УДК 681.322

С.В. Беззатеев, Н.В. Волошина, К.А. Жиданов

Система формирования фингерпринта статических изображений с использованием взвешенной метрики Хэмминга и модели взвешенного контейнера

Рассматривается алгоритм вычисления фингерпринта для статических изображений с учетом значимости различных областей (компонент, элементов) изображения с точки зрения влияния вносимых в них искажений на восприятие полученного в результате изображения – модели взвешенного контейнера. Алгоритм использует в качестве базового компонента помехоустойчивые коды, совершенные во взвешенной метрике Хэмминга.

Ключевые слова: фингерпринтинг, цифровой водяной знак, модель взвешенного контейнера, коды во взвешенной метрике Хэмминга, совершенные коды, защита авторских прав.

При распространении цифровых мультимедиа данных особо актуальной является задача защиты авторских прав на такую информацию (DRM – digital right management). Для решения этой задачи используют методы цифровых водяных знаков (DWM – digital watermarking) и цифровых фингерпринтов (DFP – digital fingerprinting) [1–5]. В первом случае для защиты в исходные мультимедиа-данные, например изображение, внедряется информация о владельце. Эта информация должна сохраняться при различных искажениях помеченного изображения, пока уровень его качества не упадет ниже некоторого порога. Второй подход подразумевает формирование некоторой дополнительной информации (фингерпринт) на базе исходного изображения с использованием специфических свойств изображения (например, опорных точек). Объем фингерпринта значительно меньше исходного изображения. Полученный фингерпринт используется для поиска копий изображений, незаконно распространяемых в сети. Метод построения фингерпринта должен обеспечивать его воспроизведение при различных искажениях исходного изображения до тех пор, пока они не достигнут определенного уровня.

Существенным различием этих методов является следующее.

При встраивании DWM часть мультимедиаданных меняется (например, метод LSB подразумевает изменения младших битов). А при построении DFP никаких изменений в исходный контейнер не вносится, а записывается только дополнительная информация об особенных свойствах изображения.

Встраиваемая при DWM-метка формируется пользователем и может иметь различный вид, по существу представляя собой некую информацию владельца. DFP получают на основе исходного изображения. Никаких пользовательских данных он не содержит.

В работе предлагается DRM метод, использующий оба подхода с использованием кодовых методов и модели взвешенного контейнера, позволяющий подготовить структуру исходного изображения (других мультимедийных данных) к дальнейшему формированию устойчивого цифрового фингерпринта, при условии внесения минимальных искажений в исходные данные.

Описание предлагаемого метода. Основными задачами любой системы DRM является построение такого метода получения (добавления) данных об авторе, который будет устойчивым к различного рода искажениям до определенного их уровня (например, сильные визуально заметные искажения), внося минимальные искажения либо совсем не внося их в исходные данные.

Метод DFP не вносит искажений. Он базируется на выделении специальных свойств (характеристик) исходных данных с дальнейшей их фиксацией. Проблема метода заключается в том, что для некоторого класса данных такие свойства, обладающие устойчивостью к искажениям, трудно найти. В то же время требование абсолютного отсутствия искажений для этих данных не является актуальным (например, фотореалистические изображения).

Для таких данных можно использовать методы DWM. В этом случае информация об авторе (метка) внедряется в исходные данные (например, в изображение), внося при этом некоторые иска-

жения. Однако из-за несогласованности метки и структуры изображения не всегда удается произвести внедрение с приемлемым уровнем искажений.

В статье предлагается метод построения DFP по свойству наличия в изображении кодовых слов (концепция F5 [3]), а при их отсутствии – создания этого свойства, т.е. внесения искажений методом DWM [1, 4, 5]. Рассмотрим суть метода на примере статических изображений. Исходное изображение или его часть преобразуется в битовый поток. Этот поток разделяется на блоки a длиной n. Эти блоки рассматриваются как кодовые слова c некоего кода C, искаженные вектором ошибок **e**. Если блок a является кодовым словом c кода C, то $e=0$ и синдром $s=0$, т.е. данный блок обладает требуемым свойством. Если $s \neq 0$, то блок не обладает требуемым свойством и для его создания необходимо исправить ошибки, т.е. произвести декодирование $a \Rightarrow c$. Если использовать совершенные коды, то задача получения $s=0$ для любого блока решается при внесении минимального числа ошибок [2], а следовательно, и искажений. Для минимизации вносимых искажений будем использовать несколько кодов, имеющих одинаковые параметры и построенных во взвешенной метрике Хэмминга. При таком подходе фингерпринтом будем считать полученную в результате декодирования последовательность кодов ($\lambda_1, \lambda_2, \ldots \lambda_i, \ldots$), кодовые слова $c_j \in C_i = \Gamma(L_{\lambda_i}, G_{\lambda_i})$ которых являются наиболее близкими к построенным по исходному изображению блокам a_j; $\Gamma(L_{\lambda_i}, G_{\lambda_i})$ – соответствующим образом выбранный код Гоппы во взвешенной метрике Хэмминга [6].

