УДК 621.391

АЛГОРИТМ МАРКИРОВАНИЯ ИЗОБРАЖЕНИЙ НА ОСНОВЕ ВИЗУАЛЬНОЙ КРИПТОГРАФИИ ДЛЯ ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО РАСПРОСТРАНЕНИЯ ИНФОРМАЦИИ

А.А. БОРИСКЕВИЧ

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

Поступила в редакцию 12 мая 2012

Предлагается алгоритм маркирования изображений для защиты от копирования и незаконного распространения информации, основанный на принципах визуальной криптографии, представлении защищаемого изображения в виде набора взвешенных битовых плоскостей и двоичной маски маркирования (ДММ) в виде двух изображений-соответствий. Результаты моделирования показали, что алгоритм обеспечивает высокую защищенность изображений без изменения их качества и качественное восстановление ДММ пользователя без использования вычислительных средств.

Ключевые слова: защищаемое изображение, визуальная криптография, маска маркирования, битовая плоскость, фрактальная структура.

Введение

Быстрое развитие и широкое распространение информационных и коммуникационных технологий, простота передачи и распространения информации в компьютерных сетях влекут за собой необходимость защиты публикуемых в открытом доступе или передаваемых по сети электронных документов. Одним из средств предотвращения несанкционированного доступа является шифрование сообщений, чтобы данные не были использованы третьим лицом. Для предотвращения несанкционированного использования данных, их модификации и нарушения авторских прав распространяемой информации (например, плагиат – присвоение авторства другим лицом), а также незаконного распространения данных используются различные технологии маркирования: ДММ в виде цифрового водяного знака (ЦВЗ) и цифрового фингерпринта (ЦФ) [1]. В первом случае все защищаемые документы маркируются кодом ЦВЗ, одинаковым для всех пользователей и разными для всех владельцев, а во втором случае – кодом ЦФ, уникальным для каждого пользователя. Они идентифицируют владельца документа, обеспечивают возможность подтверждения подлинности авторства в любой момент использования документа и удерживают пользователя от нелегального распространения контента документа.

Для повышения уровня защищенности контента изображения без любой его модификации могут быть использованы алгоритмы визуальной криптографии [2-6], обладающие следующими свойствами:

- регулярность (производятся одинаковые действия для каждого исходного пикселя);
- независимость (каждый исходный пиксель шифруется независимо от других);
- простота (возможно визуальное расшифрование посредством физического процесса наложения шумоподобных изображений без вычислений).

В [2] предложена визуальная схема разделения секретной информации k из n (ВСРС (k, n)). В данной ВСРС (k, n) секретная информация K делится на n частей (по числу участников схемы):

- любые k участников могут составить из частей секретную информацию K;

- ни одна группа из ($k-1$) участников не может восстановить всю секретную информацию K или его часть.

Секретной информацией для ВСРС может быть любая информация, например ДММ. Сущность ВСРС заключается в том, что секретное изображение разделяется на k частей и они раздаются n участникам схемы. Каждая часть представляет собой некоторое шумоподобное изображение на прозрачной пленке-диапозитиве. Если k участников совместят свои пленки-диапозитивы друг с другом в произвольной последовательности, то они смогут увидеть секретное изображение, в то время как меньшее число участников – нет. Наиболее простой структурой ВСРС является схема ($k=2$ из $n=2$). В этом случае секретное бинарное изображение шифруется двумя частями (разделениями), имеющими шумоподобную структуру, и обе требуются для успешного расшифрования. При использовании данной технологии шифрования уменьшается контраст (разность между числом черных субпикселов белого и черного пикселов расшифрованного изображения) и увеличивается размер восстановленного секретного изображения по сравнению с исходным секретным изображением в горизонтальном направлении.

Целью данной работы является разработка алгоритма маркирования изображения на основе технологии визуальной криптографии ВСРС (2, 2), который не искажает защищаемые данные и не оставляет следов встраивания, но при этом обеспечивает высокую точность распознавания авторского ДММ и надежно защищает передаваемую визуальную информацию от присваивания и дальнейшего незаконного использования третьими лицами.

Алгоритм защиты изображений от несанкционированного использования состоит из процедуры защифрования ДММ, осуществляемой перед распространением информации в сети, и процедуры восстановления ДММ, необходимой для обнаружения незаконного использования предоставляемой информации.

Процедура зашифрования ДММ I_F на основе двух изображений-соответствий E_1 и E_2

Данная процедура состоит из следующих шагов.

Шаг 1. Инициализация начальных параметров.

