МАРКИРОВКА РАСТРОВЫХ ИЗОБРАЖЕНИЙ ДЛЯ ЗАЩИТЫ ОТ ФАЛЬСИФИКАЦИИ

Белобокова Ю. А., Колистратов М. В.
Кафедра общегуманитарных и етественнонаучных дисциплин,
Московский региональный социально-экономический институт,
Кафедра Инфокоммуникационных технологий,
Национальный исследовательский технологический университет МИСИС
Видное, Москва, Российская Федерация
E-mail: yulya.belobokova@mail.ru, kolistratov.mv@misis.ru

Предлагается методика цифровой маркировки изображений с применением технологии водных знаков (ЦВЗ) для выявления фальсификаций. Используются две метки: bitmap-логотипы для подтверждения авторства и электронные подписи для фиксации изменений. Метки внедряются в красный и синий каналы RGB-изображений, обеспечивая защиту от манипуляций. Подбор оптимальных параметров гарантирует надежность и незаметность меток. Эффективность методики доказана экспериментально и реализована в программном продукте на языке C#.

Введение

Благодаря развитию инструментов обработки изображений, публикуемые в электронных СМИ, а также социальных сетях цифровые фотографии становятся уязвимыми для возможных подделок. При этом в некоторых случаях изменение даже небольшого фрагмента может полностью изменить смысл исходного фото. Поэтому разработка методов противодействия фальсификации цифровых изображений является достаточно актуальной задачей.

I. Методы защиты цифровых изображений

Технология цифровых водяных знаков (ЦВЗ) востребована в качестве защиты цифрового контента еще с середины девяностых годов прошлого века. ЦВЗ представляет собой скрытую метку, внедряемую в изображение с помощью некоторого алгоритма в соответствии с определенным ключом. Встраиваемые метки оценивают по трем критериям, причем первые два противоречат друг другу. Это незаметность (отсутствие сильных искажений в изображении), устойчивость (робастность, стойкость к возможным искажающим воздействиям) и емкость (количество информации, содержащейся в ЦВЗ).

Цифровые фотографии, предназначенные для использования в сети интернет, чаще всего сохраняют в форматах JPEG и PNG, поскольку эти форматы поддерживаются практически всеми графическими редакторами. Изображения, сохраненные в формате JPEG, из-за режима сжатия с потерями проигрывают аналогичным PNG-изображениям в качестве, но при этом обладают меньшими размерами. При высокой степени сжатия у JPEG-изображения необратимо теряется часть графической информации, что может привести к потере маркировки (у PNG-изображений такая проблема не возникает). Но такое сжатие при небольших размерах исходной JPEG-фотографии может существенно «испортить картинку», поэтому его использование станет менее вероятным.

При фальсификации исходные цифровые изображения с большей вероятностью могут подвергаться кадрированию, добавлению или удалению каких-либо элементов. Менее вероятны смена формата или цветовой модели, масштабирование, добавление фильтров цвета, применение таких инструментов, как резкость, автоуровни, автоконтраст, зашумление.

Логично, что ЦВЗ, указывающие на авторство изображения, должны быть максимально устойчивыми к этим воздействиям. Если же поставлена задача определения фальсифицированных фрагментов, внедряемые метки должны указывать на факт фальсификации. Выполнение обоих задач требует внесения ЦВЗ с разной степенью робастности, поэтому была разработана специальная методика [1,2] на основе метода Коха и Жао [3], позволяющая различать оригинальные и сфальсифицированные фрагменты изображения благодаря внедрению двух типов невидимых меток. Первый тип – это собственно ЦВЗ (симметричные bitmap-логотипы), показывающие авторство изображения и подлинность его составных частей, второй – электронные сигнатуры, (хэш-коды, строки бит, вычисляемые на основе размеров изображения или его фрагментов), которые могут свидетельствовать о факте внесения изменений, например, кадрировании, ретуши или добавлении инородных фрагментов [1]. Значения электронных сигнатур зависят от свойств маркируемой фотографии, а ЦВЗ постоянен для всех её фрагментов. профиля на сайте конференции.

II. Методика маркировки распознавания

Разработанная методика включает в себя алгоритмы множественной защитной маркировки и проверки растровых изображений на аутентичность и целостность и применяется к изображениям, сохраненным в формате RGB, поскольку из-за

особенностей человеческого зрения встраивание маркировочных меток идёт только в красный и синий каналы.

