УДК 004.932 doi: 10.15421/322014

М.Є. Сердюк, А.Г. Борисенко
Дніпровський національний університет імені Олеся Гончара

АНАЛІЗ ЦИФРОВИХ ЗОБРАЖЕНЬ НА НАЯВНІСТЬ ВНЕСЕНИХ ЗМІН

Розглянуто задачу виявлення змін цифрового зображення та методи її розв'язання на основі аналізу картини шумів, артефактів стиснення та пошуку дубльованих фрагментів. Запропонована модифікація методу знаходження повторюваних елементів на основі порівняння блоків пікселів. Представлена програмна система виявлення змін зображення різного характеру з комплексним використанням групи методів.

Ключові слова: цифрове зображення, аналіз зображень, фальсифікація зображень, виявлення втручань у зображення, криміналістика зображень.

M.E. Serdiuk, A.G. Borysenko
Oles Honchar Dnipro National University

DIGITAL IMAGES ANALYSIS FOR DETECTING MANIPULATION

The problem of digital image manipulation detection and methods of its solution are considered. Digital imaging is widely used in medicine, military affairs, security, control and supervision systems, and other fields where the integrity and authenticity of information often affect human safety, life, and health. Unauthorized changes to the images call into question their correctness and expediency of further use. Therefore, it is important to develop methods and systems for digital image analysis to identify changes.

The purpose of this research is to find effective approaches for analyzing an image to identify changes and implement them in the automated system that would answer the question about possible image adjustments in different cases of intervention.

The research analyzes different approaches to solving the problem of finding digital image manipulation. Each of these image analysis methods identifies changes in only a particular type. To detect areas with duplicate image fragments we propose a modification of the search method based on the comparison of pixel blocks. The comparison is based on the calculation of the correlation of the two blocks up to some threshold. The threshold is set depending on the noise level or other factors that may make an error. The block size for comparison is a parameter. Changing this parameter allows to control the search accuracy, to affect the number of computation and runtime of the algorithm. The practical result of this research is the software system for digital image analysis to detect manipulation. The system uses several approaches, which increases the probability of finding intervention in the image. The NLA method for detecting changes based on noise pattern analysis, the ELA method for analyzing digital image compression artifacts, and the proposed modification of the method for detecting duplicate areas in the image are implemented in the system. The data obtained from the EXIF-header of the selected image file is also checked. The experimental results have shown the effectiveness of integrated use of several approaches to image analysis with a sufficiently high level of different types of changes detection.

Keywords: digital image, image analysis, image falsification, detecting image manipulation, image forensics.

М.Е. Сердюк, А.Г. Борисенко
Днипровский национальный университет имени Олеся Гончара

АНАЛИЗ ЦИФРОВЫХ ИЗОБРАЖЕНИЙ НА НАЛИЧИЕ ВНЕСЕННЫХ ИЗМЕНЕНИЙ

Рассмотрена задача выявления изменений цифрового изображения и методы ее решения на основе анализа картины шумов, артефактов сжатия и поиска дублированных фрагментов. Предложена модификация метода обнаружения повторяющихся элементов на основе сравнения блоков пикселей. Представлена программная система выявления изменений изображения разного характера с комплексным использованием группы методов.

Ключевые слова: цифровое изображение, анализ изображений, фальсификация изображений, обнаружение вмешательств в изображение, криминалистика изображений.

