DOI 10.15276/imms.v12.no1-2.40
УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 12 (2022), No. 1-2, pp. 40-45

ВИЯВЛЕННЯ ФАЛЬСИФІКАЦІЇ ЦИФРОВОГО ЗОБРАЖЕННЯ, ВИКОНАНОЇ МЕТОДОМ ADOBE PHOTOSHOP «ЛАТКА»

М.В. Гонтар, В.В.Зоріло, О.Ю.Лебедєва

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

Сьогодення все активніше змушує нас дбати про свою інформаційну безпеку. Події у світі і в Україні, інформаційні, гібридні війни, кібервійни – це те, що стало нашою повсякденною реальністю, і те, що спонукає шукати нові та вдосконалювати існуючі методи і засоби захисту інформації. Одне з питань захисту інформації – захист графічного контенту від порушень його цілісності. Порушення цілісності цифрових зображень можливо виконувати великим різноманіття інструментів графічних редакторів. Зокрема, такий інструмент графічного редактора Adobe Photoshop «латка» - зручний спосіб виконати фальсифікацію світлини, якому у відкритому друці на даний час не приділяється уваги. Тож необхідність виявлення даного інструменту стала підставою для описаних в даній статті експериментів. Мета даної роботи – підвищення ефективності виявлення підробок світлин, виконаних засобами інструменту Adobe Photoshop «Латка», шляхом розробки алгоритму. В роботі проведено обчислювальний експеримент з використанням 100 цифрових зображень, до яких було застосовано обробку інструментом «латка». На основі обчислювального інструменту було розроблено алгоритм, який показав себе як ефективний у випадках, коли зображення після фальсифікації збережено у форматах з втратами і без втрат. В більшості випадків вдалося виявити наявність порушення цілісності у випадку, коли вона дійсно мала місце, і встановити факт відсутності обробки інструментом «латка», коли його дійсно не було.
Ключові слова: порушення цілісності інформації, захист інформації, клонування, латка, алгоритм.

У сучасному світі світлини стали невід’ємною частиною кожної людини. Вже давно соціальні мережі, інтернет-магазини та інші цифрові методи взаємодії між людьми стали дуже розвиненими, і це супроводжується використанням великої кількості світлин. Вони зустрічаються нам на кожному кроці. Кожен день безліч користувачів передивляються фото друзів, рідних та близьких. Підтвердженням цьому стали соціальні мережі Instagram, Facebook та інші. Реальність така, що фотокамера є у кожної сучасної людини як мінімум у складі смартфону. Ми непомітно для себе фіксуємо різні моменти нашого життя. Це призводить до того, що у нашому розпорядженні опиняються тисячі фотографій.

Висока доступність програмних засобів редагування цифрових зображень – графічних редакторів, зокрема, Adobe Photoshop – призводить до того, що будь-який користувач може підробити тим чи іншим чином зображення, використати підробку з метою дезінформації задля отримання власної користі в тому числі. Наприклад, можна підробити номер автомобіля та на сайті авто-інтернет-магазину чи на інших ресурсах спробувати використати дані фото задля власної наживи. Операції, які для цього часто використовують, такі як «Штамп» графічного редактора Adobe Photoshop, на сьогоднішній день можливо виявити різними методами [1-7]. Однак сучасні версії цього графічного редактора дозволяють виконувати клонування з можливістю адаптації клонованої частини в контексті від оточуючої сцени. Для цього можна використати інструмент «Латка». Виявленню даного інструмента у відкритому друці не приділяється уваги.

Мета роботи – підвищення ефективності виявлення підробок світлин, виконаних засобами інструменту Adobe Photoshop «Латка», шляхом розробки алгоритму.

В наш час засоби смартфонів як правило виробляються та зберігаються фотографії в форматі JPEG, професійне обладнання дозволяє користувачам зберігати фотографії без втрат, наприклад, у форматі BMP, щоб цифрове зображення в результаті мало найкращу можливу якість.