Обработанное в форме битовой карты изображение представляется в виде матрицы и разбивается на блоки 64x64 пикселя (некратные блоки остаются снизу и/или справа изображения), после чего каждый из блоков разделяется на 3 матрицы (по числу цветовых каналов). Далее в полные b-матрицы (синий канал) встраивается ЭП и половина бит монохромного логотипа, а в полные r-матрицы (красный) – вторая половина бит логотипа. Неполные блоки размером менее 18x18 пикселей не маркируются, в остальные неполные блоки встраиваются только биты ЦВЗ. Способ встраивания подробно описан в [1]. Очень важен правильный выбор значения параметра, называемого коэффициентом силы встраивания: чем он выше, тем больше не только робастность маркировки, но и ее заметность. Серия экспериментов показала, что для маркировки низко- и среднечастотных областей фотографий рационально использовать коэффициент силы встраивания со значением 5..7, а для Высокочастотных областей – значения 7..20.

При проверке подлинности цифрового изображения из него извлекаются внедренные ЦВЗ и электронные сигнатуры. При этом изображение также представляется в виде матрицы, разбиваемой на блоки 64x64, и маркировка извлекается из красного и синего каналов. Если в верхнем левом блоке обнаружены биты ЦВЗ, предполагается, что найден базовый блок и проверяются остальные блоки. В противном случае генерируется сдвиг, изображение переразбивается, и в новых блоках также ищется ЦВЗ. По характеру расположения бит ЦВЗ в блоках синего канала ищутся значения электронных сигнатур. При проверке блоков возможны три исхода: блок аутентичен (либо применяемые к изображению воздействия не исказили его содержание); блок содержит ЦВЗ, но значение сигнатуры указывает на наличие искажающих воздействий; блок не содержит маркировки, что говорит о сильных разрушающих воздействиях или его фальсификации.

Для повышения защиты изображений целесообразно использовать базу данных, в которой хранятся не только сами промаркированные изображения, но и такая информация, как дата маркировки, геометрические размеры, образец встраиваемого монохромного логотипа и т.д. Разработанная методика была реализована в виде программного комплекса на языке программирования C#. Серия экспериментов подтвердила эффективность разработанной методики и ее практическую применимость

III. Результаты

Для проверки устойчивости метода была сформирована база файлов с растровыми изображениями с различающимися типами объектов, изображенных на них (природа, здания и сооружения, люди, предметы обихода). Программным способом в изображения по разработанной авторами методике в синий и красный каналы были встроены маркировочные знаки двух видов (рис. 1). Каждое изображение неоднократно маркировалось с использованием различных значений коэффициента силы встраивания, после чего в результате сравнения результатов с помощью визуального анализа группой экспертов и определения соотношения сигнал-шум выбиралось рациональное значение коэффициента p, позволяющее делать маркировку не только стойкой, но и незаметной.

Показан результат работы разработанной программы по выявлению внесённых изменений в промаркированные изображения (рис. 2). Выявлены измененные фрагменты изображения и предположительные действия с ним. Белая сетка – сигнатура неизменная, черная – слетели значения. Красные блоки указывают на то, что ЦВЗ изменен, зелёные – ЦВЗ распознан.

Рис. 1 – Промаркированное исходное изображение

Рис. 2 – Изменённое изображение, прошедшее процедуру распознавания встроенных меток в разработанном программном модуле

IV. Список литературы

1. Белобокова, Ю. А. Метод многократной маркировки цифровых фотографий для защиты от фальсификации / Ю. А. Белобокова, Е. В. Булатников // Известия высших учебных заведений. Проблемы полиграфии и издательского дела. – 2014. – №2 – С. 33–41
2. Белобокова, Ю. А. Защита информационного содержания цифровых фотографий методом многократной маркировки цифровыми водяными знаками / Ю. А. Белобокова, Э. С. Клышинский // Системный администратор. – 2014. – №4 – С. 70–73
3. Koch, E. TTowards Robust and Hidden Image Copyright Labeling / Koch E., Zhao J. // IEEE Workshop on Nonlinear Signal and Image Processing. Halkidiki, Greece – 1995 – P. 452–455.