКАЦІЇ

В.В. Гулич, В.В. Зоріло, О.Ю.Лебедєва

1, пр.Шевченка, Національний університет «Одеська політехніка», 65044, Одеса
vikazorilo@gmail.com, whiteswanhelena@gmail.com

В час, коли використання цифрового контенту у всіх сферах життя неспинно зростає, можливість перевірки автентичності цифровіх файлів, зокрема, цифрових зображень, є вкрай важливою в галузі захисту інформації від порушень цілісності. В інформаційній війні повсякчас використовують фотофейки для досягнення певних, нерідко злочинних цілей. Як суспільство в цілому, так і окремі індивіди мають дбати про інформаційну безпеку та захищати свій інформаційний простір від неперевіреної інформації. Сучасні методи виявлення порушень цілісності графічної інформації певною мірою вирішують деякі питання інформаційної безпеки, однак, вони не є універсальними і часто потребують розвитку, вдосконалення, додаткових досліджень тощо. Так, існуючі методи виявлення такого поширеного способу фальсифікації зображень, як масштабування, є ефективними лише у випадках, коли фальсифікована частина збільшується, разом з цим при зменшенні частини зображення вони не є ефективними. Більше того, у відкритому друці проблема виявлення зменшених масштабованих частин зображення не висвітлена. Тому мета даної роботи - підвищення ефективності виявлення масштабування як фальсифікації цифрового зображення шляхом розробки алгоритму для детектування масштабування з від'ємним коефіцієнтом. В даній роботі проведено адаптацію метода аналізу рівня помилок для виявлення зменшених частин цифрового зображення. Ефективність адаптованого методу в термінах помилок 1 і 2 роду склала: помилки 1 роду – 2%, 2 роду – 7%. Крім того встановлено, що даний метод також є ефективним при виявленні одночасно масштабованих (зменшених) і переміщених частин цифрового зображення. Даний метод виявляє артефакти (помилки) на цифровому зображенні, які виникають при зменшенні його частини – фальсифікована ділянка має вищу високочастотну складову, ніж решта зображення, що підсилюється під впливом стиснення після збереження фальсифікації у форматі з втратами.

Ключові слова: виявлення фальсифікацій, цифрова криміналістика, масштабування.

Вступ

Сучасний світ дедалі більше стає залежним від зображень. Оскільки передача та засвоєння інформації відбувається значно легше за допомогою цифрового графічного контенту. Тому одним з головних питань постає оригінальність цього контенту, адже існує безліч способів фальсифікувати його, наприклад, клонування областей зображення, ретушування та накладання фільтрів, додавання сторонніх об'єктів до зображення та масштабування областей на зображенні.

Часто масштабування частин зображення застосовують під час його підробки як з додатнім (збільшення), так і з від'ємним (зменшення) коефіцієнтом. В той час як збільшенню у відкритому друці приділяється чимало уваги (ефективно себе показали методи, засновані на аналізі нульових сингулярних чисел блоків цифрового зображення), проблема зменшення взагалі не висвітлена. Відомі з відкритого друку методи виявлення масштабування не дають результатів при масштабуванні з від'ємним коефіцієнтом.

Мета даної роботи – підвищення ефективності виявлення масштабування як фальсифікації цифрового зображення шляхом розробки алгоритму для детектування масштабування з від'ємним коефіцієнтом.

Матеріали та методи

У той час, коли при збільшенні частини цифрового зображення відбувається додавання пікселів в збільшувану частину, яке виконується методом інтерполяції значень існуючих пікселів, при зменшенні частини зображення навпаки кількість пікселів зменшується, а розрахунок нових значень для пікселів, що лишилися, відбувається таким чином, аби зберегти інформативність підроблюваної частини. Якщо у першому випадку ставало більше низьких частот (фонових частин зображення), то у другому випадку контури стануть «щільнішими», збільшиться високочастотна складова зменшуваної частини, що в комбінації із стисненням після фальсифікації призведе до виникнення артефактів, або помилок. Виявлення артефактів, що виникають під час збереження зі стисненням, можна виконати методом Error lever analysis (ELA) [1].

В 2010 році П. Рінгвуд створив сервіс в вигляді веб-сайту під назвою «errorlevelanalysis.com». Але в 2012 році автор зачинив сайт. Після чого Hacker Factor відтворили веб-сайт Рінгвуда [2]. На сайті було створено алгоритм, який оцінює потенційний рівень помилок зображення в форматі JPEG, тобто вимірюється кількість змін під час повторного зберігання (рис. 1 – на зображення був доданий напис).

