МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Разработка системы анализа фотоизображений на наличие внесённых изменений

АВТОРЕФЕРАТ
дипломной работы

студентки 6 курса 631 группы
специальности 10.05.01 Компьютерная безопасность
факультета компьютерных наук и информационных технологий
Кващук Марии Егоровны

Научный руководитель
доцент, к.п.н _____ А. С. Гераськин
23.01.2021 г.

Заведующий кафедрой
д. ф.-м. н., доцент _____ М. Б. Абросимов
23.01.2021 г.

Саратов 2021

ВВЕДЕНИЕ

Подделка фотографий появилась задолго до цифровых камер, компьютеров и специализированного программного обеспечения. Первый в мире фотомонтаж был сделан Оскаром Рейландером в 1855 году. Известному фотографу никак не удавалось сделать групповой портрет – одна из фигур оставалась размытой. Тогда Оскар Рейландер совместил при печати три разный негатива, тем самым сделав первый фотомонтаж[1].

В настоящее же время с ростом технологий и различного программного обеспечения для редактирования изображений фотомонтаж стал доступен для всех. Вследствие этого особо остро встала проблема контроля подлинности изображения.

Фотоизображения имеют большое влияние на сознание общества. Используя фото- и видеоизображения СМИ распространяет новости, государство доносит необходимые установки до населения и влияет на общественный настрой. Немаловажно в настоящее время уметь контролировать корректность и подлинность изображений.

Кроме этого в настоящее время фотоизображения используются как способ аутентификации. Многие сервисы используют фотографии как способ подтверждения личности. Чаще всего это используется в различных государственных приложениях, где необходимо предоставить документ, подтверждающий личность. Также подобные способы аутентификации могут использоваться в сервисах как электронной, так и физической почты, отправки и доставки грузов, некоторых социальных сетях. Фотоизображения используются как прямые доказательства в таких ситуациях, как ДТП или оформлении страховых полисов. С ростом технологий область использования видео- и фотоизображений будет только расти.

В связи с этим остро встает вопрос установления оригинальности фотоизображения. Особый интерес представляют универсальные методы,

[1]Rejlander, O. G. An Apology for Art-Photography / O. G. Rejlander. - Albuquerque : University of New Mexico Press, 1988. - 141 с.

позволяющие дать заключение о подлинности цифрового изображения, при этом способные распознать модификации, внесенные различными инструментами, и устойчивые к многократным пересохранениям изображения, нанесением на изображение фильтров, добавляющих, например, шум или увеличивающие размытость изображения.

Целью данной дипломной работы является реализация системы методов, на основе результатов которой можно сделать вывод о наличии внесённых изменений в фотоизображения. Также были выбраны основные задачи, выполнение которых необходимо для достижения цели работы:

– рассмотреть методы проверки фотоизображений;

– исследовать и проанализировать методы проверки фотоизображений;

– реализовать набор методов, позволяющий проанализировать фотоизображения на наличие изменений и протестировать на практике его эффективность.

Дипломная работа состоит из введения, 2 разделов, заключения, списка используемых источников и 3 приложений. Общий объём работы – 77 страниц, из них 51 страница – основное содержание, включая 40 рисунков и список используемых источников из 20 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

Первая глава данной работы посвящена рассмотрению методов, основанных на анализе самого изображения, а именно: наблюдение, поиск похожих изображений, проверка подлинности с помощью цветокоррекции. Любой анализ фотоизображения на наличие изменений следует начать с простого наблюдения. При внимательном осмотре изображения можно выявить потенциально отредактированный области. Еще одним способом проверки изображения на наличие изменений является поиск похожих изображений. Оригинал измененного фотоизображения можно попытаться найти с помощью различных сервисов. Следующий метод основан на использовании инструментов для цветокоррекции, которые можно найти в любом графическом редакторе. Изменение тех или иных параметров поможет лучше рассмотреть детали и выявить места, где фотография была деформирована. Методы, основанные на анализе самого изображения, не требуют специального программного обеспечения, просты в применении и могут работать с любым форматом изображения, но при этом способны распознать далеко не все виды модификаций фотоизображений, а следовательно, обладают наименьшей эффективностью.