Зараз існує багато програмного забезпечення, завдяки якому можна редагувати цифрові зображення, такі як Adobe Lightroom, Affinity Photo, PhotoLab тощо. Але найпопулярнішим із великого вибору програм є Adobe Photoshop, який надає можливість використовувати гнучкі налаштування, завдяки яким редагувати фото можна як вам заманеться.

Використання інструменту «Штамп» дуже просте, для цього потрібно на панелі інструментів обрати «Штамп» (рис.1), та затиснувши клавішу Alt клацнути лівою кнопкою миші по області, яку хочемо скопіювати (рис.2).

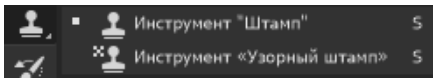

Рис. 1. Інструмент «Штамп»

Рис. 2. Вибір області для копіювання

Далі відпускаємо клавішу Alt і наводимо курсор на те місце, куди хочемо перенести (клонувати) об’єкт (рис. 3).

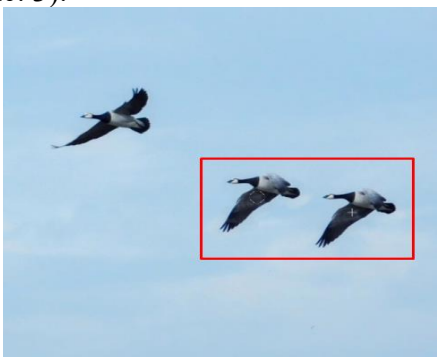

Рис. 3. Копіювання об’єкту

Завдяки цьому можна приховувати недоліки на зображені або робити більшу кількість об’єктів.

Далі ми розглянемо копіювання методом використання «Латки». Він знаходиться також на панелі інструментів (рис. 4).

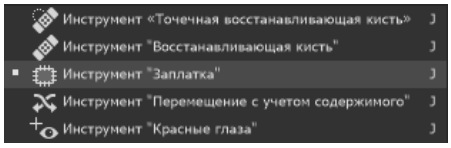

Рис. 4. Вибір інструмента «Латка»

Щоб скопіювати певну область, потрібно її виділити і натиснути клавішу M, після чого виділити область для копіювання (рис. 5) та перетягнути ЇЇ на потрібне місце (рис.6).

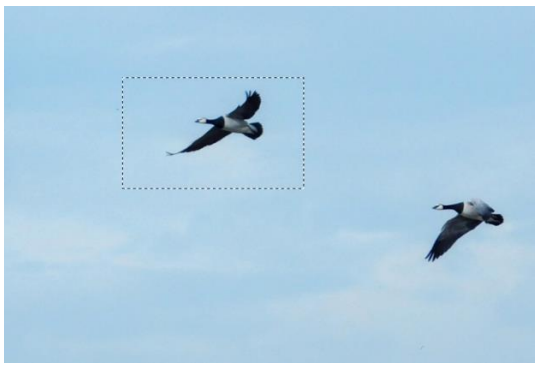

Рис. 5. Виділення об’єкту

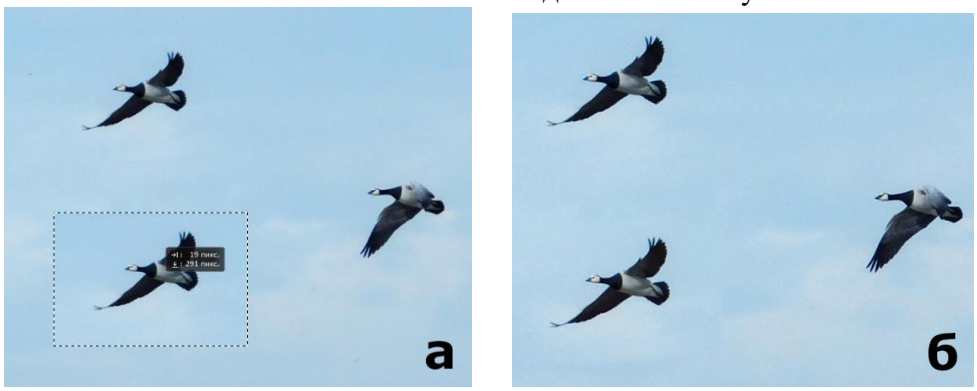

Рис. 6. Копіювання об’єкту інструментом «Латка»

Основна відмінність представлених способів копіювання у тому, що при використанні «штампу» об’єкт копіюється без змін. А при використані «Латки» перенесений об’єкт підлаштовує значення пікселів копійованої області для її органічного вбудовування в іншу частину зображення відповідно контексту.

