УДК 343.98

МЕТОД КОНТЕНТНО-ЗАВИСИМОГО МАРКИРОВАНИЯ ИЗОБРАЖЕНИЙ НА ОСНОВЕ БЕЗОПАСНОЙ ВИЗУАЛЬНОЙ СХЕМЫ РАЗДЕЛЕНИЯ СЕКРЕТА

А.А. БОРИСКЕВИЧ

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки, 6, Минск, 220013, Беларусь

Поступила в редакцию 29 июля 2016

Разработан метод контентно-зависимого маркирования изображений без внедрения цифрового водяного знака (ЦВЗ), основанный на визуальной схеме разделения секрета (ВСРС), позволяющей шифровать ЦВЗ в виде шумоподобных секретного и пуличного теневых изображений с помощью бинарных контентно-зависимых вейвлет-образов с визуально значимыми признаками и кодовой таблицы и восстанавливать ЦВЗ посредством выполнения логической операции (И, ИЛИ или исключающее ИЛИ) над секретным и публичным теневыми изображениями. Представлены результаты компьютерного моделирования.

Ключевые слова: визуальная схема, разделение секрета, бинарный контентно-зависимый вейвлет-образ.

Введение

В настоящее время одним из эффективных средств защиты мультимедийной информации является технология ЦВЗ – встраивание в защищаемый объект невидимых идентификационных меток, которые позволяют контролировать использование и распространение маркированного мультимедийного контента [1–3] Современные информационные технологии облегчают дублирование, манипуляции и распространение цифрового контента (изображения, видео и аудио). Реализация технологии защиты мультимедийного контента требует решения ряда сложных проблем: перцептуальная и статистическая незаметность ЦВЗ, устойчивость к контентно-сохраняющим воздействиям. Технология ЦВЗ наиболее подвержена коалиционным атакам [3] целью которых является генерация такой версии контента, которая не содержит идентификационной информации о пользователях или эта информация не может быть восстановлена. В свою очередь, в космических и медицинских системах не допускаются какие-либо изменения спутниковых и медицинских изображений [3, 4], которые могут повлиять на точность визуально значимой информации. В связи с этим актуальной проблемой является разработка технологий маркирования, основанных на принципах визуальной криптографии, удовлетворяющих повышенным требованиям безопасности данных и не подвергающих искажениям защищаемое изображение [5–7].

Метод контентно-зависимого вейвлет-маркирования изображений

Одним из эффективных решений проблемы робастного маркирования без искажений защищаемого изображения является использование визуальной схемы разделения секрета (ВСРС($k = 2$, $n = 2$)) [7], в которой ЦВЗ шифруется в виде $n = 2$ шумоподобных теневых изображений (частичных секретов) с помощью бинарных контентно-зависимых изображений с визуально значимыми признаками и кодовой таблицы и восстанавливается с помощью $k = 2$ теневых изображений (ТИ). Участниками при использовании схемы ВСРС (2,2) в системе

защиты авторских прав на контент (рис. 1) являются владельцы, имеющие права на контент защищаемого изображения, удостоверяющий центр, который разрешает споры посредством проверки авторских прав на изображение, и нарушитель, который модифицирует изображение для уменьшения вероятности восстановления ЦВЗ. Удостоверяющий центр генерирует личное шумоподобное бинарное ТИ, несущее информацию о защищаемом изображении, ЦВЗ и секретном ключе владельца контента. Личные ТИ и ЦВЗ регистрируются удостоверяющим центром. Для выявления нарушения цифровых прав владельца и незаконного распространения публичное ТИ извлекается из защищенного изображения. Бинарный ЦВЗ извлекается посредством выполнения логической операции (И (AND), ИЛИ (OR), исключающее ИЛИ (XOR)) над секретным и публичным ТИ.