Далее в этой главе рассматриваются методы основанные на анализе структуры изображения: анализ метаданных изображения, эффект двойного квантования, error level analysis, principal component analysis, noise level analysis и wavelet analysis.

Все файлы содержат в себе ряд дополнительной информации – метаданные, хранящиеся внутри файлов. По метаданным можно узнать место и время создания фотографии, геолокацию, было ли изображение отредактировано и каким образом[5].

[5]Метаданные в цифровой фотографии [Электронный ресурс] // Интернет-издание iXBT.com [Электронный ресурс] : [сайт]. - URL: http://www.ixbt.com/digimage/metadxph.shtml (дата обращения: 23.09.2020). - Загл. с экрана. - Яз. рус.

Метод, основанный на эффекте двойного квантования, применяется для анализа изображений в формате JPEG с потерями, основанный на принципе работы его алгоритма сжатия.

Error level analysis – это метод установления факта модификации изображения, посредством идентификации фрагментов изображения с разным уровнем сжатия. При каждом сохранении фотоизображения в JPEG, будет потерян определенный объем информации, не подлежащий восстановлению. Эта потеря информации носит название уровня ошибки. Чем больше раз изображение было сохранено в JPEG, тем выше для него уровень ошибки. Для составления картины ELA необходимо сохранить исследуемое изображения со стандартным коэффициентом сжатия 90%. А затем для каждого блока изображения 8x8 пикселей найти разницу между исходным значением и значением в пересохраненной версии. В соответствии с полученными значениями разницы составляется картина ELA[9].

Principal component analysis – метод анализа фотоизображений на наличие внесенных изменений, базирующийся на методе главных компонент. Вычисление главных компонент может быть сведено к вычислению собственных векторов и собственных значений ковариационной матрицы исходных данных.

$$C = \begin{pmatrix} cov(X,X) & cov(X,Y) & cov(X,Z) \\ cov(Y,X) & cov(Y,Y) & cov(Y,Z) \\ cov(Z,X) & cov(Z,Y) & cov(Z,Z) \end{pmatrix}, \quad (1)$$

где $cov(X,Y) = cov(Y,X)$ – ковариация между признаками X и Y, $cov(X,Z) = cov(Z,X)$ – ковариация между признаками X и Z, $cov(Y,Z) = cov(Z,Y)$ – ковариация между признаками Y и Z, $cov(X,X), cov(Y,Y), cov(Z,Z)$ – дисперсии множеств X, Y, Z соответственно. Дисперсия находится по следующей формуле:

$$cov(X,X) = \frac{\sum_{i=1}^{n}(x_i - \bar{X})^2}{(n-1)}, \quad (2)$$

где $\bar{X}$ – математическое ожидание и оно в свою очередь вычисляется по формуле:

[9]Farid, H. Digital image forensics / H. Farid. - London : Springer Nature, 2008. - 189 с.

$$\bar{X} = \frac{\sum_{i=1}^{n} x_i}{n}. \quad (3)$$

Аналогично дисперсия вычисляется для двух других признаков. Формула для нахождения ковариация между двумя величинами крайне похожа на формулу дисперсии:

$$cov(X, Y) = \frac{\sum_{i=1}^{n}(x_i - \bar{X})(y_i - \bar{Y})}{(n-1)}. \quad (4)$$

Построив ковариационную матрицу необходимо найти ее собственные значения и собственные вектора, их количество равно размеру матрицы, то есть будет получено три собственных вектора, которые и являются тремя главными компонентами[11]. Далее метод главных компонент осуществляет переход к новой системе координат в исходном пространстве признаков, которая является системой ортонормированных линейных комбинаций – главными компонентами.

Noise level analysis – эффективный метод установления факта модификации изображения. При модификации изображения зачастую остаются следы в его шумовой картине. Однако увидеть шумы и их изменения невооруженным глазом невозможно, и для составления шумовой картины изображения используется метод NLA[12]. Он использует медианный фильтр шумоподавления и инвертирует его результаты, то есть в результате работы алгоритма метод оставляет шум и удаляет остальную часть изображения. Измененные области можно будет легко заметить по их картине шумов: они будут темнее или ярче общей картины[15]. Алгоритм медианного фильтра для обработки изображения:

1) поместить значения пикселей обрабатываемого блока 3×3 в массив P и пронумеровать их от 0 до 8;

[11]Smith, L. I. A tutorial on Principal Components Analysis / L. I. Smith. - Dunedin : University of Otago Library, 2002. - 27 с.

