УДК 004.9

МОДЕЛЬ ЗАЩИТНОЙ МАРКИРОВКИ РАСТРОВЫХ ИЗОБРАЖЕНИЙ

[1] Белобокова Ю.А.

[1] Национальный исследовательский университет «Московский государственный технический университет имени Н.Э. Баумана» (МГТУ им. Н.Э. Баумана), Москва, Россия (105005, Москва, 2-я Бауманская ул., д. 5, стр. 1), e-mail: yulya.belobokova@mail.ru

Описана модель защитной маркировки растровых изображений, включающая в себя алгоритмы маркировки и проверки аутентичности и целостности защищенных изображений.

Ключевые слова: растровые изображения, цифровые водяные знаки, ЦВЗ.

MODEL SECURITY MARKING RASTER IMAGES

[1]Belobokova Yu.A.

[1] Federal state budgetary institution of higher professional education BAUMAN MOSCOW STATE TECHNICAL UNIVERSITY,Moscow, Russia (105005, Moscow, 2nd Bauman Str., D. 5, p. 1), e-mail: yulya.belobokova@mail.ru

The model of the security marking of raster images, including a marking algorithm and verify the authenticity and integrity of protected images.

Key words: bitmaps, digital watermarks, DWM.

Введение

Одним из способов доказательства аутентичности растровых изображений, не включающих в себя анимацию, заимствованных из таких источников, как электронные издания, электронные СМИ, а также сайты фотографов и графиков, является защитная маркировка цифровыми водяными знаками (ЦВЗ), представляющими собой невидимые метки. В качестве меток могут использовать другие растровые изображения, в том числе монохромные, а также различные числовые массивы или последовательности.

Заимствованные изображения могут подвергаться ряду внешних воздействий, таких, как кадрирование, изменение цветовой модели, ретуширование, клонирование фрагментов или добавление новых элементов, масштабирование, повороты, смена цифрового формата. Поэтому встроенные в растровое изображение ЦВЗ должны быть стойкими к данным воздействиям.

Проектируемая модель защитной маркировки растровых изображений должна была не только подтверждать их аутентичность, но и указывать на факт изменения их целостности, а также учитывать особенности их цифровых форматов.

Разработанная модель включает в себя алгоритмы защитной маркировки растровых изображений и проверки целостности маркированных изображений, а также базу данных, в которой хранятся защищенные изображения и сопроводительная информация (название,

дата создания, геометрические размеры, вид защитной маркировки, ключ, с помощью которых она осуществлялась и т.д.).

Поскольку за последние десятилетия было разработано большое количество алгоритмов и методов встраивания ЦВЗ [5], поэтому для основы разрабатываемых алгоритмов защитной маркировки и проверки аутентичности и целостности изображений было решено выбрать один из уже существующих методов. Критериями выбора служили тип встраиваемых водяных знаков, геометрические размеры знака, а также способ внедрения в растровое изображение.

Поскольку маркировка должна указывать на изменение целостности растровых изображений, было решено использовать метод, основанный на внедрении ЦВЗ, много меньшего, чем защищаемое изображение.

Модель защитной маркировки растровых изображений

При разработке модели предполагалось, что маркироваться будут изображения, сохраненные в наиболее распространенных растровых форматах: BMP, PNG и JPEG. Растровый формат JPEG использует алгоритм сжатия с потерями, использующий дискретное косинусное преобразование (ДКП). Считается [2], что использование в алгоритме внедрения ЦВЗ преобразования, используемого в алгоритме сжатия изображений, повышает стойкость внедренных данных. В связи с этим было решено использовать метод, внедряющий водяные знаки с использованием ДКП.

Из существующих методов для основы разрабатываемых алгоритмов был выбран метод Коха и Жао [1]. Данный метод использует поблочное ДКП для внедрения данных в изображение, нетребователен к виду встраиваемых ЦВЗ, а также производит извлечение данных по так называемой «слепой» схеме, т.е. без использования исходного изображения. Последнее важно в случае, когда к проверяемому изображению применялось кадрирование.

Для решения задачи разработки модели проверки промаркированных растровых изображений на аутентичность и целостность было решено разбить изображение на фрагменты и маркировать эти фрагменты двумя видами ЦВЗ: монохромным логотипом (одинаковым для всех фрагментов) и электронными сигнатурами (электронными подписями, ЭП).

Монохромный логотип представляет собой монохромное изображение, по размеру много меньшее фрагментов защищаемого изображения. Логотип необходим для доказательства аутентичности исследуемого изображения. Поскольку он одинаков для всех блоков, доказать факт аутентичности можно даже в случае сохранения целостности только одного исходного фрагмента. Также с помощью монохромного логотипа возможно проверить целостность промаркированных изображений: при замене их фрагментов инородными факт отсутствия

защитной маркировки укажет на фальсификацию. Таким образом, внедряемый монохромный логотип решает задачи аутентификации и подтверждения факта нарушения целостности растровых изображений при удалении их фрагментов, а также добавления инородной информации. Следовательно, монохромный логотип должен быть максимально стойким к возможным искажениям растрового изображения [3].

В отличие от монохромного логотипа, значения электронных сигнатур не являются постоянными для всех блоков, а зависят от различных параметров изображения. Электронная сигнатура является 16-ти битной строкой, в которой могут быть зашифрованы геометрические размеры изображения в пикселях (ЭП по ширине и ЭП по высоте), какие-либо характеристики фрагментов (например, ЭП по яркости зеленого канала текущего блока изображения), а также взаимосвязь блоков изображения (например, ЭП суммарных яркостей соседних блоков).