Рис. 1. Результат роботи алгоритму аналізу рівня помилок

Оскільки при редагуванні зображення змінені частини будуть мати потенційно збільшений рівень помилок, який не є характерним для більшої (нефальсифікованої) частини зображення, то даний алгоритм буде вказувати на наявність фальсифікації в конкретному місці.

Результати та обговорення

База для обчислювального експерименту по перевірці гіпотези щодо збільшеного рівня помилок в масштабованій частині зображення складається з 100 зображень з відкритого телеграм-каналу «Збройні Сили України. Війна з окупантами» [3]. Всі зображення мають різний розмір, роздільну здатність. Після цього всі зображення редагуються за допомогою графічного редактора Adobe Photoshop 2022.

Алгоритм редагування зображень такий.

1. Завантажуємо зображення і обираємо для нього профіль кольорів «Без змін».
2. За допомогою інструменту «Виділення об’єктів» виділяємо потрібний об’єкт на зображенні.
3. Копіюємо об’єкт на новий шар.
4. Робимо невидимим новий шар.
5. На оригінальному шарі знову обираємо об’єкт, що був скопійований на попередньому кроці.
6. Виконуємо заливку виділеної області «Права кнопка миші-Виконати заливку». Параметри заливки: зміст – з урахуванням змісту, режим накладання – нормальний.
7. Обираємо попередньо перенесений туди шар з об’єктом оригінального зображення та робимо його видимим.

8. Виконуємо масштабування об’єкту за допомогою трансформації. Комбінація клавіш Ctrl+T. Трансформуємо (зменшуємо) до потрібного вигляду в залежності від контексту.
9. Зберігаємо отримане зображення у форматі JPEG (параметри JPEG: якість – найкраща. Допустимі втрати 1% – менше виставити неможливо).

Пункт 6 – важливий етап виконання підробки. Заливка дозволяє виконати заповнення обраної частини зображення таким змістом, який схожий з суміжними ділянками зображення. Для отримання найкращих результатів обрана область повинна захоплювати область, яку ми хочемо відтворити на фінальному зображенні. Результат такої роботи показано на рисунку 1.

Рис. 2. Оригінальне (ліворуч) та фальсифіковане (праворуч) зображення

На фальсифікованому зображенні було зменшено чоловіка праворуч від танка. Для фальсифікованої частини відбулося збільшення високочастотної складової за рахунок маніпуляції із розміром цієї області, що саме по собі буде відрізняти цю частину від решти зображення, а в комбінації із стисненням при збереженні з втратами має проявитися ефект збільшення рівня помилок.

Основні кроки алгоритму виявлення фальсифікації наступні.

1) Завантажити зображення у форматі JPEG.
2) Виконати пере збереження даного зображення з завчасно визначеними втратами, які встановлюються вручну.
3) Розрахувати абсолютну (по модулю) попіксельну різницю між двома зображеннями, а саме початковим та збереженим із втратами.
4) Сформувати зображення з отриманої матриці різниці. Варто виділити, що мінімальна різниця буде сягати чисел, які будуть близькими до 0.
5) Знайти максимальні значення пікселів в кожному рядку матриці.
6) Серед мінімальних значень в рядках матриці знайти максимальне (k).
7) Розрахувати коефіцієнт за формулою: $255/k$.
8) Посилити яскравість всього зображення за допомогою визначеного коефіцієнту множенням його на кожен піксель зображення.
9) На отриманому зображенні виділити частини, що принципово відрізняються від решти зображення. Це і буде фальсифікація.

А на рисунку 3 представлено результати роботи алгоритму з тестовим зображенням, показаним на рисунку 1.

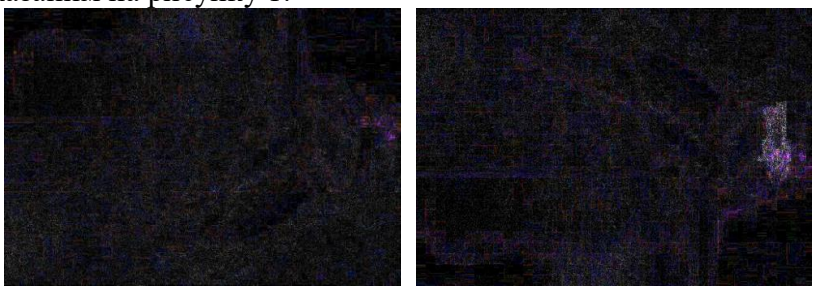

Рис. 3. Результат роботи алгоритму для оригіналу (ліворуч) та підробки (праворуч)

Як бачимо, на фальсифікованому зображенні явно виділена область масштабування, що є типовим результатом для даного експерименту (табл.1).