Следует отметить, что поскольку при таком подходе используются коды, исправляющие ошибки, согласованные с взвешенной метрикой Хэмминга, то и формируемые из битового потока блоки должны иметь взвешенную структуру. Подобная задача решается при построении взвешенного контейнера при реализации метода WDWM (взвешенного цифрового водяного знака) [1]. Для построения взвешенных блоков необходимо предварительно разделить исходные данные (например, изображение) на несколько зон. Деление производится исходя из степени влияния искажений, происходящих в зоне, на результирующее качество (например, воспринимаемое качество изображения, значение PSNR и т.д.). Таким образом, блоки a формируются посредством комбинирования частей из различных зон, найденных в процессе построения взвешенного контейнера.

Обобщенна схема метода построения взвешенного фингерпринта приведена на рис. 1.

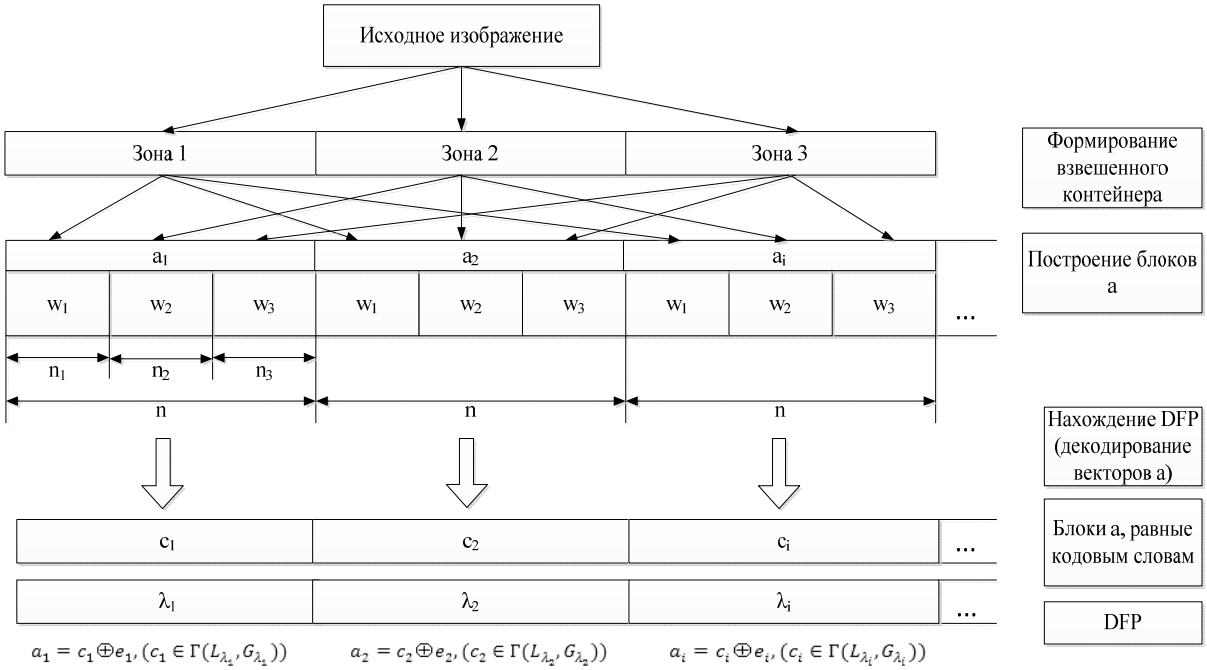

Рис. 1. Обобщенная схема построения взвешенного фингерпринта для контейнера с тремя зонами значимости

Коды во взвешенной метрике Хэмминга. Совершенные коды. Помехоустойчивые коды во взвешенной метрике Хэмминга [6] определяются следующим образом:

Длина кодового слова n задается набором длин $n_1, n_2, ..., n_l, n = \sum_{i=1}^{l} n_i$. Каждая позиция кодового слова $a = (a_1^1 a_2^1 \ldots a_{n_1}^1 \; a_1^2 \ldots a_{n_2}^2 \ldots a_1^l \ldots a_{n_l}^l)$ имеет свой вес ω_j. Будем считать, что эти веса упорядочены по возрастанию, т.е. $\omega_1 < \omega_2 < \ldots \omega_j < \ldots < \omega_l$. Вес слова a во взвешенной метрике Хэмминга определяется следующим образом:

$$wt_{WHM}(a) = \sum_{a_i^j \neq 0} \omega_j .$$

Очевидно, аналогичным образом определяется расстояние Хэмминга во взвешенной метрике Хэмминга между двумя векторами $\mathbf{a} = (a_1^1 a_2^1 \ldots a_{n_1}^1 \; a_2^1 \ldots a_{n_2}^2 \ldots a_l^1 \ldots a_{n_l}^1)$ и $\mathbf{b} = (b_1^1 b_2^1 \ldots b_{n_1}^1 \; b_2^1 \ldots b_{n_2}^2 \ldots b_l^1 \ldots b_{n_l}^1)$:

$$d_{WHM}(\mathbf{a}, \mathbf{b}) = \sum_{a_i^j \neq b_i^j} \omega_j .$$

Для двоичных кодов во взвешенной метрике Хэмминга, как и для кодов в обычной метрике, можно выписать границу Хэмминга, связывающую параметры кода n, M, d_{WHM}:

$$M \cdot W_n^{\tau} \leq 2^n,$$

где M – количество кодовых слов в коде (для двоичного линейного кода $M = 2^k$); W_n^{τ} – число векторов длины n в шаре радиуса τ во взвешенной метрике Хэмминга.

$$W_n^{\tau} = \sum_{\sum_{j=1}^{l} \tau_j \omega_j \leq \tau} \prod_{i=1}^{l} \binom{n_i}{\tau_i},$$

где $\tau = \dfrac{d_{WHM} - 1}{2}$.

Соответственно можно определить совершенный код, т.е. код, параметры которого лежат на этой границе. Для линейного двоичного кода это соотношение будет выглядеть следующим образом:

$$2^{n-k} = \sum_{\sum_{j=1}^{l} \tau_j \omega_j \leq \tau} \prod_{i=1}^{l} \binom{n_i}{\tau_i}.$$

Совершенные коды во взвешенной метрике Хэмминга могут быть построены с использованием хорошо известных методов построения оптимальных кодов (например, граница Варшамова-Гилберта). Однако такой метод построения является вычислительно трудоемким и главное не дает конструктивного метода декодирования построенных таким образом кодов. Использование специальных классов кодов Гоппы во взвешенной метрике Хэмминга позволяет решить обе эти задачи.

Специальный класс кодов Гоппы для взвешенной метрики Хэммига. Для построения кодов Гоппы, согласованных с взвешенной метрикой Хэмминга, используется конструкция обобщенных (L,G) кодов с нумераторами позиций различных степеней [6]. То есть $L = \left\{ \dfrac{v_i^j(x)}{u_i^j(x)} \right\}_{j=1,l;i=1,n_j}$, $v_i^j(x)$ – формальная производная соответствующего знаменателя $u_i^j(x)$, $\deg u_i^j(x) = \omega_j$ и $u_i^j(x)$ – многочлен, не приводимый над $F_{2^m}[x]$. Многочлен Гоппы для такого кода задается неприводимым многочленом

$$G(x), G(x) \in F_{2^m}[x], \deg G(x) = \tau \geq \omega_l, (G(x), u_i^l(x)) = 1, \forall i : i = 1, n_l .$$

Число различных кодов Гоппы из этого класса с одинаковыми параметрами (n, k, d_{WHM}) определяется числом различных неприводимых многочленов степени τ над $F_{2^m}[x]$.

Алгоритм вычисления фингерпринта на базе семейства кодов Гоппы, совершенных во взвешенной метрике Хэмминга $\Gamma_{WHM}(n,k,d)$. Опишем здесь простейший вариант алгоритма

вычисления фингерпринта для статических изображений, использующий различные по значимости области изображения и семейство кодов Гоппы, совершенных во взвешенной метрике Хэмминга.