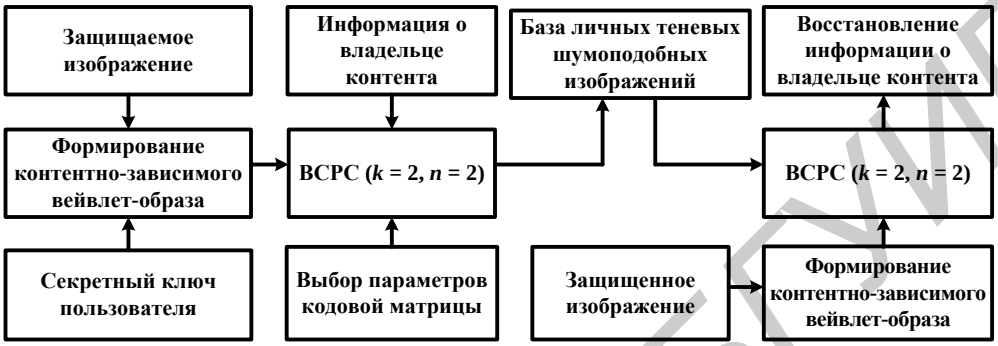


Рис. 1. Блок-схема контентно-зависимого вейвлет-маркирования изображений на основе визуальной схемы разделения секрета

Для увеличения устойчивости к контентно-неизменяющимся воздействиям (сжатие, фильтрации, аддитивный шум и другие) предлагается метод, основанный на выборе параметров элементов кодовой таблицы (табл. 1) и увеличения количество кодируемых пикселов ЦВЗ до двух (табл. 2), т.е. ВСРС (2,2) с $m = 2$ без расширения ТИ с использованием метрик их качества.

Таблица 1. **Параметры компонентов кодовой таблицы ВСРС (2, 2)**

Основные компоненты ВСРС (2, 2)	Параметры компонентов ВСРС (2, 2)
Исходное защищаемое изображение, бинарные изображения	Метрики качества, локально-глобальные статистические параметры, количество уровней вейвлет-декомпозиции, секретный ключ
ЦВЗ	Размер блока кодируемых пикселов ЦВЗ, вероятности выбора строки (столбца) с кодовыми блоками
Кодовые блоки	Количество черно-белых пикселов кодового блока, равенство вероятностей появления черных и белых пикселов кодового блока, равенство вероятностей использования кодовых блоков
Теневые изображения (ТИ)	Пороговое k и максимальное n количество теневых изображений, показатели качества ТИ
Восстановление ЦВЗ	Типы операций AND, OR, XOR, контраст и размер

Таблица 2. **Кодовая таблица ВСРС (2,2) с кодовыми блоками размером 1xm(m = 2)**

Пара пикселов ЦВЗ	Бинарный контентно-зависимый вейвлет-образ	Пара пикселов ТИ 1	Пара пикселов ТИ 2	Пара пикселов восстановленного ЦВЗ
00	0	10	10	10
Чет (01,10)	1	01	01	01
Нечет (01, 10)	0	10	01	11
11	1	01	10	11

Для обеспечения безопасности ТИ предложена процедура, основанная на увеличении количества одновременно кодируемых пикселов ЦВЗ до двух ($m = 2$), равное количеству пикселов кодового блока, при сохранении размеров восстановления ЦВЗ, то есть без расширения его размеров, и вычислении количества появлений каждой пары пикселов 01 и 10 в ЦВЗ. Предложенная кодовая таблица ВСРС (табл. 2) характеризуется множеством параметров ($k = 2, n = 2, m = 2$, $\alpha = 1/2^{k-1}$, p_r, p_{CB}, p_{BW}) (табл. 1). Параметр α определяет контраст восстановленного ЦВЗ. Предложенная кодовая таблица позволяет обеспечить

максимальный уровень безопасности информации в понятиях трех критериев качества визуального шифрования: равенство вероятностей p_r выбора строк кодовой таблицы, содержащих различные кодовые блоки ТИ для шифрования пары пикселов ЦВЗ, равенство вероятностей p_{BW} появления черных и белых пикселов кодового блока и равенство вероятностей p_{CB} использования кодовых блоков.