На рисунку 7 представлений один і той же блок 3×3, але після використання методу «Латка» міняються кольори пікселів.

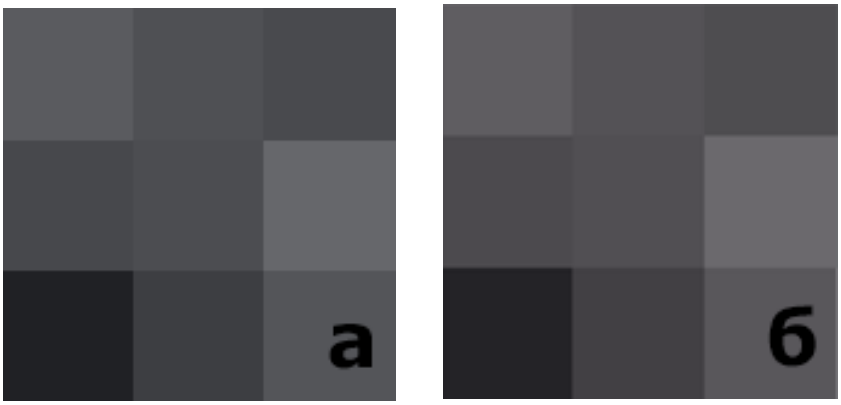

Рис. 7. Зміна кольорів копійованої області зображення після використання інструменту «Латка»

Цей ефект спостерігається по краях копійованої області і зменшується при просуванні до її центру. При достатніх розмірах області, що копіюється, в середині цієї області велика імовірність знайти однакові блоки. Зазвичай різні методи виявлення клонування й інших порушень цілісності використовують розбиття зображення на блоки 8×8, що можуть перетинатись чи не перетинатись. Крім того стандарт стиснення зображень JPEG також використовує розбиття на блоки такого розміру. Однак при виявленні «латки» розбиття на блоки 8×8 дало велику кількість помилок 1 роду. Виявлення фальсифікації було можливим лише при зберіганні без втрат та при розмірах фальсифікації, порівняних з половиною самого зображення. Тож було проведено експеримент з блоками різних розмірів, в ході якого встановлено, що оптимальним є використання блоків розміром 3×3.

Отже, основна задача алгоритму виявлення латки полягає у розбитті матриці зображення на блоки розміром 3×3, що перетинаються, та знайти серед них попарно однакові. Розглянемо роботу даного алгоритму на прикладі фальсифікації, виконаної над зображенням на рисунку 8 (оригінал). Фальсифіковано номер автомобіля інструментом «латка», а саме замість цифри 8 вставлено цифру 0 (рис.9).

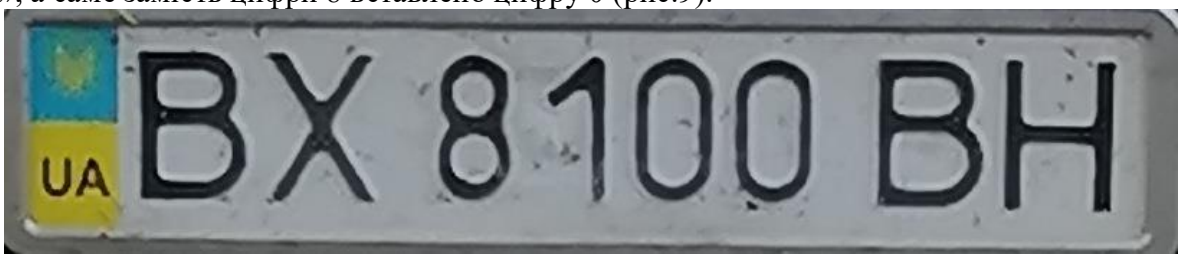

Рис. 8. Оригінальне зображення

Рис. 9. Приклад копіювання об’єкту

Результат було збережено у форматі з втратами jpg з високим ступенем якості та у форматі без втрат bmp. Результати роботи алгоритму для формату з втратами представлено на рисунку 10, для формату буз втрат – на рисунку 11.