1.1. Исходное защищаемое изображение I_C размером $M \times N$.

Защищаемое изображение $I_C = \left(I_C(m,n) \middle| m = \overline{1,M}, n = \overline{1,N} \right)$ может быть цветным или полутоновым.

1.2. Генерация уникальной ДММ I_F размером $P \times Q$

Уникальная двоичная маска маркирования

$I_F = \left(I_F(m,n) \middle| m = \overline{1,P}, n = \overline{1,Q}, I_F(m,n) \in \{0,1\} \right)$ может быть использована в качестве авторского ЦВЗ или ЦФ. Размеры ДММ должны быть меньше или равны размерам защищаемого изображения: $P \times Q \le M \times N$.

Синтезированная пространственная фрактальная структура I_F^N с парой псевдослучайных углов θ_1 и θ_2 на N-м уровне итерации определяется с помощью соотношения

$$I_F^N = \left(I_F^N(m,n,\theta_1,\theta_2) \right)_{P \times Q}, \qquad (1)$$

где $I_F^N(m,n,\theta_1,\theta_2) = \left(I_{Fj}^N(m,n,\theta_1,\theta_2) = S_j^N\left(G^N(m,n,\theta_1,\theta_2), I_j^{N-1}(m,n) \right) \middle| j = \overline{1,J_N} \right)$ – значение пиксела фрактальной структуры на N-м уровне итерации; $S_j^N(\cdot)$ – оператор замещения j-го элемента инициатора $I_j^{N-1}(m,n)$ генератором $G^N(m,\theta_1,\theta_2)$ для синтеза элементов $I_{Fj}^N(m,n,\theta_1,\theta_2)$ фрактальной структуры на N-м уровне итерации; $G^1 = \left(G^1(m,\theta_1,\theta_2) \right)$ – исходный генератор, состоящий из определенного числа линейных элементов, образующих различные формы импульсов и характеризующихся парой секретных псевдослучайных углов θ_1 и θ_2 углов наклона крайних элементов; $I^1 = \left\{ I_j^1(m,n) \middle| j = \overline{1,J_1} \right\}$ – исходный инициатор, представляющий собой простую

геометрическую фигуру (треугольник, квадрат, многоугольник) и состоящий из J_1 элементов длиной L_1; J_N – число элементов инициатора на N-м уровне итерации.

Оценка фрактальной размерности или размерности самоподобия D фрактальных структур осуществляется с помощью соотношения:

$$D = \log m / \log \mu, \qquad (2)$$

где m – число линейных элементов, из которых состоит генератор G^1 фрактальной структуры I_F^N; l_1 – размер линейного элемента генератора; L_1 – расстояние между начальной и конечной точками генератора или размер генератора; $\mu = L_1/l_1$ – параметр формы генератора.

Из (1) и (2) следует, что синтез концентрических фрактальных структур с одинаковой длиной $l = l_{N_1}^1 = l_{N_2}^2 = ... = l_{N_{N_E}}^{N_E}$ элементов генератора и числом вложений N_E осуществляется с помощью выбора числа итераций $N \in \{N_1,...,N_{N_E}\}$ для каждого вложения и скейлинговых соотношений между размерами элементов исходных инициаторов $L \in \{L_{1,1},...,L_{1,N_E}\}$.

Таким образом, фрактальная пространственная структура I_F^N характеризуется ключевыми параметрами генератора G_1 (θ_1, θ_2, m, $\mu = L_1/l_1$, D), инициатора $I^1\left(J_1, L_1 \in \{L_{1,1},...,L_{1,N_E}\}\right)$, числом вложений N_E и количеством итераций на каждом вложении $N \in \{N_1,...,N_{N_E}\}$.

1.3. Формирование псевдослучайной последовательности целых чисел Z из интервала $[0, MN]$ с помощью секретного ключа K_S.

Множество псевдослучайных целых чисел $Z = (Z_1,...,Z_k,...,Z_{PQ})$, где $k \in [1, PQ]$ – номер позиции пикселя изображения I_C, представляет собой множество псевдослучайных позиций пикселов I_C, используемых для зашифрования ДММ.

Шаг 2. Формирование одномерной последовательности пар пикселов бинарного изображения-соответствия E_2.

2.1. Выборка значения пиксела $I_C(k)$ одномерной последовательности изображения I_C с k-й позицией и l-го бита его кодового слова.