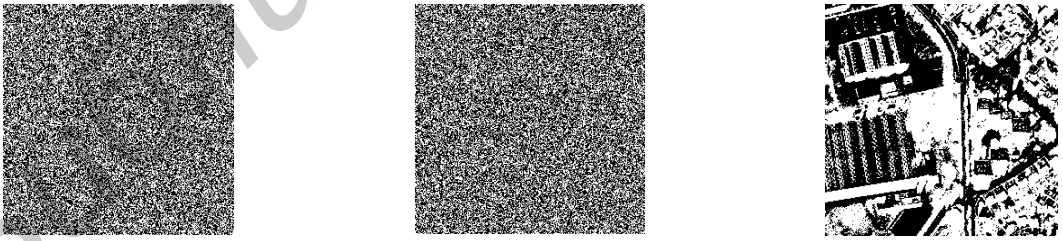
Существуют алгоритмы бинарных контентно-зависимых вейвлет-образов [8, 9], формируемые с помощью операции сравнения текущего вейвлет-коэффициента со значениями вейвлет-признака, вычисленными с помощью низкочастотных и среднечастотных вейвлет-коэффициентлв защищаемого изображения, что не обеспечивает требуемую безопасность ВСРС. Для повышения устойчивости к широкому спектру преднамеренных и непреднамеренных воздействий синтез бинарных контентно-зависимых вейвлет-образов $B_{LLj} = ((B_{LLji}(m,n), K_S))$ осуществляется с помощью соотношения

$$(B_{LLji}(m,n), K_S) = \begin{cases} 1 \text{ при } loc\,f(K_S, c_{LLji}(m,n)) \geq glob\,f(c_{LLj}(m,n)), \\ 0 \text{ при } loc\,f(K_S, c_{LLji}(m,n)) < glob\,f(c_{LLj}(m,n)), \end{cases} \quad (1)$$

где $loc\,f(\cdot)$ и $glob\,f(\cdot)$ – локальный и глобальный операторы обработки, определяющие вейвлет-признаки в окрестности определенного размера (3×3, 5×5 и 7×7) с центром в псевдослучайной i-й позиции j-го низкочастотного LLj поддиапазона значений $c_{LLji}(m,n)$ вейвлет-коэффициентов защищаемого изображения; j – индекс уровня вейвлет-разложения; K_S – секретный ключ владельца.

В качестве локальных и глобальных вейвлет-признаков предлагается использовать локальное среднее значение $loc\bar{c}_{LLji}(m,n) = (2k+1)(2l+1)^{-1}\sum_{m=-k}^{k}\sum_{n=-l}^{l}\left|c_{LLji}(m,n)\right|$, значение медианы $locmed(\left|c_{LLji}(m,n)\right|)$ в окрестности размером $(2k+1)(2l+1)$ или значение низкочастотного вейвлет-коэффициента $c_{LLj}(m,n)$ с центром в i-й псевдослучайной позиции LLj низкочастотного поддиапазона защищаемого изображения j-го уровня вевйлет-разложения, генерируемой псевдослучайным генератором с помощью секретного ключа, и глобальные среднее арифметическое значение $globaverage(\left|c_{LLj}(m,n)\right|)$ и значение медианы $globmed(\left|c_{LLj}(m,n)\right|)$ в пределах LLj низкочастотного диапазона.

На рис. 2 представлены бинарные контентно-зависимые вейвлет-образы для различных локально-глобальных статистических параметров низкочастотного поддиапазона LL одноуровневой вейвлет-матрицы изображения France с использованием вейвлет-функции Haar.



а *б* *в*

Рис. 2. Бинарные контентно-зависимые вейвлет-образы защищаемого изображения (France) для различных локально-глобальных статистических параметров низкочастотного поддиапазона:
а, б – локально-глобальные средние значения (ЛГС) и значения медианы (ЛГМ) низкочастотных вейвлет-коэффициентов; *в* – значения низкочастотных вейвлет-коэффициентов и глобальное значение медианы (ГМ) низкочастотных вейвлет-коэффициентов

Следует отметить, что безопасность схемы ВСРС зависит от соотношения вероятностией появления нулей и единиц в бинарных контентно-зависимых вейвлет-образов $B_{LLj} = ((B_{LLji}(m,n), K_S))$ кодовой книги ВСРС (табл. 2).