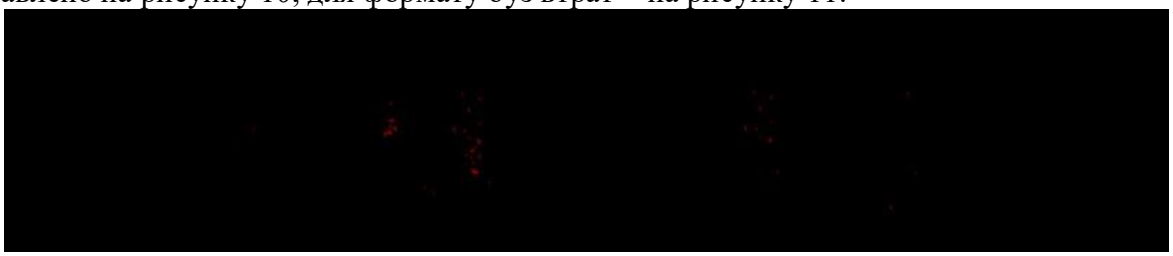

Рис. 10. Результат перевірки виявлення копіювання

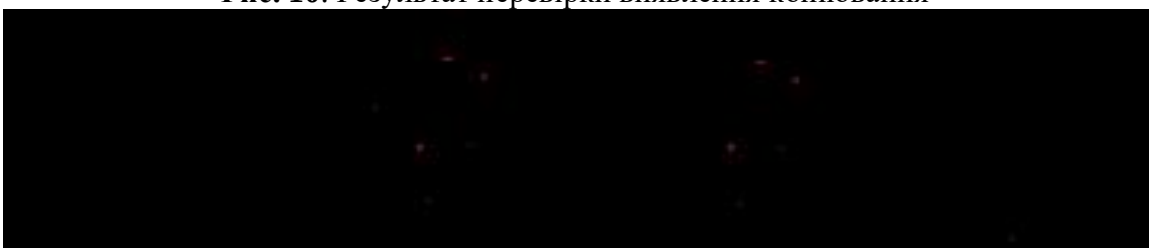

Рис. 11. Результат перевірки виявлення копіювання на зображенні без втрат

В обох випадках копійовані «латкою» області було виявлено: на місці, що відповідають образу і прообразу фальсифікації, знайдено ідентичні блоки (виділено червоним кольором). Однак, як і можна було очікувати, при збереженні з втратами виникають хибні тривоги (помилки 2 роду). Однак при виділенні сукупностей ідентичних блоків, які мають однакове розташування всередині сукупності відносно один одного, можна підвищити ефективність виявлення «латки» при збереженні у форматі з втратами. Тож на основі отриманих результатів алгоритм виявлення «латки» матиме додатковий етап у вигляді виділення зв’язних областей, виділені блоки в яких розміщені ідентично. Основні кроки алгоритму наступні.

Основні кроки алгоритму виявлення клонування, заснованого на аналізі сингулярних чисел блоків його матриці, представлені нижче. Нехай F – матриця зображення розмірів m×n.

1. Розбити матрицю F ЦЗ на 3×3-блоки $F_{ij}, i = 1,2\ldots,(n-2), j = 1,2\ldots,(m-2)$, що перетинаються так, аби кожний блок відрізнявся від сусіднього на один рядок (стовпець).

2. Побудувати матрицю S, елементи s_{ij} якої дорівнюють 1 (замалювати червоним), якщо блоки мають однакові значення пікселів, і 0 (замалювати чорним) – якщо різні ($i = 1,2\ldots,(n-2)$, $j = 1,2\ldots,(m-2)$).

