УДК 004.02 **Информационные технологии**

Бельды Анастасия Викторовна, *магистрант*
БГТУ «ВОЕНМЕХ» им Д.Ф. Устинова, г. Санкт-Петербург

КАТЕГОРИЗАЦИЯ МЕТОДОВ ОПРЕДЕЛЕНИЯ ПОДЛИННОСТИ ЭЛЕКТРОННЫХ ИЗОБРАЖЕНИЙ, ОБЗОР ИСПОЛЬЗУЕМЫХ В НИХ МАТЕМАТИЧЕСКИХ МЕТОДОВ И ВАРИАНТ ИХ ПРИМЕНЕНИЯ

Аннотация: В статье будут рассмотрены актуальность и способы подделки электронных изображений (среди которых ретушь, склейка, клонирование), техники и используемые методы проверки изображения на подлинность среди (среди которых цифровая подпись, цифровые водяные знаки), а также один из возможных вариантов их применения для создания ПО, в котором входные данные подаются на вход модуля поиска и локализации фальсификации, изображения нормализуются, после чего к ним применяются описанные ранее алгоритмы для выявления наличия одного или нескольких типов подделки и их локализации на данных изображениях. В зависимости от типа подделки и используемого алгоритма, выходные данные могут представлять собой входные изображения с добавленными на них границами области подделки, вероятностью присутствия того или иного типа подделки, либо булево или вещественное значение вероятности присутствия подделки на соответствующих изображениях.

Ключевые слова: электронные изображения, проверка подлинности, подделка изображений, цифровая подпись, водяные знаки.

Annotation: The paper will consider the relevance and techniques of electronic image counterfeiting (including retouching, gluing, cloning), techniques and used methods of image verification (including digital signature, digital watermarks) and one of their possible applications to create software in which input data are fed to the input

of a search and localization module, images are normalized and then algorithms are applied to them to detect the presence of one or more counterfeit types and Depending on the type of forgery and the algorithm used, the output data may be input images with the boundaries of the forgery area added to them, the probability of the presence of a particular forgery type, or a Boolean or real value of the probability of the presence of forgery in the corresponding images.

Keywords: electronic images, authentication, image forgery, digital signature, watermarks.

На сегодняшний день проблема выявления неоригинального (претерпевшего различные неавторизованные изменения) цифрового контента является чрезвычайно актуальной. Существует и развивается большое множество программных продуктов для редактирования растровых изображений. Наиболее известные – Adobe Photoshop и открытый GIMP. В сети интернет легко найти огромное количество обучающих материалов по ретуши, склейке и другим манипуляциям над изображением. Практически любой пользователь-неспециалист сможет сфальсифицировать фотографию или, например, цифровую копию документа. Поэтому фальсификация изображений может использоваться не только в политических или иных конкурентных целях, но и для «бытовой» подделки документов. На сегодняшний день проблема фальсификации цифровых изображений очень актуальна. С начала XX века проведены сотни исследований в области выявления фальсификации изображения [0; 2].

«Цена» такой подделки, ее последствия могут быть различными. Такие материалы могут привести к непоправимым последствиям при их использовании в качестве вещественных доказательств в судебных разбирательствах, в медицине, в ходе различных манипуляций общественным сознанием, мнением, в ходе политической борьбы и т.д. В силу этого сейчас, как никогда ранее, остро встает вопрос эффективной экспертизы подлинности того или иного цифрового контента, в частности изображений-копий документов, разработки методов

выявления и локализации нарушений их целостности [3].

Способы подделки изображений [4]:

1. Ретушь – в узком смысле, устранение ненужных деталей изображения, шумов, изменение композиции.

2. Склейка – способ создания изображений из нескольких изображений или их фрагментов.

3. Клонирование – способ изменения изображения путем копирования части (прообраза) данного изображения и перемещения его в другую подобласть данного изображения с его дальнейшей постобработкой или без нее.

Техники аутентификации (проверки подлинности) изображений [5]:

1. Активные.

1.1. Цифровые подписи.

1.2. Цифровые водяные знаки.

2. Пассивные.

2.1. Зависимые от типа подделки.

2.1.1. Обнаружение клонирования.

2.1.2. Обнаружение склейки.

2.2. Независимые от типа подделки.

2.2.1. Обнаружение ретуши.

2.2.2. Условия освещения.