Вступ. Стрімкий розвиток цифрових технологій обумовив широке розповсюдження та використання електронної інформації, зокрема цифрових зображень. Такі зображення можуть бути отримані за допомогою сучасних цифрових камер, смартфонів, планшетів та інших пристроїв, можуть легко і практично миттєво передаватися по мережам на будь-які відстані та зберігатися необмежений проміжок часу. Сукупність переваг цифрових зображень призвели до широкого їх застосування у багатьох галузях життєдіяльності людини. Проте, з іншого боку, наявність сучасних графічних редакторів дозволяє користувачеві виконувати широкий діапазон дій щодо редагування зображення. Це можуть бути невеликі модифікації, такі, як корегування кольору, обрізка зображення, а можуть бути й більш серйозні перетворення, наприклад, видалення або дублювання об’єктів. Останній вид редагування класифікується як підробка зображень. Отже, цифрові зображення можуть зазнавати несанкціонованих змін, що може поставити під сумнів їх коректність та доцільність подальшого використання. Впевненість у достовірності зображення та відсутності втручання у нього особливо важлива для таких областей життєдіяльності людини, як медицина, військова справа, судові розгляди, електронний документообіг, системи охорони, контролю та нагляду та т.п., де останнім часом широко використовується цифрова фото- та відеоінформація, а від її цілісності та справжності часто залежить безпека, життя та здоров’я людини. Це обумовлює важливість задачі аналізу цифрового растрового зображення з метою виявлення внесених в нього змін та робить актуальною розробку відповідних методів та систем.

Аналіз існуючих методів. На сьогодні існує багато різних способів внесення змін у цифрові зображення, починаючи з коригувань кольорів, яскравості, контрастності і закінчуючи вставкою або видаленням об’єктів. Оскільки природа таких змін різноманітна, то зрозуміло, що не існує єдиного універсального методу, який однозначно визначав би справжність зображення. На даний час розроблено багато алгоритмів, які спрямовані на виявлення конкретних видів втручань у зображення. Сформувався цілий напрям

комп'ютерного зору, направлений на пошук рішень цієї задачі, який називають Image Forensics, що трактується як «криміналістика зображень». У [6] визначені основні підходи, які використовуються для аналізу зображення з метою виявлення внесених змін. По-перше, багато невідповідностей, внесених шляхом цифрової обробки первісного зображення, можуть бути виявлені безпосереднім спостереженням. Часто уважний візуальний огляд зображення дозволяє виявити такі артефакти, як, наприклад, різні напрями освітлення об'єктів, невідповідності у кольорах, зокрема фонових, некоректний масштаб комбінованих частин зображення та ін. По-друге, нескладні доступні методи обробки можуть також виявити деякі невідповідності. Наприклад, висвітлення темних областей або затемнення яскравих ділянок може допомогти дослідити артефакти, склейки та інші місця, які були змінені недостатньо професійно, а зміна рівнів насиченості та яскравості різних кольорів надасть можливість помітити неприродні переливи та границі склейки. По-третє, у деяких випадках висновки про зміни у первісному зображенні можна зробити на основі аналізу EXIF-даних графічного файлу. Exchangeable Image File Format (EXIF) – стандарт, що дозволяє додавати до графічних та інших медіафайлів додаткову інформацію (метадані), а саме інформацію про джерело та час походження зображення, його опис, координати місця зйомки або іншу інформацію. Зокрема EXIF-дані містять інформацію про програму, у якій було відредаговано фото. Отже, якщо така інформація виявлена, то це свідчить про наявність втручання у зображення.

Зазначені підходи не потребують застосування складних алгоритмів, але вони не працюють на великих масивах даних, а результати аналізу часто залежать від досвіду та знань дослідника. Ще одна група підходів для виявлення маніпуляцій з зображенням, визначена в [6], це методи розширеного аналізу зображення, які є більш складними в реалізації, але дозволяють ідентифікувати специфічні маніпуляції із зображенням.

У роботах [2, 3, 6] розглядається метод Error Level Analysis (ELA) та його модифікації. Метод заснований на аналізі артефактів стиснення у цифрових зображеннях, збережених у форматах, які використовують стиснення з втратами, наприклад, у найпопулярнішому форматі JPEG. Алгоритм JPEG працює з блоками пікселів 8x8, які стискаються незалежно один від одного [7]. Для немодифікованого зображення усі блоки повинні мати однаковий рівень помилок (шум, артефакти стиснення). При повторному стисненні кожен блок має погіршуватися приблизно з однаковою швидкістю через внесення приблизно однакової кількості помилок. Якщо ж зображення містить вставлені або змінені фрагменти, то різні блоки будуть мати різні артефакти стиснення. Різниця може виникати внаслідок того, що різні деталі неодноразово піддавалися одній і тій самій операції стиснення різну кількість разів або різні деталі піддавалися різним алгоритмам або параметрам стиснення. Отже, ця різниця може свідчити про те, що дані були відредаговані. У [2] метод додатково удосконалений з використанням вертикальних та горизонтальних гістограм зображення для визначення точних місць модифікації.