Без потери общности будем рассматривать здесь статическое изображение, в котором определены три зоны значимости:

- Третья зона не предполагает внесения каких-либо искажений, т.е. $\omega_3 = \infty$.
- Вторая зона имеет относительный вес ω_2 вносимых искажений, равный 2.
- Первая зона позволяет вносить максимальное число искажений без существенных последствий для качества результирующего изображения и соответственно имеет минимальный относительный вес $\omega_1 = 1$.

Для такого изображения выберем семейство кодов Гоппы, совершенных во взвешенной метрике Хэмминга $\Gamma_{WHM}(n,k,d)$, со следующими параметрами:

$$n = n_1 + n_2 = 2^{2m-1} + 2^{m-1} - 1, n_1 = 2^m, n_2 = 2^{2m-1} - 2^{m-1} - 1, k = 2^{2m-1} + 2^{m-1} - 2m, d_{WHM} = 5.$$

Как указывалось в предыдущем разделе, число различных кодов в этом семействе определяется количеством неприводимых многочленов второй степени с коэффициентами из $GF(2^m)$:

$$I_{GF(2^m)}(2) = 2^{2m-1} - 2^{m-1}.$$

Очевидно, что, так как рассматриваемые коды совершенные, то любой вектор $\mathbf{a} = (a_1^1\, a_2^1 \ldots a_{n_1}^1\, a_1^2 \ldots a_{n_2}^2)$, полученный из изображения при разбиении его на зоны, может быть представлен во взвешенной метрике Хэмминга следующим образом:

$$(a_1^1\, a_2^1 \ldots a_{n_1}^1\, a_1^2 \ldots a_{n_2}^2) = (c_1^1\, c_2^1 \ldots c_{n_1}^1\, c_1^2 \ldots c_{n_2}^2)_i \oplus (e_1^1\, e_2^1 \ldots e_{n_1}^1\, e_1^2 \ldots e_{n_2}^2)_i,$$

где $(c_1^1\, c_2^1 \ldots c_{n_1}^1\, c_1^2 \ldots c_{n_2}^2)_i \in \Gamma(L_i, G_i), wt_{WHM}(e_1^1\, e_2^1 \ldots e_{n_1}^1\, e_1^2 \ldots e_{n_2}^2)_i = t_i \le 2$.

Таким образом, используя при декодировании вектора **a** различные $\Gamma(L_i, G_i)$ коды семейства $\Gamma_{WHM}(n,k,d)$, мы будем получать векторы ошибки с различными весами $0 \le t_i \le 2$.

Фингепринтом будем считать набор номеров $\lambda_1, \lambda_2, \ldots, \lambda_R$ кодов из семейства, соответствующих векторам, полученным из изображения при разбиении его на зоны следующим образом.

Вектору $\mathbf{a} = (a_1^1\, a_2^1 \ldots a_{n_1}^1\, a_1^2 \ldots a_{n_2}^2)$ поставим в соответствие наименьший номер λ такого $\Gamma(L_i, G_i)$ кода, для которого полученный при декодировании вектор ошибки $\mathbf{e} = (e_1^1\, e_2^1 \ldots e_{n_1}^1\, e_1^2 \ldots e_{n_2}^2)_i$ оказался наименьшего веса.

То есть $\lambda = \min_i i : wt_{WHM}(e_1^1\, e_2^1 \ldots e_{n_1}^1\, e_1^2 \ldots e_{n_2}^2)_i = \min_j wt_{WHM}(e_1^1\, e_2^1 \ldots e_{n_1}^1\, e_1^2 \ldots e_{n_2}^2)_j$.

Тогда алгоритм вычисления фингерпринта на базе семейства кодов $\Gamma(L_i, G_i)$ описывается следующим образом:

1. Изображение разбивается на зоны различной значимости.
2. В соответствии с разбиением изображения формируются блоки и выбираются подходящие параметры семейства кодов.
3. Фингерпринт $\lambda_1, \lambda_2, \ldots, \lambda_M$ формируется следующим образом:

Найденные векторы ошибок $\mathbf{e} = (e_1^1\, e_2^1 \ldots e_{n_1}^1\, e_1^2 \ldots e_{n_2}^2)_i$ исправляются, и соответственно блоки $\mathbf{a} = (a_1^1\, a_2^1 \ldots a_{n_1}^1\, a_1^2 \ldots a_{n_2}^2)$ исходного изображения преобразуются в кодовые слова кодов Гоппы из семейства $\Gamma_{WHM}(n,k,d)$. Например, первый блок превращается в кодовое слово $(c_1^1\, c_2^1 \ldots c_{n_1}^1\, c_1^2 \ldots c_{n_2}^2) \in \Gamma(L_{\lambda_1}, G_{\lambda_1})$. Согласно описанному ранее алгоритму получения номеров λ_i, искажения, вносимые при этом в исходное изображение, будут минимальны.