Таблиця 1

Результати роботи алгоритму пошуку масштабованого об'єкту

	Помилки 1 роду	Помилки 2 роду
Тестові зображення	2%	7%

Аналізуючи таблицю можна вважати, що при обробці оригінального зображення їх більшість не має жодних артефактів, що свідчить про те, що зображення не піддавалися редагуванню шляхом масштабування, а саме – зменшення. Артефакти присутні на 7% оригінальних зображень, що можна трактувати як похибку при зберіганні чи, можливо, зменшення всього зображення за допомогою сторонніх програм. Оскільки це може посилити контрастні контури, роблячи їх набагато яскравішими на виході. На зображеннях з масштабованою областю алгоритм ідентифікував її на 98% зразків.

Також було проведено експеримент не лише з масштабованими, а з масштабованими і одночасно переміщеними об’єктами на зображенні. Масштабування об’єкту відбувається за таким самим алгоритмом, а для його переміщення потрібно просто перетягнути об’єкт у графічному редакторі.

На рисунку 4 наведено оригінальне та фальсифіковане зображення. Фальсифікація була створена за допомогою масштабування та переміщення об’єкту.

Рис. 4. Оригінальне (ліворуч) та сфальсифіковане (праворуч) зображення

З рисунку 4 видно, що на фальсифікованому зображенні було зменшено чоловіка, який стоїть в лівій частині зображення, але його було ще й переміщено з лівої в праву частину зображення та розташовано перед військовою автівкою. Результат перевірки фото алгоритмом представлено на рисунку 5.

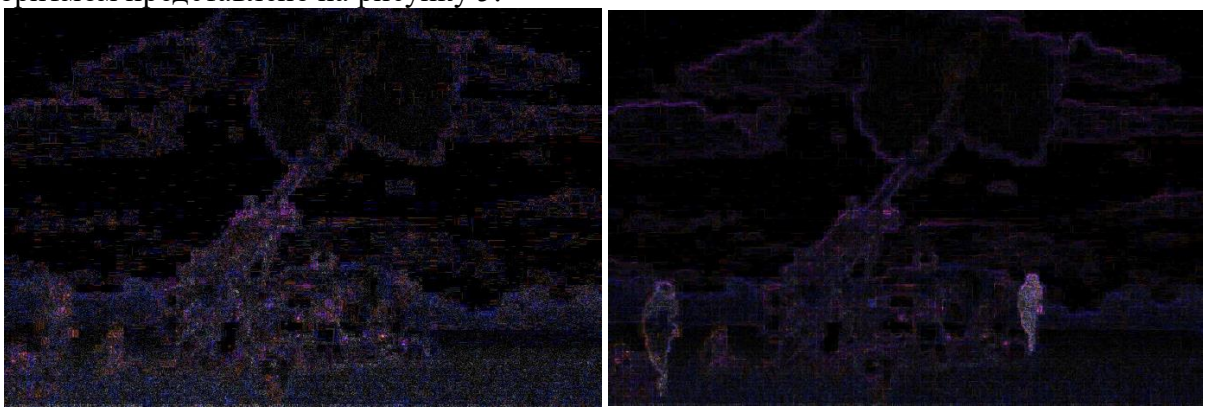

Рис. 5. Результат роботи алгоритму з фальсифікацією масштабування та переміщення

Як бачимо, оригінальне зображення містить однотонні контури зображення без видимих артефактів, що свідчить про те, що зображення є оригінальним. Зображення з правого боку має артефакти в зоні об’єкту, який було масштабовано та переміщено. Крім того, частина зображення, з якої було переміщено обєкт та в якій було виконано заливку, також виділена контуром. Результати даного експерименту показано в таблиці 2.

Таблиця 2

Результати роботи алгоритму при пошуку масштабовано-переміщеного об’єкту

Зображення	Помилки 1 роду	Помилки 2 роду
Тестові зображення	0%	0%

Після проведення другого експерименту може виникнути думка, що зазначеним методом також можна виявити клонування без масштабування. Третьою частиною експерименту стало виявлення клонування частин зображення. Клонування об’єкту відбувається за рахунок інструменту «Штамп», який дає змогу копіювати зміст з вихідної ділянки та використовувати його на інших ділянках зображення. Послідовність дій для клонування об’єкту за допомогою даного інструменту:

На рисунку 6 зображено оригінальне зображення та зображення з клонованою областю за допомогою інструменту «штамп».