Маркировка электронными сигнатурами является менее стойкой к ряду воздействий на изображения, что дает возможность выявления факта этих воздействий:

– при кадрировании промаркированного растрового изображения выявленные при проверке значения ЭП с зашифрованными геометрическими размерами изображениями не совпадут с расчетными;

– при изменении в результате некоторых атак (например, применения фильтров цвета) характеристик промаркированного изображения несовпадение текущих и расчетных характеристик электронных сигнатур укажут на факт подделки изображения.

Таким образом, защитная маркировка монохромным логотипом и различными видами электронных сигнатур дает возможность подтверждения аутентичности, выявления нарушения целостности, а также фактов кадрирования, применения цветовых фильтров и инструментов автокоррекции, а также смены цветовой модели.

Разработанные алгоритмы защитной маркировки и проверки аутентичности и целостности растровых изображений были описаны в статьях [3] и [4].

Разработанная модель и алгоритмы были реализованы в виде программного модуля, написанного на языке программирования C# и предназначенного для работы в ОС Windows (версии XP и выше). С помощью данного программного модуля была проведена серия экспериментов для проверки устойчивости защитной маркировки. Результаты экспериментов представлены в таблице 1.

Таблица 1. Результаты устойчивости встроенных ЦВЗ

№	Вид атаки	Выявление ЦВЗ и сигнатуры	
		ЦВЗ	Сигнатура (ЭП)
1	Добавление инородных	Детектируется в неизмененных блоках, не находится в полных	Имеет верное значение в неизменённых блоках, неверна в

№	Вид атаки	Выявление ЦВЗ и сигнатуры	
		ЦВЗ	Сигнатура (ЭП)
	фрагментов	блоках инородного фрагмента. Обнаружение ЦВЗ в блоках, содержащих оригинальные фрагменты и инородные элементы, зависит от расположения и площади чужеродного фрагмента.	полных блоках инородного фрагмента. Корректность ЭП в блоках, содержащих оригинальные фрагменты и инородные элементы, зависит от типа ЭП[1] и расположения и площади чужеродного фрагмента.
2	Клонирование фрагментов изображения	Детектируется в неизмененных блоках, не находится в не подогнанных по сетке клонированных блоках. Нахождение ЦВЗ в блоках содержащих оригинальные и клонированные фрагменты, зависит от расположения и площади клонированного элемента.	Имеет верное значение в неизменённых, не верна в клонированных блоках. Корректность ЭП в блоках, содержащих оригинальные и инородные фрагменты, зависит от типа ЭП[2] и расположения и площади чужеродного фрагмента.
4	Кадрирование		
А	Обрезка справа	Детектируется.	Согласно алгоритму расположения ЭП: в каждом пятом блоке значение неверно.
Б	Обрезка снизу	Детектируется.	Согласно алгоритму расположения ЭП. В каждом четвёртом блоке первого столбца значение неверно, далее циклично: значения неверны до столбца, начинающегося с начального значения ЭП.
В	Произвольное кадрирование	Детектируется, если кадрирование не произвольной формы, нарушающей геометрические размеры блока.	Согласно алгоритму расположения ЭП, циклично: значения неверны до столбца, начинающегося с начального значения ЭП.
5	Автоуровни-автоконтраст-автоцвета	Детектируется	Всегда верна только в блоках, где записаны размеры изображения.
6	Добавление фильтров цвета.	Детектируются в части блоков.	Значения неверны.
7	Резкость (исследовано на значениях 1-500%)	Детектируется в большинстве блоков.	Значения верны в случайно расположенных блоках**.**
8	Зашумление (исследовано на значении 2-4%)	Детектируются в части случайно расположенных блоков	Значения верны в случайно расположенных блоках.

[1] Может быть корректной в случае, если речь идёт о геометрических размерах не кадрированного изображения.
[2] Может быть корректной в случае, если речь идёт о геометрических размерах не кадрированного изображения.

№	Вид атаки	Выявление ЦВЗ и сигнатуры	
		ЦВЗ	Сигнатура (ЭП)
9	Смена цветовой модели (Lab, CMYK)	Детектируется в большинстве блоков.	В основном верна только в блоках, где записаны размеры изображения.
10	Смена цветовой модели (Grayscale)	Не детектируется	Не детектируется
11	Масштабиро-вание	При увеличении, а также уменьшении до 70% детектируется в большинстве блоков после возвращения исходного размера.	При увеличении, а также уменьшении до 70% детектируется в большинстве блоков после возвращения исходного размера.
12	Повороты	Детектируется в части блоков при обратном повороте.	Значения неверны.

Заключение

Анализ результатов экспериментов показал устойчивую работу и практическую применимость разработанной модели и алгоритмов. Проведенные эксперименты позволили разработать классификацию реакций защитной маркировки на различные виды модификации изображений.

Список литературы

1. Аграновский А.В., Балакин А.В., Грибунин В.Г., Сапожников С.А. Стеганография, цифровые водяные знаки и стеганоанализ. М.: Вузовская книга, 2009 г.

2. Белобокова Ю.А. Метод многократной маркировки цифровых фотографий для защиты от фальсификации. / Белобокова Ю.А., Булатников Е.В. //Известия высших учебных заведений. Проблемы полиграфии и издательского дела./ М.:МГУП, 2014. №2, С. 33–41.

3. 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. 7073.

4. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. Наука и учеба, 2002 г., 288 с.

5. Koch E., Zhao J. Towards Robust and Hidden Image Copyright Labeling //IEEE Workshop on Nonlinear Signal and Image Processing. 1995. P. 123-132.