[12]Мороз, Г. Метод главных компонент [Электронный ресурс] / Г. Мороз, О. Ляшевская, И. Щуров // НИУ ВШЭ [Электронный ресурс] : MathINFO. - URL: http://math-info.hse.ru/f/2015-16/ling-mag-quant/lecture-pca (дата обращения: 04.10.2020). - Загл. с экрана. - Яз. рус.

[15]Noise Analysis for Image Forensics [Электронный ресурс] // Image forensics creative journal [Электронный ресурс] : [сайт]. - URL: https://29a.ch/2015/08/21/noise-analysis-for-image-forensics (дата обращения: 30.11.2020). - Загл. с экрана. - Яз. англ.

2) вычислить значения медиан:

$$M_1 = median(P[0], P[4], P[8]), \quad (9)$$

$$M_2 = median(P[1], P[4], P[7]), \quad (10)$$

$$M_3 = median(P[2], P[4], P[6]), \quad (11)$$

$$M_4 = median(P[3], P[4], P[5]); \quad (12)$$

3) вычислить значения медиан:

$$M_a = median(P[4], M_1, M_3), \quad (13)$$

$$M_b = median(P[4], M_2, M_4); \quad (14)$$

4) если $P[4] \neq median(P[4],\ M_a, M_b)$, то присвоить $P[4] = median(P[4],\ M_a, M_b)$, иначе оставить без изменений[16].

Так как в методе NLA, наоборот, требуется получить шумовую картину, то есть инвертировать результат его работы, последний пункт нужно заменить на следующий:

4) если $P[4] \neq median(P[4],\ M_a, M_b)$, то добавить $P[4]$ к изображению на выходе.

Таким образом основная идея этого метода заключается в получении шумовой картины изображения и дальнейшем ее анализе на неоднородность.

Wavelet analysis – метод, основанный на применении разделимого двумерного вейвлет-преобразования к изображению. Для исследования изображений на наличие внесенных изменений применяется двумерное вейвлет-преобразование Хаара, базисные векторы ψ и φ которого задаются следующим образом:

$$\psi = \left[-\frac{1}{\sqrt{2}}; \frac{1}{\sqrt{2}}\right], \quad (18)$$

$$\varphi = \left[\frac{1}{\sqrt{2}}; \frac{1}{\sqrt{2}}\right]. \quad (19)$$

На их основе можно записать матрицу преобразования A:

$$A = \begin{pmatrix}\varphi\\ \psi\end{pmatrix} = \frac{1}{\sqrt{2}} \cdot \begin{pmatrix}1 & 1\\ -1 & 1\end{pmatrix}. \quad (20)$$

[16]Buades, A. A review of image denoising algorithms, with a new one / A. Buades, B. Coll, J.M. Morel // A SIAM Interdisciplinary Journal. - SIAM : Multiscale Modeling and Simulation, 2005. - № 4. - С. 490-530

Для каждой пары пикселей $(x,\ y)$ получим следующее преобразование:

$$A \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \frac{y+x}{\sqrt{2}} \\ \frac{y-x}{\sqrt{2}} \end{pmatrix}. \quad (21)$$

В результате получается картина изображения, состоящая из четырех подкартин, по которой можно провести анализ на наличие факта модификации[18].

Таким образом, рассмотрев методы, описанные выше, можно заключить, что методы, основанные на анализе изображения обладают наименьшей эффективностью: они наименее автоматизированы и не имеют четкого алгоритма. Методы, основанные на анализе метаданных изображения, просты в использовании, но не могут установить, что именно было изменено в фотоизображении и не всегда могут быть применимы вследствие того, что метаданные могут отсутствовать. Методы, основанные на эффекте двойного квантования, имеют большое количество ложных срабатываний, поэтому также не обладают высоким уровнем эффективности. Метод error level analysis также успешно устанавливает факт модификации фотоизображения, однако неустойчив к пересохранению изображения. Метод principal component analysis обладает высоким уровнем эффективности, однако не устойчив к размытию изображению. Метод noise level analysis успешно справляется с выявлением модификаций, сделанных с помощью различных инструментов, однако не устойчив к наложению фильтров, зашумляющих изображение, и к пересохранению изображения. Метод анализа изображения с помощью вейвлет-преобразования устойчив к пересохранению изображения и эффективно справляется с выделением различных модификаций.

Вторая глава посвящена разработанному программного комплексу, с помощью которого можно провести анализ фотоизображений на наличие внесенных изменений. В данной главе будет приведено описание выбранной системы анализа, тестовой базы изображений, а также будет описан интерфейс

[18]Walker, J. S. A Primer on Wavelets and Their Scientific Applications / J. S. Walker. - 2-е изд. - Washington, D.C. : Chapman and Hall/CRC, 2008. - 318 с.

разработанного программного продукта и его функции. В систему анализа фотоизображений на факт модификации были включены следующие методы: error level analysis, principal component analysis, noise level analysis и wavelet analysis. Выбран в пользу этих методов был сделан, опираясь на проведенный анализ: методы, основанные на анализе структуры изображения, более эффективны и универсальны, обладают широкой применимостью.

Программный комплекс был реализован в виде web-сервиса, написанного на языке программирования JavaScript и библиотек для отображения пользовательского интерфейса.

Для тестирования разработанного продукта была создана база изображений, состоящая из изображений, отредактированных совокупностью инструментов (100 шт.), изображений, отредактированных с помощью одного инструмента (60 шт.) и подлинных изображений (40 шт.).

Была протестирована вся база изображений. При анализе результатов работы системы методов внимание уделялось неоднородным фрагментам картин, резким переходам, цветовым пятнам. По результатам тестирования можно сделать следующий вывод об эффективности разработанной системы анализа изображений при работе с различными инструментами редактирования. Из-за разницы в алгоритмах строения картин каждый метод имеет свои преимущества и недостатки, результаты представлен на рисунке 40.

	ELA	PCA	NLA	WA
Чувствителен к инструменту **кисть**	+	+	+	+
Чувствителен к инструменту **вставка**	+	+	+	+
Чувствителен к инструменту **штамп**	-	+	-	+
Чувствителен к инструменту **размытие**	+	-	+	+
Устойчив к фильтрам **цветокоррекции**	+	-	+	-
Устойчив к фильтрам **зашумления**	+	+	-	-
Устойчив к **пересохранению**	-	+	-	+

Рисунок 40 – Эффективность методов при работе с различными инструментами редактирования изображений

При анализе картин с помощью разработанного программного продукта изображение стоит считать модифицированным, если хотя бы результаты двух методов свидетельствуют об этом. При этом условие о наличии двух методов, по которым можно сделать вывод о наличии факта изменения изображения, уменьшает вероятность ложного срабатывания системы. Таким образом, разработанная система анализов, состоящая из четырех методов, является устойчивой и универсальной, способной определить любую модификацию или совокупность примененных к изображению модификаций.

ЗАКЛЮЧЕНИЕ

В данной дипломной работе были рассмотрены методы проверки изображения на наличие внесенных изменений. Были изучены методы, основанные на анализе самого изображения, а именно наблюдение, поиск похожих изображений и проверка подлинности с помощью цветокоррекции, а также методы, основанные на анализе структуры файла изображения: анализ метаданных изображении, эффект двойного квантования, error level analysis, principal component analysis, noise level analysis и wavelet analysis.

Были реализованы методы ELA, строящий картины изображений по уровню ошибки, PCA, основанный на принципе главных компонент, NLA, строящий картину шумов изображений, и WA, основанный на вейвлет-преобразованиях. Было проведено сравнение этих методов, их эффективности при работе с различными инструментами модификации и устойчивости к многократному пересохранению изображений, применению фильтров, добавляющих, например, шум или увеличивающие размытость изображения.

В результате работы был написан программный комплекс, реализующий в себе методы ELA, PCA, NLA и WA, с помощью которого можно наглядно получить картины методов, провести анализ исследуемых изображений и установить факт наличия внесенных изменений.