3. Серед блоків, позначених цифрою 1, виділити зв'язні області з однаковим розташуванням виділених елементів, аби відрізнити фальсифіковані частини від хибних тривог.

Після цього ефективність алгоритму в термінах помилок першого та другого роду отримана такою, як її представлено в таблиці 1.

Таблиця 1

Результат експерименту

Формат	Помилки 1 роду	Помилки 2 роду
JPEG	6%	16%
BMP	4%	10%

Експеримент проведено із використанням 100 зображень. Таким чином можемо бачити, що розроблений алгоритм дійсно є ефективним як для зображень, збережених після фальсифікації у форматі з втратами, так і без втрат.

Висновки. Виявленню різних способів фальсифікації цифрових зображень у відкритому друці присвячено багато робіт, однак виявленню одного з можливих сучасних інструментів, - інструмент «латка» графічного редактора Adobe Photoshop, - навпаки, не приділяється уваги попри його популярність серед графічних маніпуляторів. Особливістю даного інструменту є подібність до інструменту «штамп» того ж редактора з відмінністю у підлаштуванні клонованої ділянки до частини фото, в якій вона опинилась. В даній роботі розроблено алгоритм виявлення даного порушення цілісності, який є ефективним як для зображень, збережених у форматі з втратами, так і для зображень без втрат.

Список літератури

1. Langille A. Gong M. An efficient match-based duplication detection algorithm. Canadian Conference on Computer and Robot Vision. 2006 P.64.

2. Luo W., Huang J. Qiu G. Robust detection of region duplication forgery in digital images. International Conference on Pattern Recognition. 2006. P.746–749.

3. Pan X, Lyu S. Region duplication detection using image feature matching

4. IEEE Transactions on Information Forensics and Security. 2010. Vol.5(4). P.857-867.

5. Wang J., Liu G., Li H., Dai Y., Wang Z. Detection of image region duplication forgery using model with circle block. International Conference on Multimedia Information Networking and Security. 2009. 25–29.

6. Shivakumar B.L.. Baboo S.S. Detection of Region Duplication Forgery in Digital Images Using SURF. IJCSI International Journal of Computer Science Issues. 2011. Vol.8. Issue 4. No1. P.199-205.

7. Зорило В.В. Методы повышения эффективности выявления нарушения целостности цифрового изображения. Інформаційна безпека. 2012. №1(7) . С.8.

8. Зоріло В.В. Метод підвищення ефективності виявлення порушення цілісності цифрового зображення: Дисертаційна робота кандидата технічних наук: 05.13.21. К., 2013. 127с.

DIGITAL IMAGE FALSIFICATION DONE BY METHOD OF ADOBE PHOTOSHOP PATCH

M.V.Gontar, V.V.Zorilo, O.Yu.Lebedeva

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

Today, more and more actively forces us to take care of our information security. Events in the world and in Ukraine, information, hybrid wars, cybercrimes are what have become our everyday reality, and what prompts us to look for new and improve existing methods and means of information protection. One of the issues of information protection is the protection of graphic content from violations of its integrity. Violation of the integrity of digital images can be done with a wide variety of graphic editor tools. In particular, such a tool of the Adobe Photoshop graphic editor "patch" is a convenient way to falsify a photo, which is currently not paid attention to in the open press. Therefore, the need to identify this tool became the basis for the experiments described in this article. The purpose of this work is to improve the effectiveness of detecting fake photos made using the Adobe Photoshop tool "Patch" by developing an algorithm. In the work, a computational experiment was carried out using 100 digital images, which were processed with the "patch" tool. Based on the computational tool, an algorithm was developed that proved to be effective in cases where the image after falsification is saved in lossy and lossless formats. In most cases, it was possible to detect the presence of a violation of integrity in the case when it really took place, and to establish the fact of the absence of processing with the "patch" tool, when it really was not.
Keywords: violation of information integrity, information protection, cloning, patch, algorithm.