ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

УДК 004.056

В. А. Батура, А. Ю. Тропченко

ЭФФЕКТИВНОСТЬ АЛГОРИТМОВ МАРКИРОВАНИЯ ЦИФРОВЫХ ИЗОБРАЖЕНИЙ В ЧАСТОТНОЙ ОБЛАСТИ НА ОСНОВЕ ДИСКРЕТНОГО ПРЕОБРАЗОВАНИЯ АДАМАРА

Рассмотрены особенности применения дискретного преобразования Адамара для маркирования цифровых изображений. Исследована устойчивость алгоритма цифрового маркирования Elham к изменению размеров изображения, а также сжатию JPEG и JPEG2000.

Ключевые слова: *стеганография, цифровое маркирование, преобразование Адамара, цифровое изображение, JPEG-сжатие.*

Введение. В связи с широким распространением вычислительной техники актуальной стала задача защиты авторских прав на мультимедийную продукцию, в частности, неподвижные изображения. Эффективным средством решения этой задачи являются методы цифровой стеганографии [1].

В настоящей работе в качестве объекта защиты (контейнера) рассматриваются неподвижные (статические) цифровые изображения. Под скрываемым в объекте защиты сообщением подразумевается цифровой водяной знак (ЦВЗ), который не воспринимается глазом и в общем случае является некоторым двоичным кодом. Заметим, что для наглядности при извлечении ЦВЗ из маркированного изображения такой знак может представлять собой логотип [1]. На рис. 1 представлены контейнер (*а*), ЦВЗ — логотип (*б*) и стеганоконтейнер — изображение со встроенным ЦВЗ (*в*).

а) *б*) *в*)

Рис. 1

Для защиты цифровых изображений разработано множество стеганографических алгоритмов, каждый из которых обладает разной устойчивостью к атакам различного типа. Для неподвижных изображений наиболее распространенное искажение — сжатие, примерами которого являются форматы сжатия с потерями JPEG и JPEG2000. В работе рассмотрены алгоритмы цифрового маркирования изображения для встраивания ЦВЗ в контейнер, что обеспечивается разложением контейнера на ряд частотных коэффициентов преобразования (как правило, среднечастотных или низкочастотных) с последующей их модификацией.

Существует несколько алгоритмов встраивания ЦВЗ с контейнером, приведем один из наиболее распространенных [2]:

$$c_i' = c_i + \alpha w_i, \tag{1}$$

где c_i — частотный коэффициент, подлежащий изменению; c_i' — измененный коэффициент, w_i — встраиваемый элемент водяного знака; α — коэффициент силы встраивания (весовой коэффициент).

Извлечение ЦВЗ осуществляется в соответствии с выражением:

$$w_i = (c_i' - c_i)/\alpha. \tag{2}$$

При большом значении α повышается устойчивость водяного знака, однако может сильно снизиться качество защищаемого изображения, а слишком маленькое значение α делает водяной знак крайне уязвимым к различным атакам, например, компрессии (сжатию) или зашумлению.

В ряде частотных алгоритмов применяются различные спектральные преобразования изображения, в том числе дискретное косинусное (ДКП) и дискретное вейвлет-преобразование (ДВП), что обусловлено их использованием в форматах JPEG и JPEG2000 соответственно. Однако алгоритмы цифрового маркирования, основанные на ДКП, могут быть неустойчивы к сжатию JPEG2000, то же относится к ДВП при сжатии по алгоритму JPEG [1]. В связи с этим актуальной является задача разработки алгоритмов цифрового маркирования, обладающих устойчивостью вне зависимости от метода сжатия. В исследованиях отмечена высокая эффективность преобразования Адамара в решении данной задачи [3].

В настоящей статье рассматриваются особенности алгоритмов маркирования, основанных на использовании двумерного преобразования Адамара.

Преобразование Адамара относится к классу ортогональных преобразований в диадных базисах [4], оно обладает малой вычислительной сложностью по сравнению с ДКП и ДВП.

Ядром этого преобразования является матрица Адамара, элементы которой принимают значения 1 и –1, она описывает преобразование, связанное с разложением сигнала по семейству прямоугольных базисных функций [5].

Матрицы Адамара порядка $N=2^n$ (n — целое положительное число) формируются на основе операции кронекеровского умножения:

$$\mathbf{A}_{2N} = \mathbf{A}_N \otimes \mathbf{A}_2 = \begin{bmatrix} \mathbf{A}_N & \mathbf{A}_N \\ \mathbf{A}_N & -\mathbf{A}_N \end{bmatrix}, \tag{3}$$

где $\mathbf{A}_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ — матрица наименьшего порядка.

