

АЛГОРИТМ ПОБЛОЧНОГО ВСТРАИВАНИЯ СТОЙКИХ ЦВЗ В КРУПНОФОРМАТНЫЕ ИЗОБРАЖЕНИЯ

Глумов Н.И., Митекин В.А.

Институт систем обработки изображений РАН

Аннотация

В статье предложен новый алгоритм встраивания цифровых водяных знаков (ЦВЗ) в цифровые изображения, обеспечивающий устойчивость ЦВЗ к широкому набору преобразований изображения-контейнера и обладающий рядом преимуществ по сравнению с существующими алгоритмами встраивания стойких ЦВЗ.

Ключевые слова: стойкий цифровой водяной знак, стеганография, стеганализ.

Введение

Задача встраивания так называемых «стойких» цифровых водяных знаков [1] (далее ЦВЗ) в цифровые изображения в настоящее время является наиболее актуальной в сфере защиты авторских прав и защиты от несанкционированного копирования мультимедийных данных. Подобная сфера применения обуславливает следующие основные требования к применяемым алгоритмам встраивания ЦВЗ.

1. Максимальная устойчивость встроенного ЦВЗ к широкому набору искажений изображения-контейнера [1 - 3], таких как кадрирование, линейная и нелинейная фильтрация, сжатие с потерями и т.д. (под устойчивостью в данном случае подразумевается возможность обнаружения и извлечения ЦВЗ из искажённого изображения-контейнера).
2. Низкая вычислительная сложность процедур встраивания ЦВЗ, а также возможность производить встраивание ЦВЗ в мультимедийные данные в потоковом режиме [3] (в случае цифровых изображений – поблочно).

Существующие на данный момент алгоритмы встраивания стойких ЦВЗ в цифровые изображения обладают существенным недостатком – большинство из них осуществляет встраивание в частотной области [1, 2], т.е. необходимыми этапами встраивания ЦВЗ в изображение являются прямое и обратное ДПФ всего изображения-контейнера. Данный подход, обеспечивая устойчивость встроенного ЦВЗ к повороту, масштабированию и кадрированию изображения-контейнера (так называемый RST-invariant watermarking), в то же время значительно повышает вычислительную сложность процедуры встраивания и делает невозможным поблочное встраивание ЦВЗ.

В настоящей работе представлен алгоритм встраивания стойких ЦВЗ, позволяющий встраивать ЦВЗ в изображение-контейнер путём его (изображения) поблочной обработки и не требующий выполнения спектральных преобразований изображения-контейнера при встраивании ЦВЗ. Кроме того, представленный алгоритм, как и алгоритмы, основанные на спектральных преобразованиях контейнера, обеспечивает устойчивость ЦВЗ к повороту, масштабированию, кадрированию изображения-контейнера, а также к ряду других распространённых

преобразований (сжатие с потерями, аддитивному зашумлению, линейной фильтрации и т.д.).

Разработанный алгоритм также может считаться устойчивым к наиболее известным атакам на алгоритмы встраивания стойких ЦВЗ, таким как watermark copy attack, watermark template attack.

1. Обзор существующих алгоритмов встраивания стойких ЦВЗ

Существующие алгоритмы встраивания стойких ЦВЗ могут быть условно разделены на 2 класса.

Алгоритмы встраивания ЦВЗ в области преобразования, инвариантного к заданным типам искажений. Данная группа алгоритмов [4 - 7] предполагает встраивание ЦВЗ непосредственно в области преобразования (transform domain), инвариантного к наиболее распространённым преобразованиям изображения-контейнера. Для уже упомянутых выше методов класса «RST-invariant watermarking» таким преобразованием является преобразование Фурье-Меллина. Основными недостатками данного класса алгоритмов являются вычислительная сложность и значительное искажение изображения-контейнера в процессе встраивания при вычислении прямого и обратного преобразования Фурье-Меллина. Кроме того, большинство алгоритмов данного класса используют так называемый «закрытый» детектор [1] и не позволяют встраивать в качестве ЦВЗ произвольную, не известную получателю, последовательность бит.