Проверка фингерпринта и его устойчивость к случайным и преднамеренным искажениям изображения. В соответствии с описанным алгоритмом создания фингерпринта $\lambda_1, \lambda_2, \ldots, \lambda_R$ в обработанном в результате получения фингерпринта изображении P имеется R блоков

$(c_1^1 c_2^1 \ldots c_{n_1}^1 c_1^2 \ldots c_{n_2}^2)_i \in \Gamma(L_{\lambda_i}, G_{\lambda_i}), i = 1, \ldots, R$. То есть каждый такой блок является кодовым словом соответствующего кода Гоппы из семейства $\Gamma_{WHM}(n,k,d)$. При проверке фингерпринта $\lambda_1, \lambda_2, \ldots, \lambda_R$ для изображения осуществляется декодирование блоков a с использованием $\Gamma(L_{\lambda_i}, G_{\lambda_i})$ кодов, соответствующих фингерпринту, и если для любого блока синдром $s = 0$, то фингерпринт считается соответствующим заданному, а изображение – равным P.

Наличие несущественных искажений изображения P может приводить к появлению ошибок в этих блоках. То есть будем считать, что в искаженном изображении P^* имеются блоки

$$(b_1^1 b_2^1 \ldots b_{n_1}^1 b_1^2 \ldots b_{n_2}^2)_i = (c_1^1 c_2^1 \ldots c_{n_1}^1 c_1^2 \ldots c_{n_2}^2)_i \oplus (e_1^1 e_2^1 \ldots e_{n_1}^1 e_1^2 \ldots e_{n_2}^2)_i = (\hat{c}_1^1 \hat{c}_2^1 \ldots \hat{c}_{n_1}^1 \hat{c}_1^2 \ldots \hat{c}_{n_2}^2)_i \oplus (\hat{e}_1^1 \hat{e}_2^1 \ldots \hat{e}_{n_1}^1 \hat{e}_1^2 \ldots \hat{e}_{n_2}^2)_i,$$

$$wt_{WHM}(\hat{e}_1^1 \hat{e}_2^1 \ldots \hat{e}_{n_1}^1 \hat{e}_1^2 \ldots \hat{e}_{n_2}^2)_i = wt_i \le 2,$$

$$(c_1^1 c_2^1 \ldots c_{n_1}^1 c_1^2 \ldots c_{n_2}^2)_i, (\hat{c}_1^1 \hat{c}_2^1 \ldots \hat{c}_{n_1}^1 \hat{c}_1^2 \ldots \hat{c}_{n_2}^2)_i \in \Gamma(L_{\lambda_i}, G_{\lambda_i}), i = 1, \ldots, R.$$

Используя фингерпринт $\lambda_1, \lambda_2, \ldots, \lambda_R$ и искаженное изображение P^*, легко найти соответствующий вектор ошибки $(\hat{e}_1^1 \hat{e}_2^1 \ldots \hat{e}_{n_1}^1 \hat{e}_1^2 \ldots \hat{e}_{n_2}^2)_i$ и соответствующий ему вес wt_i. Очевидно, что при небольших искажениях $(c_1^1 c_2^1 \ldots c_{n_1}^1 c_1^2 \ldots c_{n_2}^2)_i = (\hat{c}_1^1 \hat{c}_2^1 \ldots \hat{c}_{n_1}^1 \hat{c}_1^2 \ldots \hat{c}_{n_2}^2)_i$ и соответственно $(e_1^1 e_2^1 \ldots e_{n_1}^1 e_1^2 \ldots e_{n_2}^2)_i = (\hat{e}_1^1 \hat{e}_2^1 \ldots \hat{e}_{n_1}^1 \hat{e}_1^2 \ldots \hat{e}_{n_2}^2)_i$.