Наибольшее значение принимает низкочастотный DC-коэффициент, остальные коэффициенты — высокочастотные (AC). При этом полагается, что частота тем выше, чем чаще изменяется знак в строке. При этом AC-коэффициенты расположены в случайном порядке, что повышает надежность встраивания ЦВЗ [6].

Двумерное преобразование Адамара вычисляется по формуле:

$$\mathbf{F}_{KL} = \frac{1}{N}\sum_{m=0}^{N-1}\sum_{n=0}^{N-1} x_{mn}(-1)^{km+nl}, \qquad (4)$$

где m, n — номера пикселов исходного изображения; k, l — коэффициенты преобразования $(k, l = \overline{0, N-1})$.

Преобразование Адамара обладает свойством разделимости по переменным суммирования, для снижения вычислительных затрат двумерное преобразование реализуется строчно-столбцовым способом:

$$\mathbf{F}_N = \frac{1}{N}\mathbf{A}_N\left[\mathbf{X}_N\mathbf{A}_N\right], \qquad (5)$$

где $\mathbf{X}_N$ — исходное изображение, $\mathbf{F}_N$ — преобразованное в набор коэффициентов изображение, N — размер изображения. Тем самым объем вычислений сокращается с N^4 до $2N^3$ базовых операций (действий под знаками двойной суммы).

Дальнейшего уменьшения вычислительных затрат можно достичь при использовании алгоритма быстрого преобразования Адамара, позволяющего сократить число базовых операций с N^2 до $(N\log_2 N)/2$ при выполнении каждого одномерного преобразования.

Алгоритмы цифрового маркирования. В последнее время разработан ряд алгоритмов [3, 6—10], основой которых являются разновидности преобразования Адамара. Некоторые из алгоритмов предназначены для стеганосистем закрытого типа, не требующих наличия исходного изображения-контейнера для извлечения ЦВЗ [6, 8]. Для повышения устойчивости к сжатию в некоторых алгоритмах используется адаптивная модуляция [7], а для определения местоположения частотных коэффициентов внедряемого ЦВЗ — вычислительный коэффициент энтропии блоков изображения [3, 9, 10].

Алгоритм Elham [10] предназначен для стегосистем закрытого типа, поскольку для извлечения встроенного ЦВЗ необходимо наличие исходного изображения. Алгоритм основан на использовании быстрого преобразования Адамара и вычислении коэффициентов энтропии блоков контейнера.

Для уменьшения объема встраиваемой информации ЦВЗ разбивается на блоки размером 8×8 и подвергается ДКП, тем самым производится операция, подобная сжатию JPEG. Полученные блоки при помощи зигзаг-преобразования преобразуются в векторы, которые затем объединяются.

Контейнер также разбивается на блоки размером 8×8. Для каждого блока находится среднее значение коэффициентов энтропии. Блоки, среднее значение энтропии которых выше заданного, подвергаются преобразованию Адамара. В каждый преобразованный блок, с использованием коэффициента силы встраивания, по формуле (1) встраивается один коэффициент из вектора, полученного после преобразования Адамара. Операцию встраивания завершает обратное преобразование Адамара с последующим объединением модифицированных и немодифицированных блоков.

Для извлечения ЦВЗ требуется исходное изображение. Путем сегментации исходного изображения определяются координаты модифицированных блоков. Защищенное изображение также подвергается разбиению на блоки размером 8×8. Согласно формуле (2) осуществляется извлечение каждого коэффициента ЦВЗ. Полученный вектор разбивается на фрагменты

заданной длины. За счет обратного зигзаг-преобразования формируются исходные блоки коэффициентов ЦВЗ, к каждому из которых применяется обратное ДКП. Полученные блоки формируют изображение встроенного ЦВЗ.

В работе [10] данный алгоритм был проверен на ряд атак, таких как среднечастотная фильтрация, зашумление, JPEG-сжатие, изменение размера и яркости. В настоящей работе исследуется его устойчивость к:

— JPEG-сжатию с высокими коэффициентами сжатия;

— сжатию JPEG2000;

— атаке изменения размера изображения.

Исходные параметры алгоритма следующие: размер контейнера 512×512; размер ЦВЗ 64×64; порог энтропии 4,5; сила встраивания 35; контейнер и ЦВЗ разбиваются на блоки размером 8×8; число модифицированных коэффициентов каждого блока ЦВЗ 15.

