Список используемых источников

1. Ковалгин Ю. А., Вологдин Э. И. Аудиотехника : учебник для вузов. М.: Горячая линия – Телеком, 2013. 742 с. ISBN 978-5-9912-0241-1.

2. Рогозинский Г. Г. Применение метода оптимизации вейвлетов в перцепционном кодировании звука // Радиотехника. 2010. № 5. С. 94–97.

3. Lee P. Wavelet Filter Banks in Perceptual Audio Coding, Master Thesis, University of Waterloo, Canada, 2003.

ИССЛЕДОВАНИЕ МЕТОДА АУТЕНТИФИКАЦИИ ДВОИЧНЫХ ИЗОБРАЖЕНИЙ ПРИ ПОМОЩИ ЦВЗ

В.И. Коржик, И.А. Тришневская

Аутентификация двоичных изображений является важным средством обеспечения информационной безопасности, особенно медицинских и полицейских баз данных. Однако известные методы аутентификации изображений с градациями серого и использования ЦВЗ не могут быть применены для решения непосредственно данной задачи. Поэтому предлагается техника с использованием сжатия арифметическими кодами некоторых функционалов двоичных изображений. Приводятся результаты экспериментов, которые показывают, что данный подход может обеспечить достаточную надежность аутентификации при одновременном выполнении высокого качества изображения сразу после вложения.

Ключевые слова: аутентификация, двоичные изображения, арифметическое кодирование

INVESTIGATION OF BINARY IMAGE AUTHENTICATION WITH THE USE OF DIGITAL WATERMARKING

Korzhik V., Trishnevskaya I.

Authentication of binary image is a very important approach in order to provide security especially of both medical and police databases. However it is impossible to use directly well-known methods of gray-scale image authentication with digital watermarking. The technique with the use of special image compression by arithmetic codes for solution of this problem is proposed. Experimental results regarding possible authenticator sizes and quality of images just after embedding are presented.

Keywords: binary images, authentication, arithmetic codes, texture of image

Аутентификация двоичных изображений (ДИ) является важным средством обеспечения информационной безопасности, особенно медицинских и полицейских баз данных.

Фундаментальной проблемой аутентификации ДИ является поиск метода вложения, который позволит затем восстановить исходное изображение без искажений.

Обычно вложение производится в цветные изображения или в изображения с градациями серого. Методы вложения основаны на том, что незначительное изменение в одном из цветовых каналов пикселя незаметно для человече-

ского глаза. Однако данные методы не могут быть применены к ДИ, так как заметно ухудшают качество исходного изображения.

В данной статье рассмотрен метод точной аутентификации ДИ, описанный в статье [1], который можно использовать для обнаружения несанкционированного изменения изображения.

Задача настоящей работы состоит в реализации данного алгоритма и проверке количества свободного места для вложения аутентификатора.

Сначала изображение делится на области 3x3 пикселя $X = (x_{ij})_{1 \le I,j \le 3}$, где $x_{ij} = 1$, если пиксель черный и $x_{ij} = 0$, если пиксель белый.

Затем для каждой области определяется дискриминационное отображение d: $X \to d(X)$:

$$d(X) = \sum_{i=1}^{3}\sum_{j=1}^{2}\left|x_{i,j+1} - x_{ij}\right| - \sum_{j=1}^{3}\sum_{i=1}^{2}\left|x_{i+1,j} - x_{ij}\right|.$$

Определяется операция инвертирования центрального пикселя в области:

$$f : X \to f(X) = Y = (y_{ij})_{1\le i,j\le 3},$$

$$y_{ij} = \begin{cases} x_{ij}, & if\ (i,j) \neq (2,2), \\ \left|1 - x_{ij}\right|, & if\ (i,j) = (2,2). \end{cases}$$

Теперь можно определить три типа областей: R – регулярные, S – сингулярные, U – неиспользуемые.

$$R = \{X \mid d(X) \neq 0\ \&\ d\big(f(X)\big) > d(X)\},$$

$$S = \{X \mid d\big(f(X)\big) \neq 0\ \&\ d\big(f(X)\big) < d(X)\},$$

$$U = \{X \mid d(X) = 0\ or\ d\big(f(X)\big) = 0\ or\ d\big(f(X)\big) = d(X)\}.$$

Очевидно, что $f(R) = S$, $f(S) = R$, $f(U) = U$.

Далее формируется RSU-последовательность σ и R-области заменяются на 1, S-области на 0, U-области на *nil*. Из полученной последовательности σ удаляются *nil*-области и {0, 1}-последовательность сжимается с помощью адаптированного арифметического кодирования [2].

После сжатия формируется код идентификации сообщения (*message authentication code* – MAC) – последовательность двоичных символов, полученных из ДИ криптографическим алгоритмом (типичная длина аутентификатора 64–256 бит)

Проверяется, можно ли добавить MAC к сжатой последовательности. Если $n_T - n_C \geq n_0$, где n_T – общее число R и S областей, n_C – длина сжатой последовательности, n_0 – длина MAC, то можно дописать MAC к сжатой последовательности. Иначе данное изображение не подходит для вложения данных.