Інший підхід для виявлення втручання у зображення – Noise Level Analysis (NLA), він базується на аналізі картини шумів та пошуку змін в ній. Реальні фото містять як природні шуми, так і шуми, що з'являються в результаті роботи алгоритмів стиснення зображень або спричинені пристроями їх отримання. Різні зображення частіше за все мають різні ступені зашумленості, а графічні редактори шуми не створюють. Отже, якщо частина одного зображення вставляється в інше, то аналіз шумових характеристик частин останнього зображення надасть можливість робити висновки про можливе втручання у нього. У роботі [5] представлено аналіз шуму цифрових зображень, досліджені його характеристики та їх зміни в процесі отримання та обробки зображення, що надає можливість виявити локальні невідповідності на зображенні в процесі його аналізу, а також визначені деякі методи аналізу з метою перевірки справжності зображення, які не працюють, якщо зображення спотворене штучним шумом. У роботі [1] розглядається спосіб виявлення глобального додавання шуму до цифрового зображення. Для виявлення ознак маніпуляцій з додаванням шуму використовуються спеціальні постійні і смугові блоки, формулюється та аналізується вплив шуму на поблоковий розподіл значень пікселів.

Ще один підхід для перевірки справжності зображення – Luminance Gradient Analysis. Він спирається на природу розповсюдження світла та виявлення невідповідностей освітлення об'єктів на зображенні. У роботі [4] представлено метод оцінки напрямків світла від точкового джерела. Аналіз розташування векторів освітлення дозволяє зробити висновки про коректність зображення. Різноспрямованість таких векторів буде свідчити про можливі втручання у зображення.

Один з способів внесення змін у зображення – клонування ділянок вихідного зображення з метою створення дублікату або приховування деяких існуючих об'єктів. У [8] для виявлення підробки копіювання-переміщення зображення розділяють на квадратні блоки, а компоненти DCT (дискретного косинусного перетворення) приймають як представлення блоків. Співставлення ознак дозволяє виявити клоновані ділянки. У [11] ідентифікація клонованих ділянок здійснюється на основі порівняння сингулярних чисел блоків матриці зображення.

У роботі [9] представлені також такі методи аналізу зображень, як пошук відомих сигнатур, що залишаються програмами при обробці фотографій, пошук та аналіз оригіналів та мініатюр зображення, аналіз матриць квантування зображення на предмет відповідності заявленому коефіцієнту компресії, побудування гістограм коефіцієнтів дискретного косинусного перетворення для виявлення повторного збереження зображення.

Отже, існує багато різних методів дослідження зображення з метою виявлення втручань, але немає єдиного універсального методу, який дозволив би зробити висновок про справжність зображення у будь-якому випадку можливих змін.

Метою даної роботи є пошук ефективних шляхів аналізу зображення для виявлення внесених змін та реалізація їх у автоматизованій системі, яка б давала відповідь на питання про можливі корегування зображення у різних за характером випадках втручань.

Постановка задачі. Нехай є зображення, яке представлено матрицею I розміром $M \times N$ за кількістю пікселів. Елементами матриці є значення яскравості зображення у пікселі – $I(i, j)$, де $i=1..M$, $j=1..N$. Припускаємо, що зображення містить області A_k, які вставлені з інших зображень або є результатом дублювання фрагментів вихідного зображення. Задача полягає в тому, щоб визначити області A_k, наявність яких свідчить про те, що у вихідне зображення були втручання.

Метод розв'язання задачі. На основі аналізу описаних в літературі методів для визначення можливих областей втручання були обрані підходи NLA, ELA та запропоновано простий алгоритм пошуку дубльованих частин зображення.