Определим теперь штрафную функцию $F = \sum_{i=1}^{R} wt_i \cdot f_{wt_i}$. В простейшем случае можно считать весовые коэффициенты $f_{wt_i} \in \{f_1, f_2\}$ штрафной функции одинаковыми и равными 1. Однако возможен и более гибкий вариант $f_1 \ne f_2$, учитывающий природу искажений и их влияние на восприятие результирующего изображения, т.е. его качество.

Принятие решения о наличии данного фингерпринта в имеющемся изображении P^* осуществляется по значению штрафной функции F и пороговым значениям B_1 и B_2, определяющим соответственно события «ложной тревоги» и «пропуска цели».

Заключение. Предложен новый метод вычисления фингерпринта, использующий особенности исходного контейнера, связанные с различной степенью его чувствительности к искажениям, вносимым в различных зонах контейнера. Для того чтобы воспользоваться таким свойством контейнера, предлагается применять для его описания взвешенную метрику Хэмминга в отличие от используемой в известных ранее схемах обычной метрики Хэмминга. Для эффективного использования такой метрики в работе предлагается брать семейство обобщенных кодов Гоппы, совершенных во взвешенной метрике Хэмминга. Благодаря использованию такого семейства кодов удается обеспечить внесение минимального числа искажений при создании фингерпринта. Кроме того, кодовые конструкции позволяют исправлять случайные искажения, возникающие при хранении или передаче контейнера. Открытым остается вопрос оптимального выбора коэффициентов в штрафной функции, обеспечивающих минимальные вероятности «ложной тревоги» и «пропуска цели» при принятии решения о наличии фингерпринта в анализируемом контейнере.

Работа выполнена при финансовой поддержке Минобрнауки РФ в рамках базовой части государственного задания СПбГУАП на 2014 год (проект № 2452).

Литература

1. Беззатеев С.В. Специальный класс кодов для стеганографических систем / С.В. Беззатеев, Н.В. Волошина, К.А. Жиданов // Доклады ТУСУРа. – 2012. – № 1 (25), ч. 2. – С. 112–118.

2. Neeta D. Implementation of LSB steganography and its evaluation for various bits / D. Neeta, K. Snehal, J. Daisy // Proc. of digital information management: 1st International conference. – India, 2006. – P. 173–178.

3. Westfeld A. F5–A steganographic algorithm high capacity despite better steganalysis / Information hiding. 4th International workshop. Lecture notes computer science. – 2001. – Vol. 2137. – P. 289–302.

4. Bezzateev S. Steganographic method on weighted container / S. Bezzateev, N. Voloshina, K. Zhidanov // Proc. of XIII Int. symposium on problems of redundancy in information and control system. – Saint-Petersburg, Russia, 2012. – P. 10– 12.

5. Anfinogenov S. Robust digital watermarking system for still images // S. Anfinogenov, V. Korshik, G. Morales-Luna // Proc. of Federated conference on computer science and information systems (FedCSIS). – Wrocław, Poland, 2012. – P. 85–689.

6. Беззатеев С.В. Двоичные обобщенные (L,G)-коды, совершенные во взвешенной метрике Хэмминга / С.В. Беззатеев, Н.А. Шехунова // Проблемы передачи информации. – 2012. – Т. 48, № 4. – С. 47–51.

Беззатеев Сергей Валентинович
Д-р техн. наук, зав. каф. технологий защиты информации
Санкт-Петербургского государственного университета аэрокосмического приборостроения (ГУАП)
Тел.: 8 (812) 494-70-52
Эл. почта: bsv@aanet.ru

Волошина Наталия Викторовна
Канд. техн. наук., доцент каф. технологий защиты информации ГУАП
Тел.: 8 (812) 494-70-52
Эл. почта: natali@vu.spb.ru

Жиданов Константин Александрович
Ассистент каф. технологий защиты информации ГУАП
Тел.: 8 (812) 494-70-52
Эл. почта: konstantin.zhidanov@gmail.com

Bezzateev S.V., Voloshina N.V., Zhidanov K.A.

The method of digital fingerprinting for static images based on weighted Hamming metric and on weighted container model

An algorithm of digital fingerprinting is proposed. The specific feature of this algorithm is that it takes into account different significance of different parts of the image according to their influence on the resulting image quality if any distortions have been occurred. The weighted container model is used for this purpose. This algorithm uses the ECC in weighted Hamming metric as a base approach.

Keywords: fingerprinting, digital watermarking, weighted container model, ECC in weighted Hamming metric, perfect codes, digital right management.