Рис. 6. Оригінальне та фальсфіковане зображення

Тепер протестуємо алгоритм на цих зображеннях та перевіримо наявність артефактів, тим самим встановимо, чи фіксує алгоритм такі види фальсифікацій, як клонування. Роботу алгоритму з даними зображеннями буде представлено на рисунку 7.

Рис. 7. Результати роботи алгоритму на оригінальному (ліворуч) та фальсифікованому (праворуч) зображеннях

Розглядаючи отримані результати, можна зробити висновок, що алгоритм не може виявити клонування об’єктів, виконане за допомогою інструменту «штамп». В таблиці 3 наведено результати експерименту.

Таблиця 3

Результати роботи алгоритму пошуку клонованих областей зображення

Зображення	Помилки 1 роду	Помилки 2 роду
Тестові зображення	80%	7%

Результати експерименту вказують на те, що даний алгоритм не може виявити фальсифікацію клонування об’єктів.

Отож підсумок за даними результатами полягає в тому, що алгоритм аналізу рівня помилок дійсно може допомогти при аналізі зображень, які могли бути фальсифіковані методами масштабування та масштабування і переміщення об’єкту на зображенні. Саме тому було вирішено інтегрувати даний алгоритм в телеграм-бота.

Висновки

В даній роботі було проведено аналіз сучасного стану проблеми виявлення фальсифікації цифрового зображення. Серед сучасних методів виявлення основних способів підробити зображення було виділено методи виявлення клонування, ретушування та масштабування. Встановлено, що проблема виявлення масштабування має рішення, коли мова йде про збільшення частини зображення. В цей самий час зменшенню частин зображення у відкритому друці не приділяється уваги, а існуючі методи ефективні лише для виявлення збільшення.

Оскільки при зменшенні частини цифрового зображення відбувається зміна значень пікселів зони, що зменшується, та зони навколо неї, це призводить до виникнення артефактів масштабування, або до зростання рівня помилок. До виявлення слідів цих артефактів в роботі адаптовано метод, заснований на аналізі рівня помилок, який раніше застосовували для виявлення ретушування.

Даний метод показав спроможність виявляти фальсифіковані частини зображення, які було піддано зменшенню. Він також показав високу ефективність, коли зменшену частину було переміщено. Даний метод не ефективний у виявленні переміщення без зменшення, а також у виявленні збільшення частини зображення.

Ефективність методу з врахуванням обмежень його застосування: помили першого роду 2%, помилки другого роду 7%.

Список літератури

1. Експертиза фотографій: виявлення маніпуляцій з фотошопом за допомогою аналізу рівня помилок. URL: https://resources.infosecinstitute.com/topic/error-level-analysis-detect-image-manipulation/

2. Що таке фотофорензика? URL: https://fotoforensic.com/faq.php# What%20is %20 FotoForensics

3. Збройні сили України. Війна з окупантами. URL: https://t.me/zsuwar

DETECTION OF DIGITAL IMAGE PARTS REDUCED AFTER FORGERY

V.V.Gulich, V.V. Zorilo, O.Yu.Lebedeva

1, Shevchenko Ave., National Odessa Polytechnic University, 65044, Odesa, Ukraine
vikazorilo@gmail.com, whiteswanhelena@gmail.com

At a time when the use of digital content in all spheres of life is constantly growing, the ability to verify the authenticity of digital files, in particular digital images, is extremely important in protecting information from integrity violations. In the information war, photo fakes are always used to achieve certain, often criminal, goals. Both society as a whole and individuals must take care of information security and protect their information space from unverified information. Modern methods of detecting violations of the integrity of graphic information to some extent address some issues of information security, however, they are not universal and often require development, improvement, additional research and so on. Thus, existing methods for detecting such a common method of image falsification as scaling are effective only in cases where the falsified part is enlarged, however, when reducing part of the image, they are not effective. Moreover, in open printing the problem of detecting reduced scalable parts of the image is not covered. Therefore, the aim of this work is to increase the efficiency of scaling detection as digital image falsification by developing an algorithm for detecting scaling with a negative coefficient. In this paper, the method of error level analysis is adapted to detect reduced parts of the digital image. The efficiency of the adapted method in terms of errors of the 1st and 2nd kind was: errors of the 1st kind - 2%, 2nd kind - 7%. In addition, it has been found that this method is also effective in detecting simultaneously scalable (reduced) and moved parts of a digital image. This method detects artifacts (errors) in the digital image, which occur when reducing its part - the falsified area has a higher high-frequency component than the rest of the image, which is amplified under the influence of compression after saving the falsification in a lossy format.
Keywords: detection of falsifications, digital criminal science, scaling