Для аналізу шумів зображення (NLA) будемо використовувати метод, який базується на ідеях, викладених у роботі [5]. За допомогою цього методу можна виявити роботу таких інструментів графічного редактору, як пензель, штамп, розмиття, вставка фрагментів. На першому етапі методу до вихідного зображення застосовується один зі згладжуючих фільтрів та отримується оброблене зображення $\tilde{I}$. В даній роботі використовується медіанний фільтр фіксованого розміру 3x3 [10], який застосовується для кожного колірного каналу пікселя, що розглядається. Для кожного пікселя (i, j) зображення розраховується медіана його околу розміром 3x3 – п'яте значення за величиною з дев'яти значень околу. Нове значення пікселю в обробленому зображенні буде дорівнювати знайденій медіані:

$$\tilde{I}(i, j) = \text{med}\{I_k \mid k = 1, 2, ..., 9\}$$

На другому етапі методу розраховується різниця двох зображень – вихідного I та згладженого $\tilde{I}$. В результаті отримується карта шумів:

$$N = I - \tilde{I}.$$

Зауважимо, що застосування медіанного фільтру до кожного з колірних каналів R, G, B часто призводить до спотворення кольорів зображення. Але для виявлення шумів такий підхід є прийнятним. Далі необхідно проаналізувати карту шумів та виявити ділянки, які є темнішими або яскравішими, ніж решта областей зображення. Наявність чорних ділянок свідчить про відсутність в них шумів, а це означає, що були втручання за допомогою графічних редакторів. Наявність ділянок з рівнем шуму, який відрізняється від середнього за зображенням, може свідчити про вставлений з іншого зображення фрагмент. Але треба зазначити, що даний метод буде недієвим, якщо до зображення після втручання було штучно додано шумів або зображення декілька разів було оброблено алгоритмом JPEG. Тому доцільно буде перевірити зображення й іншими способами.

Для виявлення вставок та накладань тексту будемо використовувати метод ELA [6], який здійснює пошук артефактів, що виникають під час стиснення з втратами. Якщо зображення, яке зберігається у форматі з використанням стиснення з втратами (наприклад, JPEG), містить вставлені фрагменти, то скоріше за все різні частини зображення будуть мати різні рівні артефактів стиснення. Ця різниця може виникати внаслідок того, що різні деталі неодноразово піддавалися одній і тій же операції стиснення різну кількість разів або різні деталі піддавалися різним алгоритмам або параметрам стиснення. Для того, щоб зробити артефакти стиснення більш помітними, дані, що аналізуються, піддаються додатковому витку стиснення з відомим та рівномірним застосуванням алгоритму стиснення до всього зображення, і результат віднімається від первісного зображення. Якщо на результуючому зображенні є область з білим кольором, і ця область на первісному зображенні не виділяється різкою зміною кольору, можна стверджувати про внесення змін у зображення в конкретному місці. В той же час частини результуючого зображення, колір яких наближається до чорного, мають малу ймовірність втручання, адже додаткова ітерація застосування алгоритму стиснення не сильно змінила їх значення. В даній роботі результуюче зображення, яке є графічним представленням ELA, генерується таким чином:

$$\hat{I}(i,j)=\frac{1}{3}\sum_{k=1}^{3}[I(i,j,k)-I_q(i,j,k)]^2,$$

де k=1, 2, 3 відповідає значенням кольорів для каналів моделі RGB, $I(i, j, k)$ – значення кольору у пікселі (i, j) k-го колірного каналу у вихідному зображенні, I_q – результат стиснення вихідного зображення з коефіцієнтом q=90.

Додатково, цифрові графічні формати містять метадані, що описують конкретне стиснення, яке було використане. Якщо у даних спостерігаються артефакти стиснення, які відрізняються від очікуваних для даного опису метаданих, то метадані можуть не описувати фактично стислі дані і, таким чином, вказують на те, що дані були відредаговані.