Результаты моделирования

В табл. 3 и 4 приведены оценки свойств бинарных контентно-зависимых вейвлет-образов для различных изображений размером 512×512 с использованием вейвлет-функции Haar.

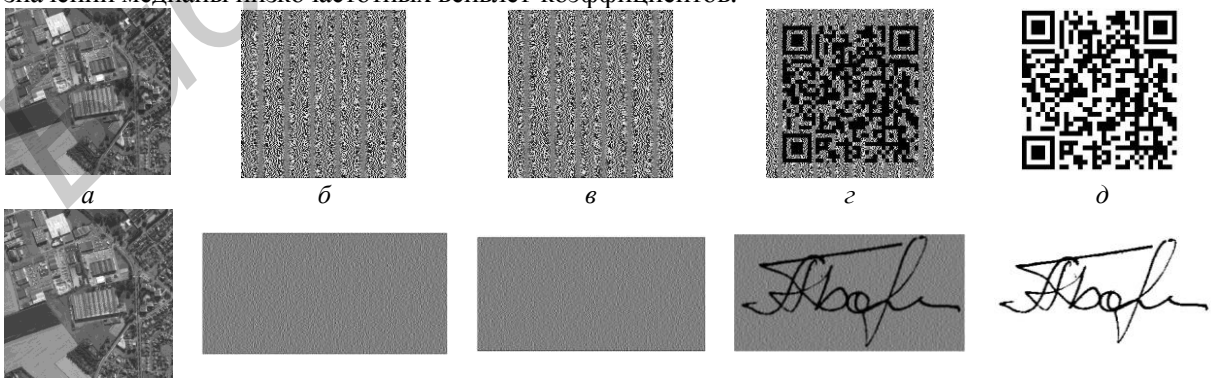
Таблица 3. **Оценка энтропии бинарных контентно-зависимых вейвлет-образов для одноуровневого уровня вейвлет-разложения различных полуионовых изображений**

Вейвлет-признаки	Lena	Barbara	Baboon	France
ГМ3 маска 3×3	0,999682	0,999928	0,999864	0,999772
ГМ5 маска 5×5	0,999995	0,999875	0,999864	0,999324
ГМ7 маска 7×7	0,999815	0,999546	0,999864	0,999324
ЛГС3 маска 3×3	0,996153	0,999594	0,999910	0,996140
ЛГС5 маска 5×5	0,997742	0,999973	0,999978	0,997866
ЛГС7 маска 7×7	0,997680	0,999997	0,999952	0,997892
ЛГМ3 маска 3×3	0,998871	0,994998	0,981232	0,992725
ЛГМ5 маска 5×5	0,999474	0,999297	0,997550	0,999804
ЛГМ7 маска 7×7	0,999825	0,999996	0,999150	0,999999

Таблица 4. **Оценка коэффициента межпиксельной корреляции бинарных контентно-зависимых вейвлет-образов для трех уровней вейвлет-разложения полутонового изображения France**

Вейвлет-признаки	1-й уровень	2-й уровень	3-й уровень
ГМ3 маска 3×3	0,669	0,509	0,394
ГМ5 маска 5×5	0,673	0,509	0,375
ГМ7 маска 7×7	0,673	0,521	0,379
ЛГС3 маска 3×3	0,0003	0,0076	0,0088
ЛГС5 маска 5×5	0,0054	0,0105	0,030
ЛГС7 маска 7×7	0,00302	0	0,0176
ЛГМ3 маска 3×3	0,00035	0,002	0,027
ЛГМ5 маска 5×5	0,006	0,0009	0,016
ЛГМ7 маска 7×7	0,0019	0,004	0,009

Из табл. 3 и 4 следует, что энтропия для бинарных контентно-зависимых вейвлет-образов, полученных из изображений размером 512×512 (Lena, Barbara, Baboon, France), почти не зависит от типа изображений, принимает значения не меньше 0,99 и достигает максимальных значений 0,999999 для использования ЛГМ вейвлет-признака (маска 7×7). Выявлено, небольшое влияние размера окрестности на увеличение энтропии и малое влияние уровня вейвлет-разложения на бинарную энтропию. Определено, что локально-глобальные алгоритмы обеспечивают минимизацию коэффициента корреляции для изображения France (от 0,0005 до 0,007) для первого и второго уровней вейвлет-разложения. В свою очередь, использование ГМ вейвлет-признака сохраняет максимальный коэффициент корреляции от 0,3 до 0,7 в зависимости от уровня вейвлет-разложения. На рис. 3 представлены результаты синтеза ТИ и восстановления ЦВЗ в виде личной подписи владельца контента и QR кода с использованием ВСРС (2,2) с $m = 2$ без расширения (табл. 2) и бинарных контентно-зависимых вейвлет-образов на основе локально-глобальных значений медианы низкочастотных вейвлет-коэффициентов.



а *б* *в* *г* *д*

е *ж* *з* *и* *к*

Рис. 3. Визуальное шифрование и восстановление ЦВЗ на основе ВСРС (2,2) с $m = 2$ без расширения: *а*, *е* – защищаемое изображение; *б*, *ж* – теневые изображения 1; *в*, *з* – теневые изображения 2; *г*, *и* – восстановленные ЦВЗ (операция OR); *д*, *к* – восстановленные ЦВЗ (операция XOR)

Для оценки защищенности маркированных изображений (табл. 5) использованы коэффициент $r_{x,y}^{(l)}$ межпиксельной (вертикальной, диагональной и горизонтальной) корреляции [10] и информационная энтропия H бинарных ТИ:

$$r_{x,y}^{(l)} = \frac{\mathrm{cov}_l(x,y)}{\sqrt{D_l(x)} \cdot \sqrt{D_l(y)}}, \quad (2)$$

$$H = -p\log_2 p - (1-p)\log_2(1-p), \quad (3)$$

где $\mathrm{cov}_l(x,y) = N^{-1}\sum_{i=1}^{N}(x_{l,i} - E_l(x))(y_{l,i} - E_l(y))$ – среднее значение ковариации пар l-го типа значений соседних пикселов $x_{l,i}$ и $y_{l,i}$ ТИ; $l = \{V, H, D\}$ – тип вертикальных *V*, горизонтальных *H* и диагональных *D* пар соседних пикселов ТИ; $E_l(x) = N^{-1}\sum_{i=1}^{N} x_{l,i}$ и $D_l(x) = N^{-1}\sum_{i=1}^{N}(x_{l,i} - E_l(x))^2$ – среднее значение и дисперсия значений пикселов $x_{l,i}$ ТИ для пар l-го типа; *i* и *N* – индекс и количество пар соседних пикселов, случайно выбранных из ТИ и равное 1000; *p* и (1–*p*) – вероятности появления значений черных и белых пикселов ТИ соответственно.

Таблица 5. **Оценка эффективности визуального шифрования WDP на основе ВСРС (2,2) с кодовыми блоками размером 1×*m*(*m* = 2) и 2×2 (*m* = 4)**

Метрики качества ТИ	Личная подпись			QR-код		
	m = 2		*m* = 4	*m* = 2		*m* = 4
	расшифровано	не расшифровано	расшифровано	расшифровано	не расшифровано	расшифровано
H_S	1,000	1,000	0,9999	1,0000	1,0000	0,9999
$r_{x,y}^{(l)}$	0,4985	0,0769	0,1639	0,5038	0,0790	0,1619

Из табл. 5 видно, что ВСРС (2,2) с парой пикселов ($m = 2$) без расширения в 6,25 и 2,0 раза безопаснее, чем ВСРС (2,2) с парой пикселов ($m = 2$) и четырьмя пикселами ($m = 4$) с расширением соответственно в понятиях коэффициента межпиксельной автокорреляции $r_{x,y}^{(l)}$ теневого изображения независимо от типа визуального шифруемого секретного изображения («личная подпись» и QR-кода).