Одномерная последовательность $I_C = (I(1),...,I(k),...,I(MN))$ из изображения размером $M \times N$ формируется с помощью одного из способов его развертки (горизонтальная, вертикальная и другие). Псевдослучайная выборка значений пикселов из одномерной последовательности значений изображения I_C осуществляется с помощью множества псевдослучайных целых чисел $Z = (Z_1,...,Z_k,...,Z_{PQ})$ для формирования псевдослучайной последовательности значений пикселов $I_C = \{I_C(k) | k = \overline{1, PQ}\}$. Для повышения крипостойкости шифрования одномерной последовательности изображения I_C дополнительно используется поточный алгоритм шифрования RC4 с размером секретного ключа, равным 1700 бит.

Значение пикселя $I_C(k)$ можно представить в двоичной форме с помощью соотношения

$$I_C(k) = \sum_{l=0}^{L-1} b_l(k) 2^l, \qquad (3)$$

где L – длина кодового слова $b = b_{L-1}...b_l...b_0$ значения пиксела $I_C(k)$; $b_l(k) \in \{0,1\}$ – значение l-го бита кодового слова значения пиксела $I_C(k)$.

Выбор *l*-го бита $b_l(k) \in \{0,1\}$ из кодового слова *k*-го пикселя $I_C(k)$ обусловлен требованиями устойчивости выбранных бинарных изображений, используемых для зашифрования ДММ, к различного рода воздействиям на качество защищаемого изображения: сжатие, фильтрация, шумы канала и т.п. Для определения количества битовых плоскостей, из которого осуществляется выбор визуально значимой битовой плоскости, и количественной оценки психовизуальной значимости битовых плоскостей целесообразно использовать объективные перцептуальные критерии качества изображения [7]. Обычно это наиболее визуально значимые биты: $l \in \{7,6,5,4\}$ при $L = 8$ бит. Выбор трех определенных бинарных изображений дает возможность формирования устойчивого, полухрупкого и хрупкого ДММ за счет выбора, например, соответственно 6, 4 и 0 битовых плоскостей исходного изображения.

2.2. Формирование пикселов бинарного изображения-соответствия E_1 изображению I_C.

В соответствии с правилом формирования изображения-соответствия E_1 (см. табл. 1) значению $b_l(k)$ пиксела $I_C(k)$ изображения I_C должна соответствовать пара пикселов изображения-соответствия E_1, определенная посредством выбора пары строк: одна строка для нулевого бита и вторая строка для единичного бита. Например, $b_l(k) \to \{01,10\}$.

Таблица 1. **Правило формирования бинарного изображения-соответствия E_1 изображению I_C**

Значение бита $b_l(k)$ пиксела $I_C(k)$ изображения I_C	Значение пиксела $E_1(k)$ изображения-соответствия E_1
0	10
0	01
1	10
1	01

Конечным результатом данного шага является значение пиксела $E_1(k)$, определенное с помощью выбранного правила формирования бинарного изображения-соответствия E_1 для $b_l(k)$: $E_1(k) \to \{01,10\}$. Это приводит к увеличению размера изображения-соответствия E_1, равного $2P \times Q$, по сравнению с размером $P \times Q$ изображения I_C.

2.3. Формирование пикселов бинарного изображения-соответствия E_2 ДММ.

Таблица 2. **Правило формирования бинарного изображения-соответствия E_2 ДММ**

Значение пиксела изображения-соответствия E_1	Значение пиксела изображения-соответствия E_2	Значение пиксела $\tilde{I}_F(k)$ при наложении пикселов изображений-соответствий E_1 и E_2
10	10	10
01	01	01
10	01	11
01	10	11

С помощью пары пикселов изображения-соответствия E_1 и правила формирования бинарного изображения-соответствия E_2 ДММ (см. табл. 2) определяется такая пара пикселов изображения-соответствия E_2, которая позволяет вычислить *k*-ю пару пикселов бинарного изображения ДММ: $E_1(k) \vee E_2(k) = \tilde{I}_F(k)$, где $\vee$ – символ логической операции ИЛИ. Например, $E_1(k) \to \{01,10\}$ и $\tilde{I}_F(k) \to \{01,11\}$ соответствует $E_2(k) \to \{01,01\}$.

2.4. Проверка условия окончания формирования одномерной последовательности изображения-соответствия E_2.

Если $k < P \times Q$, то переход к шагу 2.1. В противном случае – к шагу 3.

Конечным результатом данного шага является одномерная последовательность $E_2 = \left(E_2(k) \middle| k = 1,2P \times Q\right)$ пар пикселов изображения-соответствия E_2.