Під час зміни фотографії шляхом накладення іншого зображення або його фрагменту ймовірність того, що знайдені зображення будуть з однаковим рівнем артефактів, дуже мала. Якщо підібрати кольорову гаму, вдало змінити геометрію вставки, зробити плавні переходи між вставкою та оригінальним зображенням, то таке перетворення не буде помітним для людського ока, але алгоритм ELA покаже різницю в кількості артефактів між оригіналом зображення та вставленою в нього частиною. Таким чином, даний алгоритм не втрачає своєї точності навіть після застосування до зображення алгоритмів стиснення даних. Але велика кількість повторів процедури збереження файлу може зробити неефективним використання даного алгоритму. Через особливості роботи алгоритмів стиснення первісне зображення та вставлені фрагменти можуть призвести свої артефакти до одних значень за рахунок того, що під час кожного збереження відбуваються різноманітні перетворення зображення, серед яких є пошук середнього значення між сусідніми пікселями.

Одним із способів обробки зображення є використання клонування елементів самого зображення. Більшість графічних редакторів надають спеціальні інструменти для реалізації цієї дії, яка полягає у піксельному переносі інформації з однієї області зображення в іншу. Такі дії надають зображенню природний перехід кольорів, збіжність шумів та інші переваги, що приховують внесені зміни. За таких умов більшість алгоритмів виявлення змін у зображенні будуть недієвими. В такому випадку необхідно застосувати методи пошуку схожих частин на одному зображенні. В даній роботі для пошуку дубльованих елементів безпосередньо на зображенні пропонується алгоритм, в основу якого лягло правило порівняння кожного з кожним [11].

Зображення, яке необхідно дослідити, розбивається на блоки фіксованого розміру $a \times a$. Величина a є параметром, який можна змінювати у залежності від певних умов перевірки. Кожний наступний блок отримується рухом по матриці на один стовпець вправо, тобто блок відрізняється від попереднього на один стовпець. Рух продовжується до $(N-a+1)$-го стовпця – до кінця рядка матриці. Далі здійснюється зсув на один рядок вниз, виділення блоків продовжується до $(M-a+1)$-го рядка. Отже, для зображення розміром $M \times N$ отримуємо $(M-a+1)\times(N-a+1)$ блоків розміром $a \times a$, які необхідно порівняти між собою. Якщо рядки блоку записати послідовно у один рядок, то кожен блок можна розглядати як елемент простору R^p p-вимірних векторів, де $p=a \times a$. Відстань між елементами такого простору визначається евклідовою метрикою. Отже квадрат відстані між l-тим блоком ($l = 1, 2, \ldots, (M-a+1)\times(N-a+1)$) та блоком-зразком, з яким відбувається порівняння на черговому кроці алгоритму, можна обчислити за формулою

$$d_l^2 = \sum_{i=1}^{a}\sum_{j=1}^{a}[x(i,j,l) - t(i,j)]^2, \qquad (1)$$

де $x(i, j, l)$ – значення яскравості у пікселі (i, j) блоку l, $t(i, j)$ – значення яскравості у пікселі (i, j) блоку-зразку. Будемо вважати, що схожість між блоком-зразком та деяким блоком зображення має місце, якщо величина d_l^2 близька до нуля. Перепишемо формулу (1) у вигляді

$$d_l^2 = \sum_{i=1}^{a}\sum_{j=1}^{a}x^2(i,j,l) - 2\sum_{i=1}^{a}\sum_{j=1}^{a}x(i,j,l)\cdot t(i,j) + \sum_{i=1}^{a}\sum_{j=1}^{a}t^2(i,j). \qquad (2)$$

Перший доданок у формулі (2) характеризує енергію l-того блоку. Це значення змінюється досить повільно при переході від блоку до блоку та мало характеризує шуканий об’єкт. Третій доданок характеризує енергію блоку-зразку і не залежить від l. Для виявлення схожості суттєвим є другий доданок, який з точністю до постійного множника задає взаємну кореляцію двох блоків зображення. Отже, для виявлення схожості блоків будемо використовувати другий доданок у нормованому вигляді:

$$D_l = \frac{\sum_{i=1}^{a}\sum_{j=1}^{a} x(i,j,l)\cdot t(i,j)}{\sqrt{\sum_{i=1}^{a}\sum_{j=1}^{a} x^2(i,j,l)}\cdot\sqrt{\sum_{i=1}^{a}\sum_{j=1}^{a} t^2(i,j)}}.$$

У випадку співпадіння l-го блоку зі зразком величина D_l буде дорівнювати одиниці. Отже, будемо вважати, що знайдена відповідність блоку l та блоку-зразку, якщо

$$|D_l - 1| < L_\varepsilon,$$

де L_ε – деякий поріг, який можна встановлювати в залежності від рівня шумів або інших факторів, що можуть внести похибку. Порогове значення необхідне для того, щоб не виключати з розгляду скопійовані елементи зображення, які піддалися впливу різноманітних згладжуючих інструментів графічних редакторів. Для кольорових RGB-зображень величина D_l обчислюється за кожним каналом, середнє значення використовується для порівняння з порогом. Якщо співпадіння блоків встановлено (із заданою точністю), то ці блоки маркуються певним чином. Для цього створюється додаткове зображення, в якому однакові частини вихідного зображення маркуються однаковим кольором. Наприкінці роботи алгоритму на додатковому зображенні кольорами будуть виділені схожі ділянки. Далі марковані зони можуть бути досліджені більш детально.

Треба відзначити, що на результат роботи наведеного алгоритму впливає вибір параметру a, яким визначається розмір блоків для перевірки. Якщо цей розмір обрати занадто великим, ймовірність ідентифікації дублювань на зображенні буде малою, проте пошук буде відбуватися швидко. З іншого боку, надмірне зменшення параметру a призведе до зростання кількості обчислень, необхідних для коректного аналізу зображення, та помилкових співпадінь. Таким чином, необхідно шукати баланс між точністю пошуку, об’ємом обчислень та часом виконання аналізу зображення.

Програмна реалізація системи аналізу зображення. Кожен з розглянутих вище методів аналізу зображення з метою пошуку внесених змін не може бути використаним у якості точного інструменту, проте їх комбінація та спільне використання дадуть змогу давати більш точні результати під час аналізу зображення з метою виявлення втручання у зображення. Тому був розроблений програмний додаток, у якому реалізовані методи NLA, ELA та запропонований варіант пошуку клонованих частин зображення. Для розробки додатку використано мову програмування Python, а також бібліотеки Pillow, OpenCV. Для реалізації користувацького інтерфейсу використано бібліотеку графічного інтерфейсу користувача Tkinter.

Програмний додаток для проведення аналізу зображення з метою виявлення внесених змін складається з єдиного вікна, в якому користувач обирає файл зображення та спостерігає за аналізом та демонстрацією його результатів. Обране зображення відображається у відповідному полі вікна. Поряд відображаються дані, отримані з EXIF-заголовку файлу обраного зображення.

Якщо в EXIF-даних є згадування про відомий графічний редактор, поле виводу тексту буде червоного кольору. Якщо ж заголовки будуть містити стандартну інформацію про зображення, а саме: марка та модель пристрою, що створив зображення, розмір піксельної сітки, розмір пікселя, дата проведення зйомки або ж параметри алгоритму стиснення, застосовуваного до зображення, – колір поля для тексту буде зеленим. Запуск процесу аналізу здійснюється відповідною кнопкою у вікні. Далі до зображення по черзі застосовуються визначені алгоритми. Кожний алгоритм формує результуюче зображення і відображає його мініатюру у вікні інтерфейсу програми. Отже, в результаті буде сформовано 3 файли, кожен з яких є результатом обробки зображення конкретним алгоритмом. До результуючих файлів додатково застосовуються методи обробки (операції висвітлення та збільшення контрастності) з метою полегшення подальшої інтерпретації результатів. У результуючому зображенні третього методу кольором будуть виділені ті ділянки, де знайдено співпадіння груп пікселів. Отримані результати підлягають інтерпретації.

Аналіз результатів. Розроблена система була протестована на низці зображень, які попередньо були змінені за допомогою графічного редактору Adobe Photoshop з використанням широкого набору інструментів: від засобів малювання до засобів геометричних перетворень частини зображення. Оброблені зображення зберігались з різним рівнем стиснення та форматом. Тестування показало, що система достатньо ефективно виявляє різні варіанти втручань у зображення. Наведемо деякі приклади.

На рис. 1а представлено вихідне зображення, на рис.1б – зображення, видозмінене шляхом повтору частин всередині самого зображення. Змінені частини на рисунках позначені рамками.

а) **б)**

Рис. 1. Тестове зображення: а) вихідне, б) змінене графічним редактором

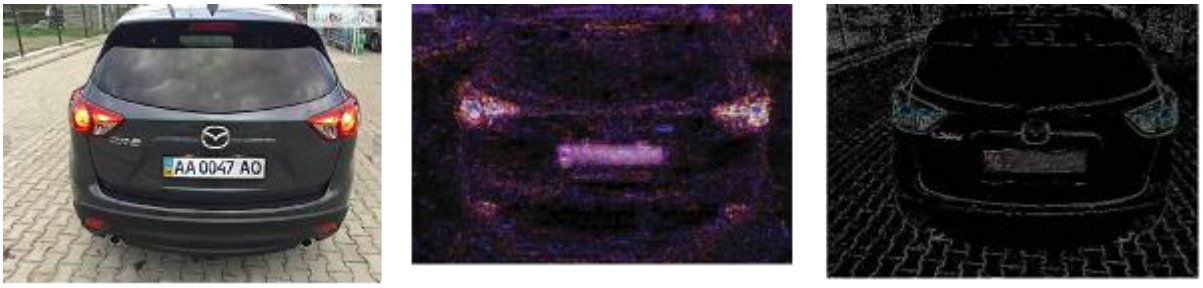
Дублювання було виконано інструментом «штамп» у графічному редакторі Adobe Photoshop. Один із дубльованих фрагментів можна помітити на номері, інші фрагменти візуально не визначаються. Результати аналізу зміненого зображення програмним додатком представлені на рис.2.

а) б) в)

Рис. 2. Результати роботи алгоритмів аналізу зображення: а) алгоритм ELA, б) алгоритм NLA, в) алгоритм пошуку дубльованих частин

Дослідження результату роботи алгоритму ELA дозволяє зробити висновок про відсутність внесених змін у зображення. Такий результат зумовлено тим, що під час втручання у зображення використовувались його власні елементи, що не призвело до виникнення артефактів стискання. Саме на виявлення цих артефактів направлений алгоритм ELA. Аналіз результату роботи алгоритму NLA також не надає інформації про можливе втручання у зображення. Це очікувано, оскільки дублювання частини зображення в ньому самому не призведе до появи шумів, які відрізнялися б від решти шуму на зображенні. Насамкінець, як видно з рис. 2в, на зображенні було знайдено області пікселів, які були скопійовані з одного місця в інше. Проте не всі скопійовані області були знайдені. Так, не ідентифікована зміна номера автомобіля. Це пояснюється тим, що перевірка зображення на наявність повторюваних фрагментів проводилась з параметром a=30, який у даному випадку виявився недостатнім для виявлення подібних змін. Додаткова перевірка з параметром a=12 дозволила ідентифікувати і цю зміну.

У другому тестовому прикладі у вихідне зображення був вставлений фрагмент з іншого зображення – повністю змінений номер автомобіля (рис. 3а).



а) б) в)

Рис. 3. Тестовий приклад: а) вихідне зображення зі зміненим номером автомобіля, б) результат роботи алгоритму ELA, в) результат роботи алгоритму NLA

Як бачимо на рис.3 б, в, місце вставки фрагменту у вихідне зображення добре ідентифікується алгоритмами ELA та NLA. Проте третім методом втручання такого типу виявлено не було, оскільки фрагмент для вставки був взятий з іншого зображення.

Відзначимо, що в обох тестових прикладах EXIF-дані були показані на червоному фоні, тобто наявність корегування фото за допомогою графічного редактору була визначена системою до початку аналізу.

Отже, дослідження різних тестових прикладів підтвердило працездатність та ефективність розробленої системи, а також доцільність застосування групи методів для аналізу зображення з метою виявлення втручань різного походження.