Затем {0,1}-последовательность трансформируется обратно в RS. (U-области сохраняются неизменными)

Если элементы полученной последовательности и исходной не совпадают, значение центрального пикселя в соответствующих областях меняется ($f(R) = S$, $f(S) = R$).

Для проверки подлинности изображения с ЦВЗ выполняются следующие действия:

1. Берется ДИ с вложенным МАС. Формируется *RSU*-последовательность и назначаются 1, 0 и *nil*, как при вложении.

2. {0,1}-битный поток разделяется на МАС и сжатый *{R,S}*-вектор. Последовательность декодируется.

3. Изображение обрабатывается с целью регулирования состояния всех *R* и *S* областей, инвертируя, если это необходимо, центральный пиксель в исходное положение. Таким образом, получается точная копия исходного сообщения.

4. Формируется МАС, соответствующий полученному изображению и сравнивается с извлеченным в п. 2. Если МАС совпадают, значит ДИ подлинное.

В процессе исследования была собрана статистика для 100 ДИ.

Результаты для первых десяти изображений представлены в таблице 1. Затем на основании статистики для 100 изображений построен график (рис. 1). Большая часть из них при сжатии дает достаточно места для вложения МАС (64–500 свободных бит). Однако, около 18 % исследованных изображений непригодны для вложения.

ТАБЛИЦА 1. Результаты расчетов для первых 10 изображений.
N_R, N_S и N_U – количество *R*, *S* и *U* областей соответственно. $N_T = N_R + N_S$

Изображение	N_R	N_S	N_U	N_T	**Длина сжатой последовательности**	**Количество свободных бит**
0	10465	5367	13068	15832	14635	1197
1	9186	9246	10468	18432	18440	–8
2	15193	4557	9150	19750	15399	4351
3	6642	11571	10687	18213	17246	967
4	8641	9036	11223	17677	17678	-1
5	13191	5208	10501	18399	15823	2576
6	10537	7512	10851	18049	17690	359
7	11198	7748	9954	18946	18499	447
8	3343	4942	20615	8285	8069	216
9	15206	1687	12007	16893	7924	8969
10	16864	1396	10640	18260	7122	11138

Отрицательные значения последней колонки (табл. 1) указывают на то, что после арифметического кодирования длина последовательности, наоборот, увеличивается. Однако, в общем случае при достаточно большой последовательности арифметический кодер всегда приводит к возможности сжатия.

Далее была проверена связь между текстурностью изображения и количеством свободных бит после сжатия.

Текстурность была рассчитана как предлагается в [3]:

$$t_n = \frac{1}{n_1 \times n_2} \sum_{ij} (\max_k B_{ij}^k - \min_k B_{ij}^k).$$

Рис. 1. Кривая распределения частоты появления изображений для доступного объёма вложения после сжатия

Значения рассчитывались для областей 2x2, 3x3, 5x5, 6x6 и 10x10 (табл. 2).

ТАБЛИЦА 2. Фрагмент таблицы текстурностей

Номера изображений	**Количество свободных бит**	**Область 2x2**	**Область 3x3**	**Область 5x5**	**Область 6x6**	**Область 10x10**
28	89	0.003	0.002	0.002	0.001	0.001
26	93	0.003	0.002	0.002	0.002	0.001
14	1422	0.005	0.007	0.006	0.005	0.004
15	1894	0.054	0.034	0.016	0.012	0.005
12	8247	0.059	0.052	0.036	0.027	0.011
35	3805	0.067	0.047	0.024	0.018	0.007
46	1151	0.068	0.042	0.023	0.018	0.008
36	1974	0.075	0.049	0.029	0.023	0.01
93	5519	0.091	0.065	0.034	0.026	0.01

Таким образом, в данном исследовании связи между текстурностью ДИ и его пригодностью к вложению МАС выявлено не было. Как видно по рисунку 1, существуют некоторые изображения, для которых невозможно вложение. В дальнейшем исследовать расширение класса изображений, которые при сжатии дают достаточное количество бит для вложения. Также необходимо найти параметры, связанные с количеством свободных бит, чтобы предположить возможность вложения до выполнения алгоритма.

Список используемых источников

1. Korzhik V., Morales-Luna G. and Zubarev M. Distortion Free Exact Authentication of Binary Images // Journal of latex class files, vol. 6, no. 1, January 2007.

2. Кудряшов Б. Д. Теория информации : учебник для вузов. СПб.: Питер, 2009. 322 с. ISBN 978-5-388-00178-8.

3. Fridrich J. Steganography in digital media // Cambridge University Press, 2009. 466 p. ISBN-10: 0521190193, ISBN-13: 978-0521190190.