Шаг 3. Формирование бинарного изображения-соответствия E_2 ДММ.

Из одномерной последовательности $E_2 = \left(E_2(k) \middle| k = 1,2P \times Q\right)$ пар пикселов изображения-соответствия E_2 с помощью строчной развертки формируется изображение-соответствие E_2: $E_2 = \left(E_2(m,n) \middle| m = \overline{1,2P}, n = \overline{1,Q}\right)$.

Процедура восстановления ДММ $\tilde{I}_F^N$ на основе исходного изображения I_C и изображения-соответствия E_2

Данная процедура требует официальной регистрации ДММ в виде авторского ЦВЗ или ЦФ. Кроме того, она требует знания правила формирования изображений-соответствий E_1 и E_2, секретного ключа K_S и она состоит из следующих шагов.

Шаг 1. Инициализация начальных параметров.

1.1. Исходное защищенное (маркированное) изображение $I_C = \left(I_C(m,n) \middle| m = \overline{1,M}, n = \overline{1,N}\right)$.

1.2. Уникальная ДММ $I_F^N = \left(I_F^N(m,n) \middle| m = \overline{1,P}, n = \overline{1,Q}, I_F^N(m,n) \in \{0,1\}\right)$.

1.3 Секретный ключ K_S для генерации псевдослучайной последовательности целых чисел, принадлежащих интервалу $[0, MN]$: $Z = \left(Z_1, ..., Z_k, ..., Z_{PQ}\right)$ при $P \times Q \le M \times N$, и секретный ключ алгоритма RC4.

1.4 Изображение-соответствие $E_2 = \left(E_2(m,n) \middle| m = \overline{1,2P}, n = \overline{1,Q}\right)$, формируемое при внедрении ДММ I_F^N.

Шаг 2. Формирование бинарного изображения-соответствия E_1.

2.1. Выборка значения пиксела $I_C(k)$ из одномерной псевдослучайной последовательности изображения I_C с k-й позицией и определение l-го бита $b_l(k) \in \{0,1\}$ кодового слова $I_C(k)$.

2.2. Формирование одномерной последовательности пар пикселов изображения-соответствия E_1.

Одномерная последовательность пар пикселей изображения-соответствия E_1 имеет вид: $E_1 = \left(E_1(k) \middle| k = \overline{1,2P \times Q}\right)$.

Конечным результатом шага 2 является изображение-соответствие E_1, формируемое с помощью развертки определенного типа из одномерной последовательности пар пикселов данного изображения-соответствия: $E_1 = \left(E_1(m,n) \middle| m = \overline{1,2P}, n = \overline{1,Q}\right)$.

3. Восстановление уникального ДММ для установления подлинности авторства.

Уникальный ДММ восстанавливается посредством сложения бинарных изображений E_1 и E_2 по правилу дизъюнкции:

$$\tilde{I}_F^N = E_1 \vee E_2 = \left(I_F(m,n) = E_1(m,n) \vee E_2(m,n) \middle| m = \overline{1,2P}, n = \overline{1,Q}\right). \quad (4)$$

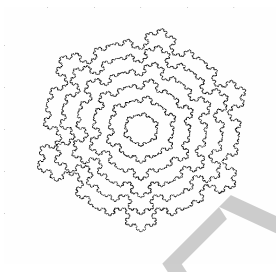
Из (4) видно, что восстановление ДММ возможно с помощью наложения двух диапозитивов, на которых зарегистрированы бинарные изображения E_1 и E_2, без использования вы-

числительных средств. Восстановленный ДММ имеет по сравнению с исходным ДММ увеличенные размеры $2P \times Q$.

Результаты моделирования

Для оценки эффективности предложенного алгоритма используется спутниковое изображение размером 512×512 и ДММ в виде фрактальной структуры с уникальными параметрами (рис. 1). Уровень защищенности исходного изображения зависит от выбора размера секретных ключей, бинарных изображений с требуемой визуальной значимостью и количества структурных параметров уникального ДММ.

а



б

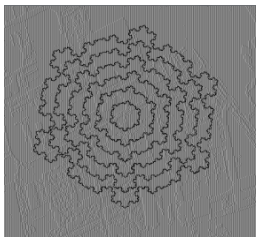
Рис. 1. Исходные защищаемое полутоновое изображение и уникальная двоичная маркирующая маска: *а* – спутниковое изображение; *б* – фрактальная структура с секретными параметрами

На рис. 1,*б* приведена концентрическая двухмерная структура, состоящая из шести вложенных структур с одинаковым числом итераций (N=6), разными диаметрами инициатора, находящимися в линейном отношении $L_1 : L_2 : L_3 : L_4 : L_5 : L_6$=1 : 2 : 3: 4 : 5: 6. В качестве генератора и инициатора используются соответственно треугольная линейная форма и шестиугольник, $\theta_1 = \theta_2 = 6{,}39368$. Фрактальная размерность данной структуры составляет d = 1,2618 при μ=3.