Висновки. У роботі проаналізовані різні підходи до розв'язання задачі пошуку змін цифрового зображення. Оскільки окремі методи ідентифікують зміни зображення лише певного характеру, то доцільним є використання одразу декількох підходів комплексно для аналізу зображення, що дозволяє збільшити ймовірність знаходження втручань у зображення. Для детектування ділянок з дубльованими фрагментами зображення запропонована модифікація методу пошуку на основі порівняння блоків пікселів. Практичним результатом роботи є програмна система для аналізу цифрових зображень з метою виявлення втручань. У системі реалізовано метод NLA для виявлення змін на основі аналізу картини шумів, метод ELA для аналізу артефактів стиснення цифрових зображень та запропонована модифікація методу виявлення дубльованих ділянок на зображенні. Тестування системи показало ефективність комплексного використання декількох підходів для аналізу зображення з достатньо високим рівнем виявлення внесених змін різного характеру.

Бібліографічні посилання

1. **Cao, G.** Forensic detection of noise addition in digital images [Text] / G. Cao, Y. Zhao, R. Ni, B. Ou, Y. Wanga. Journal of Electronic Imaging. Vol. 23(2), 2014. [Electronic resource] – Access mode: https://www.researchgate.net/publication/262951015_Forensic_detection_of_noise_addition_in_digital_images
2. **Gunawan, T.S.** Development of photo forensics algorithm by detecting photoshop manipulation using error level analysis [Text] / T.S. Gunawan, S.A. Hanafiah, M. Kartiwi, N. Ismail, N.F. Za'bah, A.N. Nordin. Indonesian Journal of Electrical Engineering and Computer Science Vol. 7, No. 1, July 2017, pp. 131-137.
3. **Hilal, A.** Development of the Error Level Analysis Forensic Tool for Images Shared Over Messaging and Social Networking Applications [Text] / A. Hilal, S. A. Chakra. International Journal of Electrical, Electronics and Data Communication (IJEEDC). Vol. 6, Issue-10, 2018, pp. 42-46.
4. **Johnson, M.** Exposing digital forgeries by detecting inconsistencies in lighting [Text] / M. Johnson, H. Farid // Proc ACM Multimedia and Security Workshop.New York. – 2005.
5. **Julliand, T.** Image Noise and Digital Image Forensics [Text] / T. Julliand, V. Nozick, H. Talbot. IWDW 2015, Oct 2015, Tokyo, Japan. pp.3-17.
6. **Krawets, N.** A Picture's Worth: Digital Image Analysis and Forensics [Text]. Hacker Factor Solution, 2007. [Electronic resource] – Access mode: https://www.hackerfactor.com.
7. **Luo, W.** JPEG Error Analysis and Its Applications to Digital Image Forensics [Text]/ W. Luo, J. Huang, and G. Qiu. IEEE Transactions on Information Forensics and Security. Vol. 5, no. 3, 2010, pp. 480-491.
8. **Mahmood, T.** Copy-Move Forgery Detection Technique for Forensic Analysis in Digital Images [Text] / T. Mahmood, T. Nawaz, A. Irtaza, R. Ashraf, M. Shah, M.T. Mahmood. Math-

ematical Problems in Engineering. Volume 2016. [Electronic resource] – Access mode: http://dx.doi.org/10.1155/2016/8713202

9. **Гераськин, А.Н.** Анализ методов проверки фотоизображений на наличие внесённых изменений [Текст] / А.Н. Гераськин, С.Ю. Желтов. Информационная безопасность регионов, Саратов. № 4(25), 2016, с.5-10.
10. **Гонсалес, Р.** Цифровая обработка изображений [Текст] : пер. с англ. // Р.Гонсалес, Р. Вудс. – М. : Техносфера, 2005. – 1072 с.
11. **Зорило, В.В.** Выявление клонирования как фальсификации цифрового изображения [Текст] / В.В. Зорило // Вісник Національного технічного університету «ХПІ». Збірник наукових праць. Тематичний випуск «Системний аналіз, управління та інформаційні технології». – 2011. – № 35. – С.31-38.

Надійшла до редколегії 11.09.2020.