Заключение

Разработан метод контентно-зависимого маркирования изображений без внедрения ЦВЗ, основанный на визуальной схеме разделения секрета (ВСРС(*k* = 2, *n* = 2)), позволяющей шифровать ЦВЗ в виде шумоподобных ТИ ($n = 2$) с помощью бинарных контентно-зависимых вейвлет-образов с визуально значимыми признаками и кодовой таблицы и восстанавливать ЦВЗ посредством выполнения логической операции (И (AND), ИЛИ (OR), исключающее ИЛИ (XOR)) над секретным и публичным ТИ (*k* = 2), что обеспечивает высокий уровень защищенности контента изображений без изменения их качества за счет выбора оптимальных параметров кодовой таблицы в понятиях критериев (равенство вероятностей выбора строк кодовой книги, равенство вероятностей появления черных и белых пикселов кодового блока и равенство вероятностей использования кодовых блоков) и критериев качества теневых изображений (информационная энтропия, коэффициенты межпиксельной автокорреляции).

Из результатов оценки качества синтеза контентно-зависимых изображений в вейвлет-области следует, что использование локально-глобальных средних арифметических значений вейвлет-коэффициентов обеспечивает энтропию (0,996...1,0) и коэффициент межпиксельной. корреляции (0,0003…0,003) для трех уровней вейвлет-разложения при использовании маски 3×3; локально-глобальных значений медианы вейвлет-коэффициентов – энтропию (0,999...1,0)

и коэффициент межпиксельной корреляции (0,0019...0,009) для трех уровней вейвлет-разложения при использовании маски 7×7 и глобальных значений медианы вейвлет-коэффициентов – энтропию (0,999...1,0) и коэффициент межпиксельной корреляции (0,375...0,673) для трех уровней вейвлет-разложения при использовании масок 3×3, 5×5, 7×7.

Установлено, что что ВСРС (2,2) с парой пикселов ($m=2$) без расширения в 6,25 и 2,0 раза безопаснее, чем ВСРС (2,2) с парой пикселов ($m=2$) и четырьмя пикселами ($m=4$) с расширением соответственно в понятиях коэффициента межпиксельной автокорреляции теневого изображения независимо от типа визуального шифруемого секретного изображения («личная подпись» и QR-кода).

METHOD OF CONTENT-DEPENDENT WATERMARKING IMAGES BASED ON SECURITY VISUAL SECRET SHARING SCHEME

A.A. BORISKEVICH

Abstract

A method of content-dependent watermarking images without embedding digital watermark based on visual secret sharing scheme, which allows to encrypt the digital watermark as a noise like secret and public shadow images using binary content-dependent wavelet-pattern with visually significance features and code table and to reconstruct the digital watermark by means of performing a logical operation (AND, OR or XOR) on a secret and a public shadow images. The results of computer simulation are represented.

Keywords: visual secret sharing scheme, binary content-dependent wavelet-pattern.

Список литературы

1. *Lu C.* Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property. Idea Group Publishing, 2004.
2. *Рябко Б.Я., Фионов А.Н.* Основы современной криптографии и стеганографии. М., 2013.
3. *Борискевич А.А., Полещук П.Л.* // Специальная техника. 2013. № 1. С. 22–33.
4. *Huang H.K.* PACS and Imaging Informatics. Basic Principles and Applications. John Wiley and Sons Ltd Publisher, 2010.
5. *Naor M., Shamir A.* // Eurocrypt. 1995. P. 1–12.
6. *Cimato S., Ching–Nung Yang Cimato S.* Visual Cryptography and Secret Image Sharing. CRC Press, Taylor & Francis Group, 2011.
7. *Борискевич А.А.* // Докл. БГУИР. 2012. № 5 (67). С. 73–79.
8. *Fu R., Jin W.* // The 2010 International Conference on Multimedia Technology (ICMT). 2010. P. 1–4.
9. *Rupachandra Singh T., Manglem Singh K., Roy S.* // Wavelet Transform International Journal of Computer Applications. 2012. Vol. 39, № 1. P. 18–24.
10. *Борискевич А.А.* // Докл. БГУИР. 2010. № 5(51) С. 31–39.