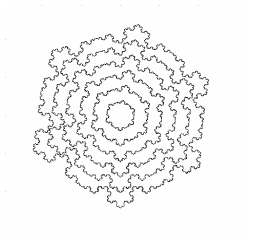
Реализация процедур зашифрования ДММ и его восстановления происходит без потерь качества защищаемого изображения. Восстановление ДММ $\tilde{I}_F^N$ может осуществляться посредством наложения изображений-соответствий E_2 и E_1 (рис .2).

а

б



в



г

Рис. 2. Восстановление ДММ посредством наложения бинарных шумоподобных изображений: *а* – изображение-соответствие E_2; *б* – изображение-соответствие E_1; *в* – восстановленная ДММ; *г* – восстановленная ДММ после пороговой обработки

Из рис. 2 видно, что любое из изображений-соответствий не несет никакой информации, но вместе они восстанавливают ДММ с уменьшенным контрастом и увеличенным размером. Это обусловлено тем, что когда два расширенных бинарных изображений-соответствий совмещаются вместе, черные пиксели на формируемом бинарном изображении ДММ остаются такими же, а белые становятся серыми. Несмотря на то, что контраст ДММ становится меньше, расшифрованное изображение ДММ достоверно распознается. После пороговой обработки восстановленный ДММ не отличается от исходного ДММ. Данный алгоритм позволяет формировать устойчивый, полухрупкий и хрупкий ДММ за счет выбора соответствующих битовых плоскостей защищаемого изображения с целью обеспечения различной чувствительности ДММ к возможным воздействиям на исходное защищаемое изображение для контроля его подлинности.

Заключение

Предложен алгоритм защиты изображений от копирования и незаконного распространения информации, основанный на представлении защищаемого изображения в виде набора взвешенных битовых плоскостей, ДММ в виде двух бинарных шумоподобных изображений-соответствий и восстановление ДММ пользователя посредством наложения двух диапозитивов сформированных изображений-соответствий. Он обеспечивает высокий уровень защищенности контента изображений без изменения их качества за счет возможности использования секретных ключей шифрования большой длины (1700 бит и более), восьми параметров генерации фрактальной ДММ, различных правил формирования изображений-соответствий с учетом визуальной информации о ДММ и контенте защищаемого изображения и требует официальной регистрации ДММ пользователя.

Представлены результаты моделирования разработанного алгоритма в среде программирования C#.

AN ALGORITHM OF MARKING IMAGES BASED ON THE VISUAL CRYPTOGRAPHY FOR PROTECTING FROM UNCONFIDENTIALITY INFORMATION DISTRIBUTION

A.A. BORISKEVICH

Abstract

An algorithm of marking image protecting from copying and illegal distribution of information based on the visual cryptography principles, representing an original image in form of the weighted binary plane set and binary marking mask in form of two shadow image is proposed. The modeling result have shown that the algorithm provides the high protection level of the images without changing of the image quality and qualitative reconstruction of the binary marking mask without the computational tools.

Список литературы

1. *Milano D.* Content control: Digital watermarking and fingerprinting [Electronic resource]. Mode of access: www.rhozet.com/whitepapers/Fingerprinting_Watermarking.pdf.
2. *Noar M., Shamir A.* // Advances in Cryptology: Eurocrypt'94. 1995. Vol. 950. P. 1-12.
3. *Ateniese G., Blundo C., De Santis A. et al.* // Inf. Comput. 1996. Vol. 129, №2. P. 86-106.
4. *Hwang, R.J.* // Tamkang Journal of Science and Engineering. 2000. Vol. 3, №2. P. 97-106.
5. *Surekha B., Swamy G.N., Srinivasa R.K. et al.* // Journal of Information Assurance and Security. 2009. №4. P. 470-473.
6. *Pal J.K., Mandal K., Dasgupta K.* // International Journal of Network Security & Its Applications. 2010. Vol. 2, №4. P. 118-127.
7. *Борискевич А.А., Руис Л.А.* // Сборник научных статей 6-я Международной научно-технической конференции Медэлектроника-2010. С. 34-37.