Для оценки качества защищенного изображения используем пиковое отношение сигнала к шуму (PSNR):

$$\mathrm{PSNR} = 10\log_{10}\frac{255^2 MN}{\sum\limits_{m,n}^{M,N}(f(m,n)-\hat{f}(m,n))^2}, \qquad (6)$$

где $f(m,n)$ и $\hat{f}(m,n)$ — исходное и защищенное изображения; m, n — номера пикселов; M и N — высота и ширина изображения.

В качестве меры качества извлеченного ЦВЗ используем коэффициент корреляции Пирсона:

$$K = \frac{\sum\limits_m\sum\limits_n (A(m,n)-\bar{A})(B(m,n)-\bar{B})}{\sqrt{\sum\limits_m\sum\limits_n\left((A(m,n)-\bar{A})^2\right)\left(\sum\limits_m\sum\limits_n (B(m,n)-\bar{B})^2\right)}}, \qquad (7)$$

где $A(m, n)$, $B(m, n)$ — исходный и извлеченный ЦВЗ; $\bar{A}$, $\bar{B}$ — среднее арифметическое пикселов исходного и извлеченного ЦВЗ.

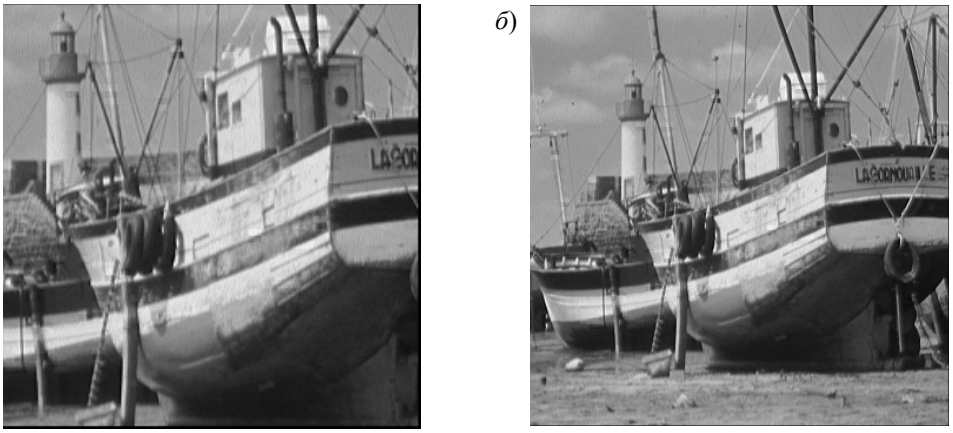
Качество маркированного изображения считается удовлетворительным, если PSNR не менее 40 дБ, извлеченный ЦВЗ устойчив к определенной атаке, если коэффициент корреляции Пирсона не ниже 0,5.

В таблице представлены коэффициенты сжатия JPEG и JPEG2000 и соответствующие им коэффициенты корреляции. Устойчивость к изменению размера иллюстрирует рис. 2.

Коэффициент сжатия JPEG, %	Коэффициент корреляции	Коэффициент сжатия JPEG2000, %	Коэффициент корреляции
73,6532	0,9918	4,8175	0,9932
83,3284	0,9874	83,9365	0,9741
87,4279	0,9812	92,1363	0,9028
89,4857	0,9706	94,6910	0,7446
91,9054	0,9478	96,0526	0,6390
94,8762	0,8338	96,8634	0,5132
97,5797	0,3260	97,3967	0,3506

На рис. 2 приведен стеганоконтейнер, усеченный до размеров 256×256 (*а*) и 356×356 (*б*). Соответствующие извлеченные ЦВЗ представлены на рис. 2, *в* (коэффициент корреляции Пирсона 0,1853) и *г* (0,3295).

а) *б*)



в) *г*)

Рис. 2

На основании полученных данных можно сделать вывод о том, что алгоритм Elham устойчив к JPEG-сжатию. Однако его устойчивость к сжатию JPEG2000 не столь высока. Кроме того, алгоритм является уязвимым к атаке изменения размера изображения.

Заключение. В работе установлено, что использование преобразования Адамара позволяет повысить устойчивость ЦВЗ к JPEG-сжатию и обеспечивает удовлетворительную устойчивость к сжатию JPEG2000.