Алгоритмы, использующие так называемые «метки синхронизации» для оценки и компенсации искажений изображения-контейнера. В данном случае до встраивания ЦВЗ в изображение-контейнер встраиваются устойчивые к искажениям «метки», позволяющие впоследствии оценить и компенсировать искажения, внесённые в изображение-контейнер после встраивания. В качестве таких меток наиболее часто используются локальные экстремумы в заданных областях энергетического спектра изображения [8 - 9]. Основным недостатком алгоритмов данной группы является их неустойчивость к атаке «watermark template attack». Фактически, нарушитель, не зная ключа встраивания, может обнаружить и удалить из изображения-контейнера «метки синхронизации» (данные метки одинаковы

для всех изображений-контейнеров со встроенным ЦВЗ и не зависят от ключа встраивания), что сделает невозможным дальнейшее обнаружение ЦВЗ.

В следующих разделах представлен и исследован разработанный авторами алгоритм встраивания стойких ЦВЗ, не обладающий рассмотренными недостатками и позволяющий производить встраивание стойкого ЦВЗ путём поблочной обработки изображения-контейнера.

2. Разработанный алгоритм встраивания стойкого ЦВЗ в цифровые изображения

Предлагаемый алгоритм встраивания основан на суммировании изображения-контейнера с шумоподобным двумерным сигналом, кодирующим ЦВЗ. В качестве ЦВЗ может быть использована произвольная последовательность бит $W_{bit}(m)$, где $m \in [0, M - 1]$, например, код правообладателя, номер серии или дата получения изображения.

Синтез изображения, кодирующего ЦВЗ (далее изображения-ЦВЗ) производится следующим образом.

В качестве стеганографического ключа выступает пара одномерных бинарных кодовых последовательностей $S_1(k)$ и $S_0(k)$, соответствующих 1 и 0 встраиваемого ЦВЗ. Длина последовательностей принята равной $K = 180$, последовательности выбираются таким образом, чтобы для обеих последовательностей выполнялись условия:

$$\begin{cases} \sum_{k=0}^{K-1} S_0(k) \ll K \\ \sum_{k=0}^{K-1} S_1(k) \ll K \\ \sum_{k=0}^{K-1} S_1(k) \approx \sum_{k=0}^{K-1} S_0(k) \\ \max_{\Delta k} \sum_{k=0}^{K-1} S_0(k) \cdot S_1(\text{mod} \frac{(k + \Delta k)}{K}) \ll \sum_{k=0}^{K-1} S_1(k). \end{cases}$$

Далее изображение-ЦВЗ $W(n_1, n_2)$ размером $N \times N$ отсчетов, кодирующее последовательность бит $W_{bit}(m)$, синтезируется следующим образом.

1. Спектр $C_{pol}(r, \varphi)$ изображения-ЦВЗ в полярных координатах, где $r \in [0, N/2]$, $\varphi \in [0, 179]$, формируется следующим образом:

$$|C_{pol}(r, \varphi)| = \begin{cases} 1, & \text{если } r = R_0 + m \cdot R_{step} \cap S_1(\varphi) = 1 \cap W_{bit}(m) = 1, \\ 1, & \text{если } r = R_0 + m \cdot R_{step} \cap S_0(\varphi) = 1 \cap W_{bit}(m) = 0, \\ 0, & \text{иначе,} \end{cases}$$

где $R_{step} \in \left[1, \frac{N/2 - R_0}{M}\right]$ и $R_0 \in [1, N/2]$ – некоторые константы. При этом значения фазы ненулевых компонент $C_{pol}(r, \varphi)$ выбираются случайным образом.

2. Выполняется преобразование спектра $C_{car}(u, v) = \text{cartesian}(C_{pol}(r, \varphi))$, где cartesian – дискретное преобразование из полярных в декартовы координаты с использованием билинейной интерполяции [10].

3. Изображение-ЦВЗ $W(n_1, n_2)$ размером $N \times N$ вычисляется путём обратного ДПФ от $C_{car}(u, v)$.

Пример синтезированного для $M = 12$ изображения-ЦВЗ размером 512×512 пикселей приведён на рис. 1.

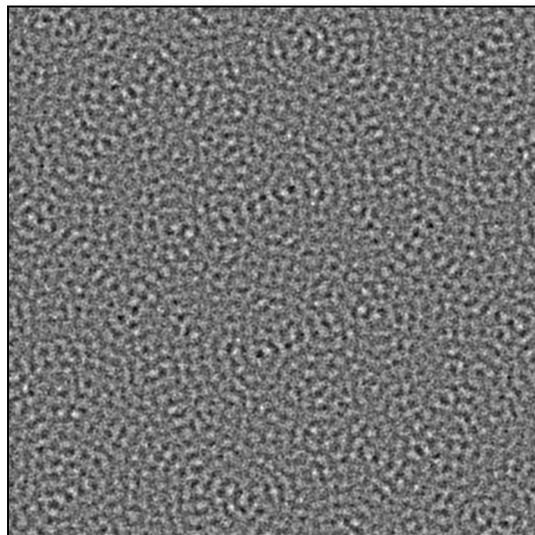


Рис. 1. Пример шумоподобного изображения ЦВЗ

Встраивание ЦВЗ производится путём сложения изображения-контейнера $I(m_1, m_2)$, где $m_1 \in [0, M_1 - 1]$, $m_2 \in [0, M_2 - 1]$, и изображения-ЦВЗ $W(n_1, n_2)$:

$$I'(m_1, m_2) = I(m_1, m_2) + Q \cdot \sqrt{\frac{I_{disp}(m_1, m_2)}{W_{disp}}} \times (W(\text{mod}(m_1 / N), \text{mod}(m_2 / N)) - W_{mean}),$$

где $I_{disp}(m_1, m_2)$ – поле локальной дисперсии изображения-контейнера, W_{mean} и W_{disp} – средняя яркость и дисперсия изображения-ЦВЗ $W(n_1, n_2)$ соответственно, $I'(m_1, m_2)$ – изображение-контейнер со встроенным ЦВЗ, Q – коэффициент усиления ЦВЗ, mod – остаток от деления.

Следует отметить, что предложенный алгоритм позволяет встраивать ЦВЗ, обрабатывая изображение-контейнер поблочно, с размером блока $N \times N$ пикселей. При этом размеры изображения-контейнера M_1 и M_2 могут быть сколь угодно большими.

Примеры изображений-контейнеров со встроенным ЦВЗ приведены на рис. 2. Необходимо отметить, что выбор параметров встраивания Q значительно влияет на визуальное качество изображения

(при увеличении Q визуальное качество снижается); экспериментальным путём установлено, что визуально заметным ЦВЗ становится при $Q > 0,25$.

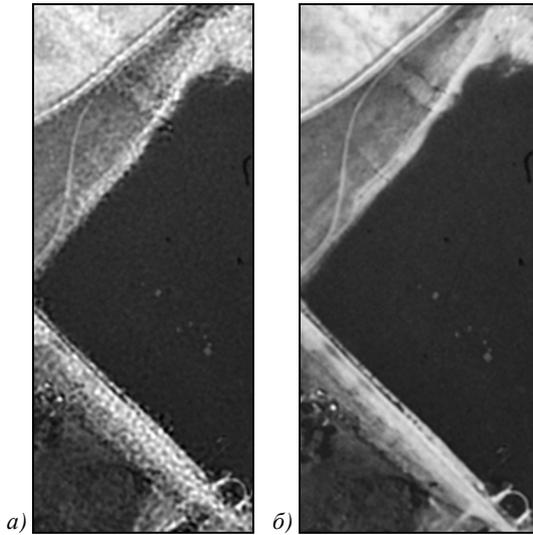


Рис. 2. Изображения-контейнеры со встроенным ЦВЗ (фрагменты): $Q=0,5$ (а); $Q=0,07$ (б)

Извлечение ЦВЗ производится следующим образом. Изображение-контейнер $I'(m_1, m_2)$ делится на L непересекающихся фрагментов $I'_i(n_1, n_2)$, где $n_1, n_2 \in [0, N-1]$. Далее, для каждого из фрагментов вычисляется модуль центрированного спектра $C_i(n_1, n_2)$ и усреднённый модуль спектра $C'(n_1, n_2) = \frac{1}{L} \sum_{i=0}^{L-1} C_i(n_1, n_2)$.

После чего вычисляется представление $C_{pol}(r, \varphi)$ усреднённого модуля спектра $C'(n_1, n_2)$ в полярных координатах (аналогично [10]), где $r \in [0, N/2]$, $\varphi \in [0, 179]$.

Далее вычисляются значения $R_0(r)$ и $R_1(r)$ как максимумы построчной нормированной взаимной корреляции $C_{polar}(r, \varphi)$ с кодовыми последовательностями $S_1(k)$ и $S_0(k)$, соответственно.

Обнаружение и извлечение битов ЦВЗ производится независимо для каждой строки $C_{pol}(r, \varphi)$. Бит ЦВЗ обнаружен в строке r_0 в том случае, если $|R_1(r_0) - R_0(r_0)| > T$, где T – пороговое значение, определяемое экспериментально на обучающей выборке изображений-контейнеров. В случае, если при некотором r_0 условие $|R_1(r_0) - R_0(r_0)| > T$ выполнено, первый бит ЦВЗ считается обнаруженным и его значение вычисляется как

$$W(0) = \begin{cases} 0, & \text{если } R_1(r_0) < R_0(r_0), \\ 1, & \text{если } R_1(r_0) > R_0(r_0). \end{cases}$$

Далее последовательно производится поиск значений $r_m \in [r_{m-1}, N/2]$, удовлетворяющих условию

$|R_1(r_m) - R_0(r_m)| > T$, и обнаружение очередного бита ЦВЗ $W(m)$.

3. Результаты экспериментального исследования стойкости ЦВЗ

Для исследования устойчивости алгоритма извлечения и обнаружения ЦВЗ к искажениям изображения-носителя был проведён следующий вычислительный эксперимент. Было синтезировано изображение $W(n_1, n_2)$, кодирующее ЦВЗ, с параметрами $N = 1024$, $R_{step} = 15$, $R_0 = 128$, $M = 12$. Далее для набора из 100 изображений-контейнеров размером 4096×4096 пикселей было произведено встраивание ЦВЗ в каждое изображение-контейнер. Для каждого изображения-контейнера было произведено 3 реализации встраивания с различными значениями $Q = \{0,07; 0,15; 0,25\}$. Во всех случаях встраивание производилось в зелёный канал цветного изображения, представленного в виде RGB-компонент. В результате встраивания было получено 300 выходных изображений-контейнеров со встроенным ЦВЗ.

Далее все изображения тестового набора подвергались заданному типу искажений (табл. 1, первый столбец) и из искажённых изображений извлекался ЦВЗ.

Для каждого типа искажений по выборке из 300 изображений-контейнеров была вычислена эффективность извлечения ЦВЗ $P_{изв} = N_{изв}/100$. В качестве величины $N_{изв}$ выступало количество изображений выборки, для которых после искажения были обнаружены и корректно извлечены все биты ЦВЗ и не было обнаружено «ложных» бит. Результаты экспериментального исследования эффективности извлечения ЦВЗ, а также результаты сравнения предложенного метода с существующими методами встраивания стойких ЦВЗ приведены в табл. 1.

Полученные результаты показывают, что разработанный алгоритм встраивания ЦВЗ обладает достаточной для применения на практике устойчивостью к основным типам искажений изображения-контейнера и по ряду показателей превосходит существующие аналоги.

Заключение

В настоящей работе представлен алгоритм встраивания стойких ЦВЗ, позволяющий встраивать ЦВЗ в изображение-контейнер путём его (изображения) поблочной обработки и не требующий выполнения спектральных преобразований изображения-контейнера. Разработанный алгоритм также позволяет встраивать в качестве ЦВЗ произвольную последовательность бит, неизвестную получателю, т.е. реализует так называемый «открытый» детектор ЦВЗ.

Таблица 1. Эффективность извлечения ЦВЗ из искажённого изображения-контейнера, $P_{обн}$

	Разработанный метод		Метод Digi-marc [11]	Метод Сох [12]
	$Q = 0,07$	$Q = 0,25$		
Искажения изображения-контейнера				
Кадрирование (до 25%)	0,99	1,00	нет данных	0,827
Аддитивный шум $\sigma = 15$	0,99	1,00	нет данных	нет данных
Медианная фильтрация окном 3×3	0,92	0,99	нет данных	нет данных
Поворот на 15° и кадрирование до 25% площади	0,98	1,00	0,95	нет данных
JPEG-сжатие, $q = 80$	0,94	1,00	0,65	нет данных

Кроме того, как показывают результаты экспериментального исследования, представленный алгоритм обеспечивает устойчивость ЦВЗ к повороту, масштабированию, кадрированию изображения-контейнера, а также к ряду других распространённых преобразований (сжатию с потерями, аддитивному шуму, линейной фильтрации и т.д.).

Разработанный алгоритм, в отличие от ряда существующих алгоритмов, не предполагает использование фиксированных «меток синхронизации» для обеспечения устойчивости ЦВЗ к искажениям и, следовательно, может считаться устойчивым к так называемым атакам с известным шаблоном ЦВЗ (watermark copy attack, watermark template attack).

Благодарности

Работа выполнена при поддержке ФЦП «Научные и научно-педагогические кадры инновационной России» (контракт № 02.740.11.00001) и РФФИ

(гранты 11-07-12059-офи-м-2011, 11-07-12062-офи-м-2011, 09-01-00511).

Литература (References)

1. Cox, I.J. Digital watermarking and steganography / M. Miller, J. Bloom, J. Fridrich. – San Francisco: Morgan Kaufmann Publishing, 2008. – 624 p.
2. Barni, M. Watermarking Systems Engineering: Enabling Digital Assets Security and Other Applications / M. Barni, F. Bartolini. – New York: Marcel Dekker, 2004. – 446 p.
3. Furht, B. Multimedia Security Handbook / B. Furht, D. Kirovski – Boca Raton, Florida: CRC Press, 2005. – 815 p.
4. O'Ruanaidh, J.K. Rotation, scale, and translation invariant digital image watermarking / J.K. O'Ruanaidh, T. Pun // Proceedings of ICIP. – 1997. – Vol. 1. – P. 536-539.
5. O'Ruanaidh, J.K. Rotation, scale, and translation invariant spread spectrum digital image watermarking / J.K. O'Ruanaidh, T. Pun // Signal Processing. – 1998. – Vol. 66. – P. 303-317.
6. Lin, C.Y. Rotation, scale, and translation resilient watermarking for images / C.Y. Lin, M. Wu, J.A. Bloom, I.J. Cox, M.L. Miller, Y.M. Lui // IEEE Trans on Image Processing. – 2001. – N 10(5). – P. 767-782.
7. Kim, B.S. Robust digital image watermarking method against geometrical attacks / B.S. Kim, J.G. Choi, C.H. Park, J.U. Won, D.M. Kwak, S.K. Oh, C.R. Koh, K.H. Park // Real-Time Imaging. – 2003. – Vol. 9. – P. 139-149.
8. Pereira, S. Template based recovery of Fourier-based watermarks using log-polar and log-log map / S. Pereira, J.K. O'Ruanaidh, F. Deguillaume, G. Csurka, T. Pun // Proceedings of ICMCS. – 1999. – P. 870-874.
9. Pereira, S. Robust template matching for affine resistant image watermarks / S. Pereira, T. Pun // IEEE Trans. on Image Processing. – 2000. – Vol. 9(6). – P. 1123-1129.
10. Reddy, B. A FFT-Based Technique for Translation, Rotation, and Scale-Invariant Image Registration / B. Reddy, B. Chatterji // IEEE Trans. on Image Processing. – 1996. – Vol. 5. – P. 1266-1270.
11. Peticolas, F.P. Evaluation of copyright marking systems / F.P. Peticolas, R.J. Anderson // Proc. of IEEE Multimedia Systems. – 1999. – Vol. 1 – P. 574-579.
12. Bloom, J.A. Rotation, scale and translation resilient public watermarking for images / J.A. Bloom, I.J. Cox, M.L. Miller, C.Y. Lin, Y.M. Lui, M. Wu // Proc. SPIE Security Watermarking Multimedia Contents II. – 2000. – Vol. 3971. – P. 90-98.

THE ALGORITHM FOR LARGE-SCALE IMAGES ROBUST WATERMARKING USING BLOCKWISE PROCESSING

N.I. Glumov, V. A. Mitekin
Image Processing Systems Institute of the RAS

Abstract

A new algorithm for digital watermarking of large-scale digital images is proposed in the article. The proposed algorithm provides watermark robustness to a wide range of host image distortions and has a number of advantages compared to an existing algorithms of robust watermarking.

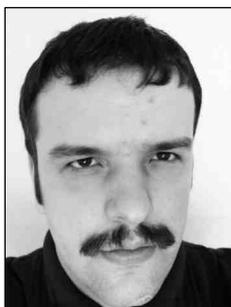
Key words: digital watermarking, robust watermark, blind watermark detection, watermark template attack.

Сведения об авторах

Глумов Николай Иванович родился в 1962 году. В 1985 году окончил Куйбышевский авиационный институт (ныне Самарский государственный аэрокосмический университет). В 1994 году защитил диссертацию на соискание степени кандидата технических наук. В настоящее время работает старшим научным сотрудником в Институте систем обработки изображений РАН. Круг научных интересов включает обработку изображений и распознавание образов, компрессию изображений, моделирование систем формирования цифровых изображений. Имеет свыше 100 публикаций, в том числе более 50 статей, две монографии (в соавторстве). Член Российской ассоциации распознавания образов и анализа изображений.

E-mail: nglu@smr.ru.

Nikolai Ivanovich Glumov (b. 1962) graduated from the Kuibyshev Aviation Institute (now Samara State Aerospace University) in 1985. In 1994, he defended his Ph.D. thesis in engineering. At present, Glumov is a senior scientist at the Institute of Image Processing Systems, Russian Academy of Sciences. His scientific interests include image processing and recognition, image compression, and simulation of digital image formation systems. He has more than 100 publications, including 50 articles and two monographs (with co-authors). He is a member of the Russian Association of Image Recognition and Analysis.



Митекин Виталий Анатольевич родился в 1983 году. В 2006 году окончил Самарский государственный аэрокосмический университет (СГАУ) по специальности «Прикладная математика и информатика». В 2009 году защитил диссертацию на соискание степени кандидата технических наук. В настоящее время работает научным сотрудником в Институте систем обработки изображений РАН. Круг научных интересов включает обработку изображений и распознавание образов, стеганографию и стегоанализ, криптографию. Имеет 19 публикаций, в том числе 5 статей.

E-mail: mitekin@smr.ru.

Vitaliy Anatolyevich Mitekin (b. 1983) graduated from the S. P. Korolyov Samara State Aerospace University (SSAU), majoring in Applied Mathematics and Informatics in 2006. He received his Candidate in Technical Sciences degree from Samara State Aerospace University in 2009. Currently he works as the researcher at the Image Processing Systems Institute of the Russian Academy of Sciences. He has 19 publications, including 5 articles. His scientific interests include image processing and recognition, steganography and steganalysis, cryptography.

Поступила в редакцию 24 июня 2011 г.