В техниках активной аутентификации для собственно аутентификации изображения необходима предварительно встроенная определенная информация. Данная информация встраивается в изображение во время его генерации в скрытом или открытом виде. Таким образом, методы активной аутентификации подразделяются на два типа: цифровые водяные знаки и цифровые подписи.

Цифровые водяные знаки встраиваются в изображение в открытом виде на этапах создания или обработки изображения. Информация водяного знака содержится непосредственно в матрице изображения и соответственно будет видна пользователю при просмотре данного изображения [6; 7].

Цифровые подписи помещаются в специальный служебный (второстепенный) блок файла изображения согласно его формату. Данная информация не видна пользователю при просмотре изображения [8; 9].

Главным недостатком данных подходов является необходимость предварительной подготовки изображения (вставки водяного знака или цифровой подписи). Таким образом, изображения, предоставленные третьими лицами, невозможно аутентифицировать с помощью описанных методов.

Пассивная аутентификация – это процесс аутентификации изображений, не требующий предварительно добавленной в данное изображение информации. Пассивные методы основаны на предположении о том, что хотя вмешательство при фальсификации может не оставить никаких видимых визуальных следов, оно может изменить основные статистические данные. Именно статистические несоответствия и аномалии лежат в основе пассивных методов обнаружения фальсификации. Большое количество исследований пассивных методов было проведено для криминалистики как российскими, так и зарубежными исследователями. Пассивные методы в свою очередь классифицируются как методы, зависящие от типа подделки, и методы, не зависящие от типа подделки [10; 11].

Методы обнаружения подделки, зависящие от типа подделки, очевидно, могут использоваться для обнаружения только определенных типов подделок, таких как клонирование и склейка.

Методы, не зависящие от типа подделки, основаны на поиске следов (т.н. артефактов) ресамплинга (передискретизации) изображения и несоответствия освещения частей изображения. Артефакты ресамплинга появляются в результате изменения разрешения изображения, то есть интерполяции или децимации. Таким образом, при обнаружении следов ресамплинга можно однозначно утверждать, что изображение подвергалось обработке. Несоответствие освещения появляется в результате склейки двух или более изображений. Например, если вставить на фотографию, сделанную при пасмурной погоде, какой-либо предмет или человека, которые были сняты под

солнечными лучами, невооруженным глазом будет заметно несоответствие жесткости теней, цветовой температуры, баланса белого цвета и т.п.

ПО для поиска и локализации подделки может быть размещено централизованно на общедоступном сервере и использоваться различными организациями в своих целях. От задач конкретной организации будут зависеть сценарии взаимодействия и интерфейсы.

В настоящее время организация эффективного поиска, обработки и анализа подделки одно из приоритетных направлений развития информационных систем. Рассмотрим модель разрабатываемой информационной системы (рис.1). В состав информационной системы введем модуль поиска и локализации фальсификации.

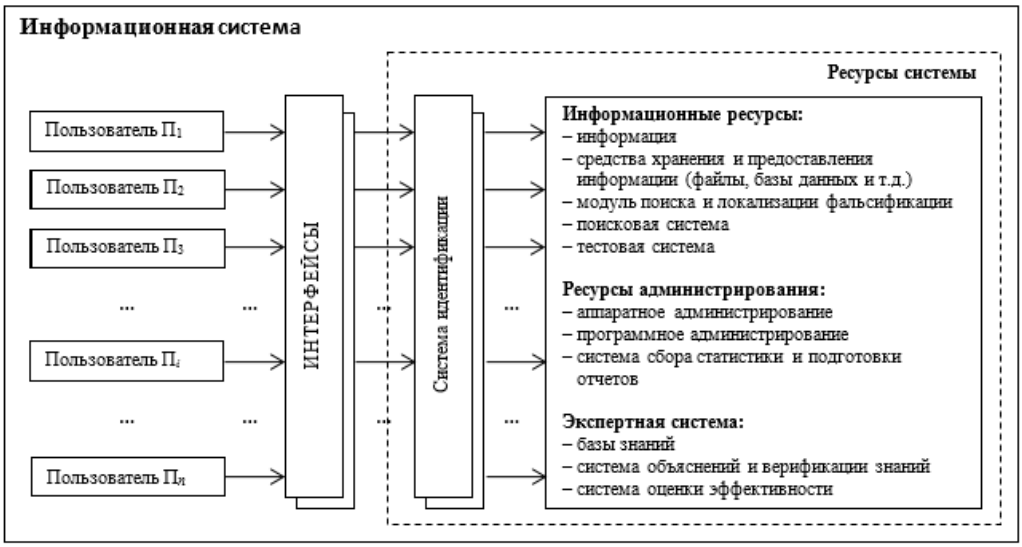

Рис 1. – Модель разрабатываемой информационной системы

На рис. 2 приведена модель модуля поиска и локализации фальсификации (рис.2), которая условна разделена на 3 части: входные данные, выходные данные, блок проверки.

Пользователь предоставляет входные данные – изображение или набор изображений в одном из популярных форматов изображений (например, jpg, png, bmp).

Входные данные подаются на вход модуля поиска и локализации

фальсификации. Изображения нормализуются, после чего к ним применяются описанные ранее алгоритмы для выявления наличия одного или нескольких типов подделки и их локализации на данных изображениях. После выполнения алгоритмов, результат приводится к понятному для человека виду.

В зависимости от типа подделки и используемого алгоритма, выходные данные могут представлять собой входные изображения с добавленными на них границами области подделки, вероятностью присутствия того или иного типа подделки, либо булево или вещественное значение вероятности присутствия подделки на соответствующих изображениях.

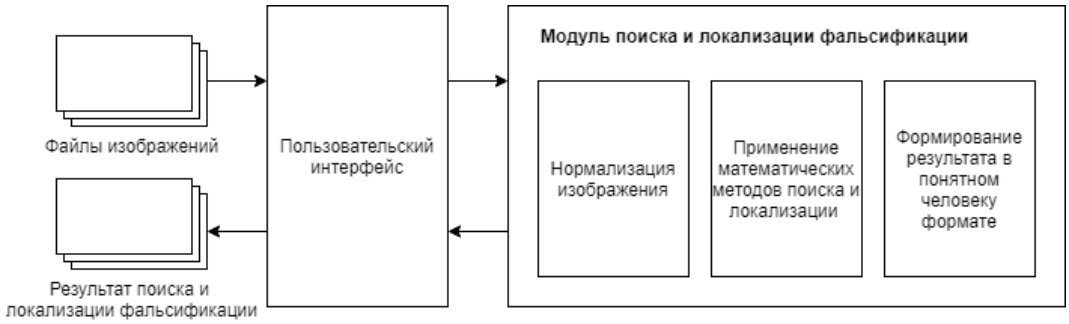

Рис 2. – Модель модуля поиска и локализации фальсификации.

Библиографический список:

1. Farid, H. Image Forgery Detection – IEEE Signal processing magazine – 2009. — 16-25.

2. Haouzia, A. Methods for image authentication: a survey / A. Haouzia, R. Noumeir. Multimedia Tools and Applications. — 2008. — c. 1-46.

3. Redi, J. A. Digital image forensics: A booklet for beginners / J.A. Redi, W. Taktak, J.L. Dugelay // Multimedia Tools and Applications. — 2011. — 133–162

4. M. N. O. Sadiku, Sarhan M. Musa , and S. R. Nelatury. DIGITAL FORGERY [Электронный ресурс]. – URL: https://www.researchgate.net/publication/327022702_DIGITAL_FORGERY (дата обращения 10.10.2022).

5. Saba Mushtaq, Ajaz Hussain Mir. Digital Image Forgeries and Passive Image Authentication Techniques: A Survey. – International Journal of Advanced

Science and Technology. – 2014. – с. 15-32.

6. C.-Y. Lin and S.-F. Chang. Generating Robust Digital Signature for Image/Video Authentication. – Multimedia and Security Workshop at ACM Multimedia ’98, Bristol, U.K.

7. C.-S. Lu and H.-Y. Mark Liao. Structural Digital Signature for Image Authentication: An Incidental Distortion Resistant Scheme. – IEEE transactions on multimedia. – 2003.

8. J.-M. Shieh, D.-C. Lou and T. Ming-Chang Chang. A semi-blind digital watermarking scheme based on singular value decomposition. – Computer Standards & Interfaces. – 2006. – 428–440.

9. R. Chamlawi, A. Khan and I. Usman. Authentication and Recovery of images using multiple watermarks. – Computers and Electrical Engineering. – 2010. – 578–584.

10. T.-T. Ng, S.-F. Chang, C.-Y. Lin and Q. Sun. Passive-blind image forensics. – Multimedia security technologies for digital rights. USA: Elsevier. – 2006.

11. П.В. Зотов. Использование компьютерных технологий для выявления подделок текста в электронных документах. – Вестник Саратовской государственной юридической академии. – №2 (84). – 2012. – 208-212.