СПИСОК ЛИТЕРАТУРЫ

1. *Грибунин В. Г., Оков И. Н., Туринцев В. И.* Цифровая стеганография. М.: СОЛОН-Пресс, 2002. 272 с.
2. *Cox I., Kilian J., Leighton T., Shamoon T.* Secure spread spectrum watermarking for multimedia // IEEE Transact. on Image Processing. 1997. Vol. 6, N 12, P. 1673—1687.
3. *Maity S. P., Kundu M. K.* Perceptually adaptive spread transform image watermarking scheme using Hadamard transform // Information Sciences. 2011. Vol. 181. P. 450—465.
4. *Тропченко А. Ю., Тропченко А. А.* Цифровая обработка сигналов. Методы предварительной обработки: Учеб. пособие по дисциплине „Теоретическая информатика“. СПб: СПбГУ ИТМО, 2009. 100 с.
5. *Прэтт У.* Цифровая обработка изображений. М.: Мир, 1982. Кн. 1. 312 с.
6. *Ho A. T. S., Shen J., Chow A. K. K., Woon J.* Robust digital image-image watermarking algorithm using fast Hadamard transform // Intern. Symp. on Circuits and Systems. 2003. Vol. 3. P. 826—829.
7. *Maity S. P., Kundu M. K.* DHT domain digital watermarking with low loss in image informations // Int. J. Electron. Commun. 2010. Vol. 64. P. 243—257.
8. *Saryazdi S., Nezamabadi-pour H.* A Blind Digital Watermark in Hadamard Domain // World Academy of Science, Engineering and Technology. 2007. Vol. 3.
9. *Rajkumar F.* // J. of Computer Applications. 2011. Vol. 12, N 9.
10. *Fami E. Sh., Samavi Sh., Kaviani H. R., Radani Z. M.* Adaptive Watermarking in Hadamard Transform Coefficients of Textured Image Blocks // 16th Intern. Symp. on Artificial Intelligence and Signal Processing (AISP). 2012.

Сведения об авторах

Владимир Александрович Батура — аспирант; Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, кафедра вычислительной техники; E-mail: batu-vladimir@yandex.ru

Александр Ювенальевич Тропченко — д-р техн. наук, профессор; Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, кафедра вычислительной техники; E-mail: tau@d1.ifmo.ru

Рекомендована кафедрой вычислительной техники

Поступила в редакцию 23.12.13 г.

УДК 004.056.53

К. А. Щеглов, А. Ю. Щеглов

НЕПРОТИВОРЕЧИВАЯ МОДЕЛЬ МАНДАТНОГО КОНТРОЛЯ ДОСТУПА

Исследована модель мандатного контроля доступа, выявлены противоречия и недостатки, не позволяющие реализовать на ее основе безопасную систему. Разработаны и обоснованы модель целостности и доступности и „непротиворечивая модель мандатного контроля доступа“, применение которой позволяет предотвращать нарушение конфиденциальности информации, а также решать задачи обеспечения ее целостности и доступности в комплексе.

Ключевые слова: *защита информации, контроль доступа, правила доступа, мандат, категории информации, уровни конфиденциальности.*

Введение. Сегодня широкое практическое применение нашла модель мандатного контроля доступа, основанная на использовании меток безопасности (или мандатов) [1]. Эта предложенная Белла—ЛаПадулой [2] модель, согласно нормативному документу в области информационной безопасности [1], предназначена для использования в наиболее критичных приложениях с целью защиты обрабатываемой информации от нарушения конфиденциальности. Однако существует и альтернативная модель мандатного контроля доступа, предложенная Бибом [3], предназначенная для обеспечения целостности и доступности информации. Правила контроля доступа, определяемые этими моделями, полностью исключают друг друга. Вместе с тем задачи защиты конфиденциальности информации и обеспечения ее целостности и доступности системы должны решаться комплексно.

Альтернативные модели мандатного контроля доступа. Основу мандатного контроля доступа составляет возможность ранжирования (присвоения категории) обрабатываемой информации на основании какого-либо признака.

Практика секретного делопроизводства в компьютерной обработке информации, согласно модели Белла—ЛаПадулы [2], предполагает классификацию информации по уровням конфиденциальности.

Метки безопасности *объектов* отражают категорию конфиденциальности информации, которые могут быть сохранены в соответствующих объектах. Метки безопасности *субъектов* отображают полномочия или уровень допуска (по аналогии с формой допуска в секретном делопроизводстве) субъектов к информации различных уровней конфиденциальности.

Будем считать, что чем больше полномочия субъекта C и выше уровень конфиденциальности объекта O, тем меньше их порядковый номер в упорядоченных множествах: