УДК 004.932

МЕТОД СОЗДАНИЯ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ НА ОСНОВЕ ДЕФОРМАЦИИ СИНТЕЗИРОВАННЫХ ИЗОБРАЖЕНИЙ С КВАЗИПЕРИОДИЧЕСКОЙ СТРУКТУРОЙ

А. А. Сирота, А. В. Швырева

Воронежский государственный университет

Поступила в редакцию 23.09.2017 г.

Аннотация. Описывается метод и реализующий его алгоритм создания цифровых водяных знаков для защиты электронных и бумажных документов, основанный на встраивании последовательности данных во фрагменты (блоки) синтезированных изображений с квазипериодической структурой путем внесения субпиксельных деформирующих искажений. Особенностью алгоритма является возможность внесения субпиксельных деформаций за счет представления исходного цифрового изображения в виде непрерывной функции пространственных координат. Для повышения скрытности встраиваемых цифровых водяных знаков на изображения дополнительно проводится наложение случайного шума. Извлечение цифрового водяного знака для выделения элементов ранее встроенной последовательности данных осуществляется с использованием нейросетевого классификатора фрагментов изображений. Приведены результаты экспериментальных исследований алгоритма.
Ключевые слова: стеганография, цифровые водяные знаки, деформирующие искажения, радиально-базисная функция, нейронная сеть.
Annotation. The method and its implementing algorithm for creating digital watermarks intended to protect electornic and paper documents are described. It is based on embedding data into the blocks of synthesized images with quasiperiodical structure by introducing subpixel deformation. A feature of this algorithm is the possibility of making sub-pixel deformation by representing image as a continuous function. In order to increase the safety of digital watermarks random noise can be added to the images. Extraction of digital watermark is performed with usage of neural network classifier of images. The results of experimental studies of the algorithm are presented.
Keywords: steganography, digital watermarks, deformation, radial basis function, neural network.

ВВЕДЕНИЕ

Для защиты бумажных или электронных документов в настоящее время используются различные методы и технологии, включая методы криптографической защиты и электронной цифровой подписи. Одним из перспективных методов защиты, отвечающим требованиям конфиденциальности и, в тоже время, минимальных временных и стоимостных затрат, является метод стеганографического скрытия информации (ССИ), который в приложении к задачам защиты документов реализует применение технологий цифровых водяных знаков (ЦВЗ), получивших своё название по аналогии с бумажными водяными знаками [1–4]. В основе этих технологий лежит внедрение в объект цифрового контента стеганографически скрытых и защищенных от модификации данных, которые тем или иным образом маркируют этот объект. В случае несанкционированного использования, распространения объекта или его подмены, а также фальсификации какой-либо его части наличие или отсутствие ЦВЗ позволяет идентифицировать возникающую ситуацию.

В настоящее время технологии ЦВЗ развиваются для защиты авторских прав на медиаданные и документы, представленные в электронном виде. ЦВЗ бывают различных типов. Прежде всего, различают невидимые и видимые ЦВЗ. Невидимые ЦВЗ встраива-

© Сирота А. А., Швырева А. В., 2017

ются таким образом, чтобы пользователь не догадывался о наличии данных, подтверждающих авторство или подлинность электронного объекта защиты. Защищаемые файлы, в данном случае, выступают в роли контейнера, хранящего ЦВЗ в скрытой форме, недоступной для стороннего наблюдателя. В качестве встраиваемых данных обычно выступает последовательность данных, содержащих кодируемую информацию ЦВЗ.

В качестве видимых ЦВЗ выступают логотипы и всевозможные маркировки, а также другая информация, идентифицирующая автора документа или подлинность. Такие ЦВЗ, имеют главный недостаток, который состоит в том, что их можно подделать или совсем удалить.

Целью данной работы является обоснование и исследования метода и реализующих его алгоритмов создания ЦВЗ для защиты электронных и бумажных документов, основанного на внедрении невидимых и защищенных цифровых меток в искусственно синтезируемые контейнеры – изображения квазипериодической структуры, являющиеся аналогом двумерного штрих-кода.

Таким образом, в данном случае фактически реализуется сочетание технологий невидимых и видимых ЦВЗ, поскольку сам факт их использования известен. При этом надо разделять возможности создания подобных ЦВЗ только для защиты электронных документов и возможности их использования для защиты создаваемых на основе электронных – бумажных документов. Последнее означает, что формируемые таким образом ЦВЗ должны быть устойчивы по отношению к цифро-аналоговым и аналого-цифровым преобразованиям, сопутствующим процессам распечатки и сканирования документа.

1. АНАЛИЗ ИЗВЕСТНЫХ ПУБЛИКАЦИЙ ПО РАССМАТРИВАЕМОЙ ТЕМАТИКЕ

Применение технологий ЦВЗ для защиты электронных и бумажных документов имеет свою специфику, связанную с формой представления текстовых данных. Основными требованиями, предъявляемыми к ЦВЗ, в этом плане являются возможность реализации технологий встраивания и извлечения ЦВЗ без использования специального оборудования (минимальные финансовые затраты), обеспечение необходимой емкости (пропускной способности) контейнера ЦВЗ, защищенность от подделки и уничтожения ЦВЗ, устойчивость к цифро-аналоговым и аналого-цифровым преобразованиям (для бумажных документов). В этом же плане в работе [6] представлен обобщенный алгоритм встраивания цифровых водяных знаков, который реализует математическую модель построения алгоритмов, устойчивых к цифро-аналоговым преобразованиям за счет учета параметров печатающего и сканирующего устройства (разрешающая способность). Модель позволяет определить такие основные параметры конкретной стегосистемы, как тип декодера, тип ключа, требования к ЦВЗ, требования к изображению-контейнеру.

Рассмотрим с точки зрения предъявляемых требований известные результаты в области создания невидимых и видимых ЦВЗ в интересах защиты электронных и бумажных документов.

Стандартными и достаточно тривиальными методами создания невидимых ЦВЗ в электронных текстовых документах являются методы, основанные на манипуляции при расстановке переносов, табуляций или пробелов в тексте, а также встраивание ЦВЗ в пустоты и управляющие элементы файлов, дисков и сетевых пакетов (более низкий уровень архитектуры) [4]. Несмотря на очевидную простоту и дешевизну таких алгоритмов, у них есть один большой недостаток: при любом переформатировании текста происходит потеря данных ЦВЗ.

Известным методом создания невидимых ЦВЗ является метод обратимого сокрытия данных (RDH – reversible data hiding), применимый для электронных документов. Суть данного метода заключается во встраивании незаметных контрольных данных, содержащих информацию об изменяемой части документа, в сам документ, подлежащий защите. Извлечение контрольных данных из файла приводит его к первоначальному виду. Данное

свойство позволяет убедиться, проводились ли с документом какие-нибудь изменения после вставки контрольных данных или нет [4].

Широкое применение в целях удостоверения личности и аутентификации и при скрытой передаче информации в бумажных документах получила стегосистема «Invisible Personal Information», или IPI [8, 11, 12]. Встраивание ЦВЗ в этой системе осуществляется путем малого сдвига всех выбранных точек контейнера на одинаковую величину в одном направлении. Принцип извлечения ЦВЗ заключается в наложении на изображение-контейнер линзового растра, сетка которого совпадает с исходным изображением, тогда в местах сдвига произойдет изменение средней яркости и ЦВЗ будет виден.

Универсальный способ формирования невидимых ЦВЗ представлен в работе [13]. Он заключается в сдвиге некоторых выбранных пикселей относительно центра изображения. Документ разбивается на строчки, в каждой из которых может быть выбран только один пиксель. Для встраивания «0» выбирается пиксель с координатами левее центра, а для встраивания «1» – правее.

В работе [14] представлен метод сокрытия информации, основанный на свойстве глифов различных кодировок. Информация вносится заменой отдельных символов текста символами той же кодировки, но другого алфавита, соответствующих по внешнему отображению, в результате чего текст будет иметь различное двоичное представление без видимых визуальных признаков.

К видимым методам относятся различные виды полиграфической защиты: дизайн, печать, использование специальной бумаги, красок и отделки [5], а также встраивание штриховых кодов [5, 7–10].

Для рассматриваемого в данной статье подхода ближайшим аналогом является технология маркеров подлинности, разработанная компанией «Генкей» [15]. Технология дает возможность создавать ЦВЗ, позволяющий обеспечить проверку авторства и содержания документа. Данный ЦВЗ имеет вид структурированной матрицы-изображения с квазипериодической структурой, состоящей из черных и белых элементов (ЦВЗ формируется с использованием метода двумерного матричного кодирования, обладающего высокой пропускной способностью). Содержание документа архивируется, дополняется ЭЦП и сертификатом открытого ключа (для проверки подлинности подписи) и встраивается в маркер. В случае несовпадения содержания маркера и документа, документ считается подделкой. Технология применяется на пропусках на режимные объекты, на номерных знаках транспортных средств, на талонах технического осмотра и паспортах транспортных средств. Данную технологию также можно использовать для «плотного хранения на бумаге» и быстрого считывания бумажных документов. Один такой маркер имеет размер 120 на 120 элементов (3.6 см) и обладает информационной емкостью с точки зрения объема скрываемой информации ЦВЗ порядка 1 килобайта.

В целом можно сделать вывод, что существующие на данный момент методы и алгоритмы, в большинстве своем, не могут применяться как средства универсальной защиты разных типов документов, так как основываются на индивидуальных особенностях каждого типа контенейра (например, особенностях двоичного представления данных или специальных красок, бумаги и др.). Решение проблемы создания универсального метода внесения ЦВЗ для защиты бумажных и электронных документов нуждается в дальнейшем развитии.

2. ПРЕДЛАГАЕМЫЙ МЕТОД СОЗДАНИЯ ЦВЗ

Идея предлагаемого алгоритма создания цифрового водяного знака (см. рис. 1) состоит во встраивании информации (битовой последовательности) путем внесения субпиксельных деформирующих искажений (ДИ) во фрагменты (блоки) искусственно синтезированных изображений с квазипериодической структурой. Исходное искусственно синтезированное изображение обычно получается на основе использования синусоидальных пространственных функций и при визуаль-

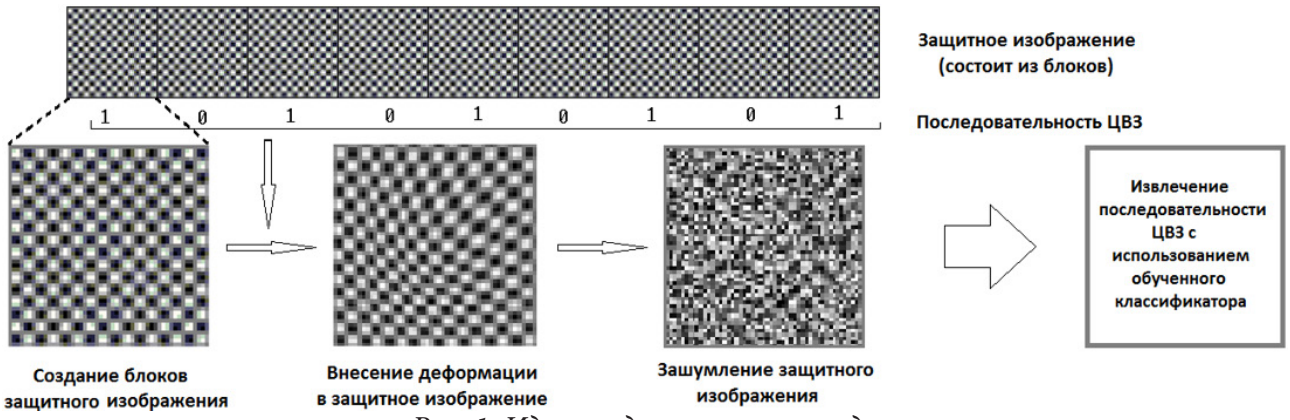

Рис. 1. Идея предлагаемого метода

ном восприятии имеет вид, подобный виду шахматной доски. Чтобы затруднить визуальное восприятие изображения – контейнера квазипериодической структуры, далее при встраивании ЦВЗ осуществляется дополнительной закрытие изображения аддитивным шумом.

Принципиальной особенностью метода является использование практически малозаметных субпиксельных сдвиговых деформаций фрагментов контейнера. Поэтому после генерации изображение, формируемое как решетчатая функция пространственных координат, преобразуется к непрерывной функции пространственных координат. Именно после этого появляется возможность внесения деформаций в блоки контейнера, сопоставимых с долями пикселя.

Извлечение цифрового водяного знака осуществляется с использованием обученного специальным образом классификатора фрагментов изображений для выделения элементов ранее встроенной последовательности данных. Обычно для этих целей используется нейросетевой классификатор, структура которого определяется размерностью анализируемых блоков и количеством разрядов встраиваемой последовательности ЦВЗ. Следует отметить, что в данном случае отсутствует проблема получением достаточного объема обучающей выборки, так как изображения-контейнеры и закрывающий их шум генерируются искусственно в процессе применении реализуемого алгоритма.

2.1. Математическая модель внесения деформаций

Математическая модель процесса внесения деформирующих искажений для данного алгоритма создания ЦВЗ основана на использовании аппроксимации решетчатой функции двух целочисленных переменных при ее представлении как непрерывной функции пространственных координат с помощью радиальных – базисных функций (РБФ) [16]. Каждая такая функция зависит от расстояния между аргументом функции и фиксированной точкой (центром РБФ):

$$\psi(u,c)=\psi\left(\|u-c\|^2\right)= \\ =\psi[(u-c)^T(u-c)/2\sigma^2], \quad (1)$$

где $\psi(\|u-c\|^2)$ – убывающая функция своего аргумента; вектор $u=u(x,y)=(x,y)^T$ – вектор пространственных координат; вектор $c=(c_x,c_y)^T$ – вектор, определяющий точку нахождения центра РБФ, в которой она достигает своего максимального значения; σ – параметр влияния РБФ, определяющий скорость убывания по мере отклонения x от центра. Применение РБФ для аппроксимации решётчатых позволяет достаточно просто вносить непрерывные деформирующие искажения любого вида [16]. Рассмотрим применение подобной аппроксимации для решения поставленной задачи.

Пусть исходная решетчатая функция (блок изображения) $w(i,j)$ задана на прямоугольной дискретной сетке: $\Omega_{ij}=\{i=\overline{1,N_x}, j=\overline{1,M_y}\}$. Здесь $w(i,j)\in \mathrm{R}^1$ для монохромных изображений или $w(i,j)\in \mathrm{R}^3$ для цвет-

ных изображений. Пусть, без принципиального ограничения общности, $N_x = rn_x$, $M_y = rm_y$, где $r \geq 1$ целое число. Для определенности будем рассматривать в качестве РБФ гауссовскую функцию вида

$$\psi\left(\left\|u-c\right\|^2\right) = \exp[-(u-c)^T (u-c)/2\sigma^2]. \quad (2)$$

Тогда аппроксимацию исходной функции с помощью РБФ для получения функции вещественных переменных $\tilde{w}(x,y)$ на множестве значений $\Omega_{xy} = \Omega_x \times \Omega_y$, $\Omega_x = [0, x_{\max}]$, $\Omega_y = [0, y_{\max}]$ можно выполнить следующим образом:

$$\tilde{w}(x,y) = \sum_{k=1}^{n_x}\sum_{t=1}^{n_y} h_{kt}\psi[u(x,y), c_{kt}] =$$

$$= \sum_{k=1}^{n_x}\sum_{t=1}^{n_y} h_{kt} \exp\left[-(u(x,y)-c_{kt})^T \times \right. \quad (3)$$

$$\left. \times (u(x,y)-c_{kt})/2\sigma^2\right],$$

где h_{kt}, $k = \overline{1, n_x}$, $t = \overline{1, n_y}$ – коэффициенты используемого представления, которые требуется определить; $c_{kt} = (c_{x,k}, c_{y,t})^T$, $c_{x,k} = (k-1)r\delta_x$, $c_{y,t} = (t-1)r\delta_y$ – координаты точек размещения центров РБФ; δ_x, δ_y – интервалы дискретизации пространственных координат при переходе от непрерывного к дискретному представлению, значения которых могут быть заданы по отношению к σ в относительных величинах $\rho_x = \delta_x / \sigma$, $\rho_y = \delta_y / \sigma$.

Если теперь для $\tilde{x}_i = (i-1)\delta_x$ и $\tilde{y}_j = (j-1)\delta_x$, $(i,j)^T \in \Omega_{ij} = \{i = \overline{1, N_x}, \quad j = \overline{1, M_y}\}$, соответствующих координатам точек в исходной решетчатой функции, вместо $\tilde{w}(x,y)$ подставить в (3) соответствующие этим точкам значения $w(i,j)$, то получится система алгебраических линейных уравнений (СЛАУ) из $N_x \times M_y$ для нахождения $n_x \times m_y$ неизвестных коэффициентов h_{kt}, $k = \overline{1, n_x}$, $t = \overline{1, m_y}$:

$$w(i,j) = \sum_{k=1}^{n_x}\sum_{t=1}^{n_y} h_{kt}\psi[u(\tilde{x}_i, \tilde{y}_j), c_{kt}],$$

$$i = \overline{1, N_x}, \quad j = \overline{1, M_y}. \quad (4)$$

Выполнив развертку исходного блока изображения $w(i,j)$, $(i,j)^T \in \Omega_{ij}$ по столбцам в вектор-столбец $W = (W_1, ..., W_{N_{xy}})^T$, $N_{xy} = N_x M_y$ и, также, представив аналогичным образом, совокупность неизвестных коэффициентов h_{kt}, $k = \overline{1, n_x}$, $t = \overline{1, m_y}$ как вектор-столбец $H = (H_1, ..., H_{n_{xy}})^T$, $n_{xy} = n_x m_y$ получим СЛАУ (4) в матричном виде

$$\Psi H = W, \quad (5)$$

где матрица Ψ, каждая s-я строка которой после умножения на H соответствует одной их компонент $W_s = w(i,j)$ вектора W, полученного после выполнения соответствующей развертки исходного блока изображения $w(i,j)$, $(i,j)^T \in \Omega_{ij}$. Ее элементами являются:

$$\Psi_s = (\Psi_{s,1}, ..., \Psi_{s,nxy}), \quad s = \overline{1, N_{xy}},$$

$$\Psi_{s,g} = \psi[u(\tilde{x}_i, \tilde{y}_j), c_{kt}] =$$

$$= \exp\left[-\frac{(\tilde{x}_i - c_{x,k})^2 + (\tilde{y}_j - c_{y,t})^2}{2\sigma^2}\right],$$

где индекс g соответствует компоненте $H_r = h_{kt}$ вектора H, полученного после выполнения соответствующей развертки исходной совокупности неизвестных коэффициентов h_{kt}, $k = \overline{1, n_x}$, $t = \overline{1, n_y}$.

Матрица Ψ имеет размеры $N_{xy} \times n_{xy}$, т. е. в общем случае является прямоугольной, поэтому СЛАУ в форме (5) является переопределенной системой уравнений. В случае, когда $r = 1$ и, соответственно, $N_{xy} = n_{xy}$ (центры РБФ размещаются во всех точках исходной решетчатой функции) матрица Ψ является квадратной. Однако и в этом случае решение СЛАУ часто оказывается затруднительным ввиду возможной плохой обусловленности матрицы Ψ. Поэтому для решения подобных СЛАУ могут быть использованы специальные методы, в том числе метод псевдоинверсии Мура-Пенроуза (нормальное псевдорешение), метод основанный на разложении SVD (Singular Value Decomposition), метод регуляризации по А. Н. Тихонову [17]. Как показали исследования, последний вариант позволяет сформировать устойчивые решения в виде

$$H = (\lambda I + \Psi^T \Psi)^{-1} \Psi^T (W - \Psi W_0), \quad (6)$$

где I – единичная матрица размером $n_{xy} \times n_{xy}$; λ – параметр регуляризации, W_0 – априорное решение (в простейшем случае нулевое). При регуляризации, чем больше λ, тем лучше обусловленность и решение ближе к априорной оценке W_0, но дальше от точного решения исходной некорректной задачи.

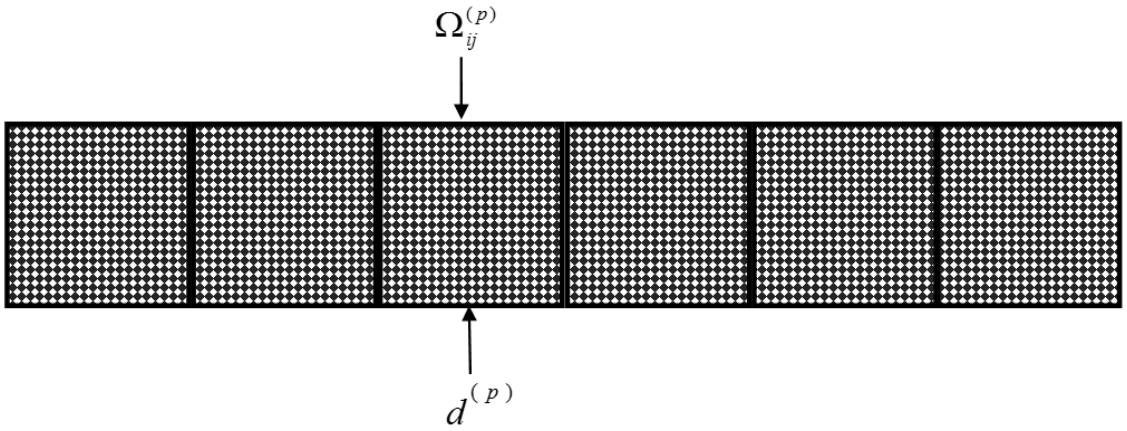

Рис. 2. Встраивание ЦВЗ в совокупность блоков изображений

После получения подобным образом непрерывного представления $\tilde{w}(x,y)$ на множестве значений $\Omega_{xy}=\Omega_x\times\Omega_y$, $\Omega_x=[0,x_{\max}]$, $\Omega_y=[0,y_{\max}]$ может проводиться внесение деформирующих искажений. В данном случае для полученной непрерывной функции с помощью РБФ оно осуществляется исключительно просто в соответствии с соотношениями

$$\tilde{w}_d(x,y)=\tilde{w}(x+v_x(x,y),y+v_y(x,y))=$$
$$=\sum_{k=1}^{n_x}\sum_{t=1}^{n_y}h_{kt}\psi[u(x+v_x(x,y),y+v_y(x,y)),c_{kt}]=$$
$$=\sum_{k=1}^{n_x}\sum_{t=1}^{n_y}h_{kt}\exp\left[-\frac{(x-c_{x,k}+v_x(x,y))^2}{2\sigma^2}+\right. \quad (7)$$
$$\left.+\frac{(y-c_{y,t}+v_y(x,y))^2}{2\sigma^2}\right],$$

где $\tilde{w}_d(x,y)$ – результирующая деформированная функция, а $v_x(x,y)$, $v_y(x,y)$, функции деформации искажений вносимых по каждой координате (в векторном виде $v(x,y)=(v_x(x,y),v_y(x,y))^T$).

Таким образом, в соответствии с (7) процесс внесения деформации в данном случае состоит в перемещении центров РБФ по закону, определяемому вектор-функцией $v(x,y)=(v_x(x,y),v_y(x,y))^T$. При этом необходимо следить, чтобы аргументы деформированной функции не выходили за пределы области определения $\Omega_{xy}=\Omega_x\times\Omega_y$, $\Omega_x=[0,x_{\max}]$, $\Omega_y=[0,y_{\max}]$. Это условие можно реализовать различными способами, простейший из которых состоит в умножении компонент вектор-функции деформации на оконную функцию $O(x,y)$, обеспечивающую выполнение условий $|v_x(x,y)|<$ $<\min\{x,\ x_{\max}-x\}$, $|v_y(x,y)|<\min\{y,\ y_{\max}-x\}$

$$v_{x(y)}(x,y)=O(x,y)v_{0x(y)}(x,y), \quad (8)$$

где $v_{0x(y)}(x,y)$ – исходные неограниченные функции деформации.

2.2. Встраивание и извлечение ЦВЗ

При реализации предлагаемого метода создания ЦВЗ, как уже упоминалось выше, реализуется внесение деформаций в совокупность блоков изображений, подобных рассмотренному в п. 2.1. Пусть ЦВЗ представляет собой закодированную последовательность m – разрядных данных $D=\{d^{(p)},\ p=\overline{1,P}\}$. Тогда для встраивания каждого элемента этой последовательности $d^{(p)}$ путем внесения деформирующих искажений будет использоваться свой блок $\Omega_{ij}^{(p)}$ с заданным на нем исходным изображением $w^{(p)}(i,j)$, $p=\overline{1,P}$ в общей дорожке блоков, как это показано на рис. 2.

Таким образом, общая блок-схема алгоритма внесения деформирующих искажений в «дорожку» блоков может быть представлена в виде, показанном на рис. 3.

В качестве функции деформации $v(x,y)=(v_x(x,y),v_y(x,y))^T$ предлагается использовать детерминированные функции, выполняющие смещения вдоль координатных осей и имеющие вид

$$v_x(x,y)=AK_{dx}O(x,y),$$
$$v_y(x,y)=AK_{dy}O(x,y), \quad (9)$$

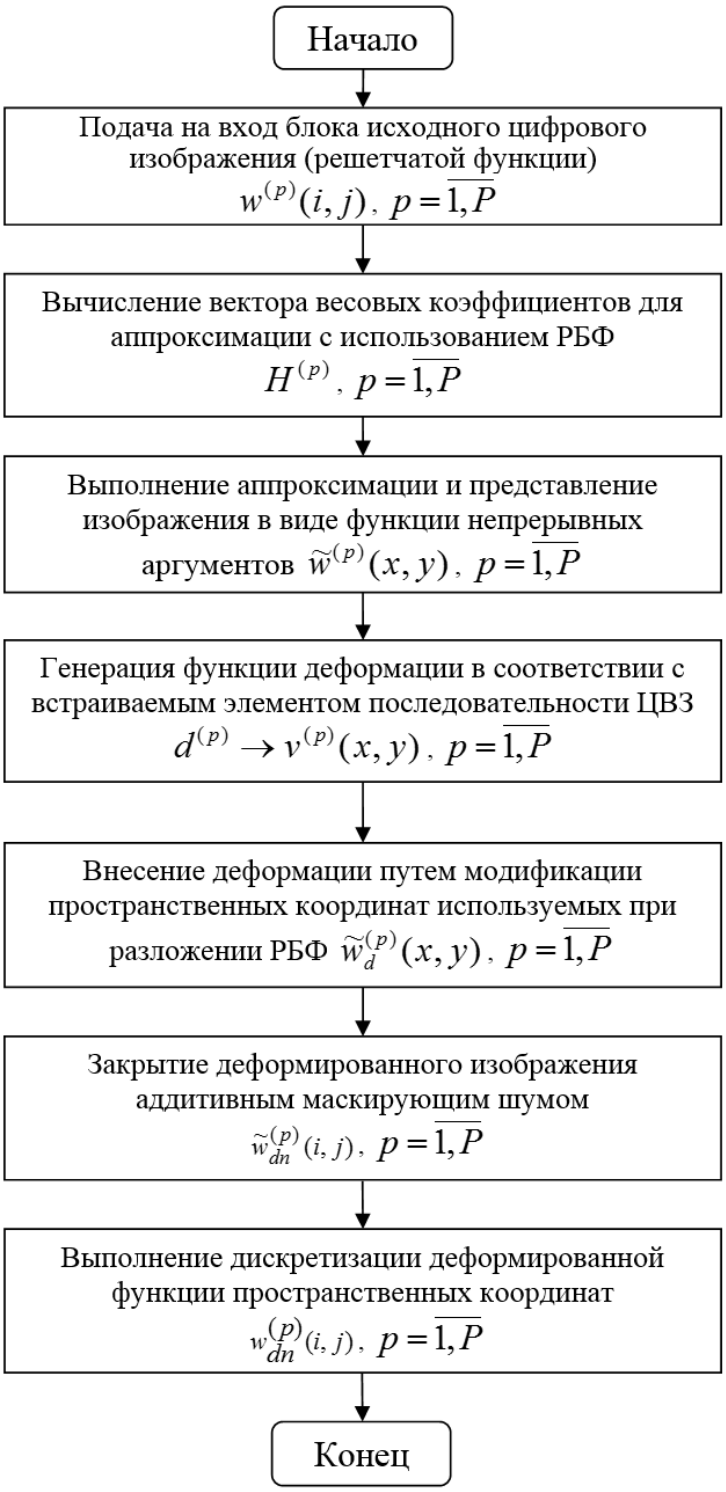

Рис. 3. Блок-схема внесения деформирующих искажений во фрагменты (блоки) изображения

где A – амплитуда вносимой деформации; $K_d\in\{-1,0,1\}$ – коэффициенты при A определяющие направления смещения по осям; $O(x,y)$ – оконная функция, имеющая вид гауссианы.

Амплитуда вносимой деформации рассчитывается с учетом шага дискретизации исходного изображения. Если принять $x_{\max}=y_{\max}=1$, то для $N_x=N_y=N$ выполняется $\delta_x=\delta_y=\delta=1/N$. Амплитуду деформации по каждой координате удобно задать в долях пикселя как $A=0.05k_s\delta$, где k_s – коэффициент, который может принимать целые положительные значения больше 0.

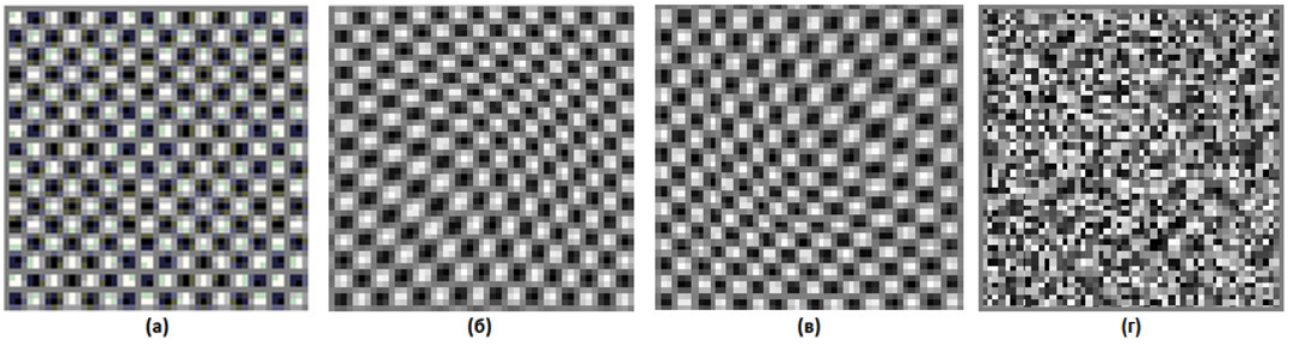

Рис. 4. (а) вид исходного изображения, (б) – деформированное изображение с направлением перекоса вправо вверх, (в) – деформированное изображение с направлением перекоса влево вниз, (г) – деформированное изображение с добавлением маскирующего шума

Таким образом, при $k_s = 1$ величина смещения относительно шага дискретизации составляет 0.05 пикселя, а при $k_s = 20$ будет производиться деформация с максимальным смешением на целый пиксель. Возможность получения субпиксельных смещений обеспечивает переход от дискретного представления исходного блока изображения на множестве $\Omega_{ij}^{(p)}$ $p = \overline{1,P}$, к функции непрерывных переменных, определенных на множестве $\Omega_{xy}^{(p)}$ $p = \overline{1,P}$. Далее для каждой области $\Omega_{xy}^{(p)}$ $p = \overline{1,P}$ полученная функция непрерывных аргументов $\tilde{w}_d^{(p)}(x,y)$ дискретизируется и получается новая – деформированная решетчатая функция $\tilde{w}_d^{(p)}(i,j)$, $p = \overline{1,P}$.

На рис. 4 (а, б, в, г) представлены примеры исходного не деформированного изображения, задаваемого функцией вида

$$w(i,j) = 0.5 + \sin\left(N_x \cdot i \cdot dx\right) \cdot \sin(N_y \cdot j \cdot dy), \quad (10)$$

деформированные изображения с различными направлениями деформации и зашумленное деформированное изображение. Здесь шум задается функцией вида

$$sh = shStd \cdot randn(nx, ny), \quad (11)$$

где $shStd$ принимает значения в диапазоне $[0..1]$ соответственно диапазону изменения полезного сигнала, а $randn(nx, ny)$ – распределенная по нормальному закону случайная величина с нулевым математическим ожиданием и единичной дисперсией. Для наглядности амплитуда смещения и уровень шума здесь задавались значительными ($k_s = 19$, $shStd = 0.7$).

Для внесения разного количества бит информации в один блок, требуется использование разного количества направлений сдвиговой деформации исходного изображения. Так, в случае внесения 1 бита информации достаточно иметь 2 направления ДИ. Схема возможных направлений внесения ДИ для различной разрядности последовательности $D = \{d^{(p)}, p = \overline{1,P}\}$ представлена на рис. 5.

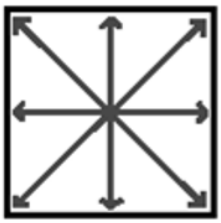

Рис. 5. Возможные направления внесения ДИ

Для внесения одного бита информации достаточно выбрать два противоположных направления из предложенных на рис. 5. Для внесения двух бит – два ортогональных и два противоположных им направления, а для внесения трех бит – все предложенные 8 направлений.

Извлечение ЦВЗ осуществляется с использованием нейронной сети прямого распространения, имеющей однослойную архитектуру с линейной функцией активации, условное обозначение которой представлено на рис. 6.

Количество нейронов в выходном слое сети зависит от количества встраиваемых в один блок бит и эквивалентно количеству возможных комбинаций «0» и «1». Формальное описание работы сети представлено ниже

$$y = \begin{pmatrix} y_1 \\ y_2 \\ \dots \\ y_m \end{pmatrix} = k \cdot \begin{pmatrix} w_{11} & w_{12} & \dots & w_{1n} \\ w_{21} & w_{22} & \dots & w_{2n} \\ \dots & \dots & \dots & \dots \\ w_{m1} & \dots & \dots. & w_{mn} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ \dots \\ x_n \end{pmatrix}, \quad (12)$$

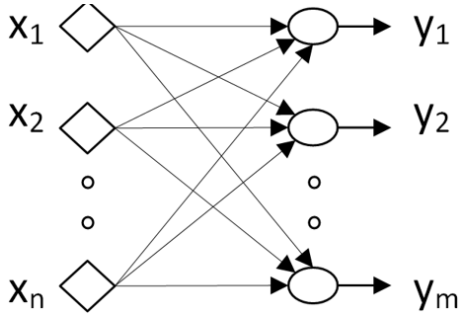

Рис. 6. Архитектура нейронной сети, реализующей извлечение информации

где w_{mn} – весовые коэффициенты связи идущей к выходу m от входа n, а k – коэффициент линейной функции активации ядра.

В случае встраивания 1 бита, вектор выходных сигналов сети будет иметь вид $y = (y_1, y_2)$. Решение будет приниматься в пользу выхода, имеющего большее значение сигнала. Если значение $y_1 > y_2$, результат интерпретируется как «0», иначе, если $y_1 < y_2$, результат интерпретируется как «1» (двухальтернативное решающее правило).

3. РЕЗУЛЬТАТЫ ЭКСПЕРИМЕНТАЛЬНЫХ ИССЛЕДОВАНИЙ И ИХ ОБСУЖДЕНИЕ

Для изучения эффективности алгоритма были проведены экспериментальные исследования, в ходе которых был реализован полный цикл встраивания и извлечения ЦВЗ в среде MATLAB с использованием разработанного в нем алгоритма. При проведении экспериментов исследовались зависимости вероятности ошибочного восстановления данных от различной амплитуды деформации и различного уровня маскирующего шума. Уровень маскирующего шума задавался на основе среднего квадратичного отклонения (СКО) случайной величины, распределенной по нормальному закону (величина *shStd* в (11)). С увеличением уровня добавляемого шума вероятность ошибочного восстановления растет при одинаковой амплитуде вносимых искажений, а при отсутствии шума она равна нулю. Полученные результаты представлены на рис. 7.

Как видно из приведенных зависимостей, нейронная сеть реализует полное восстановление встроенных данных, и при увеличении уровня шума необходимо увеличивать амплитуду вносимой деформации для надежного восстановления данных.

Одной из важных характеристик ЦВЗ является его информационная емкость. Поэтому было проведено исследование для определения минимального размера блока, содержащего в себе информацию, из которого нейронная сеть извлекает элементы ранее встроенного ЦВЗ с нулевой вероятностью

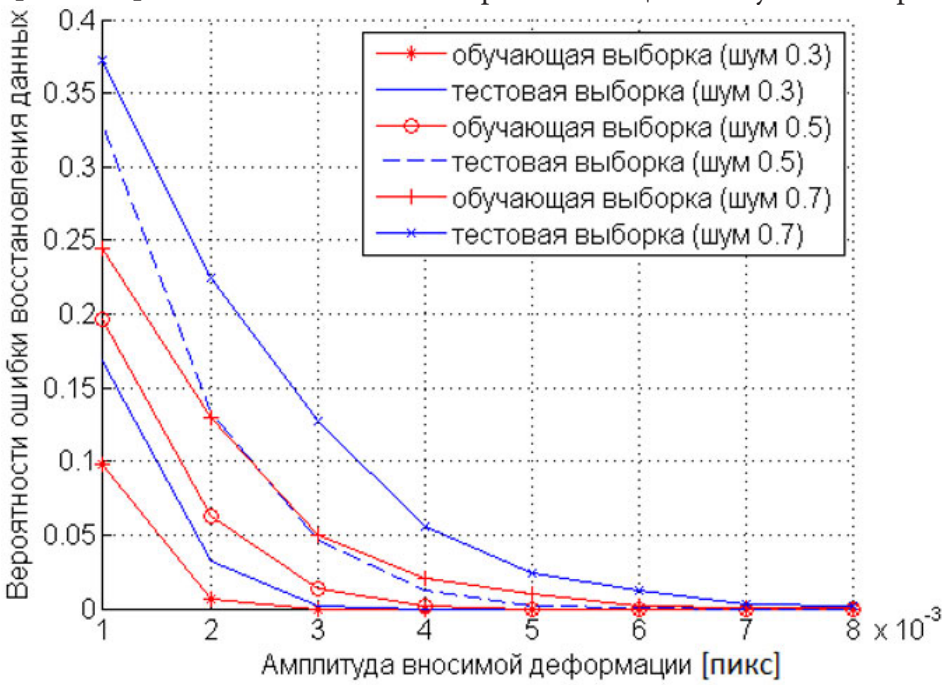

Рис. 7. Зависимость вероятности ошибки восстановления данных от амплитуды деформации (при различном уровне маскирующего шума)

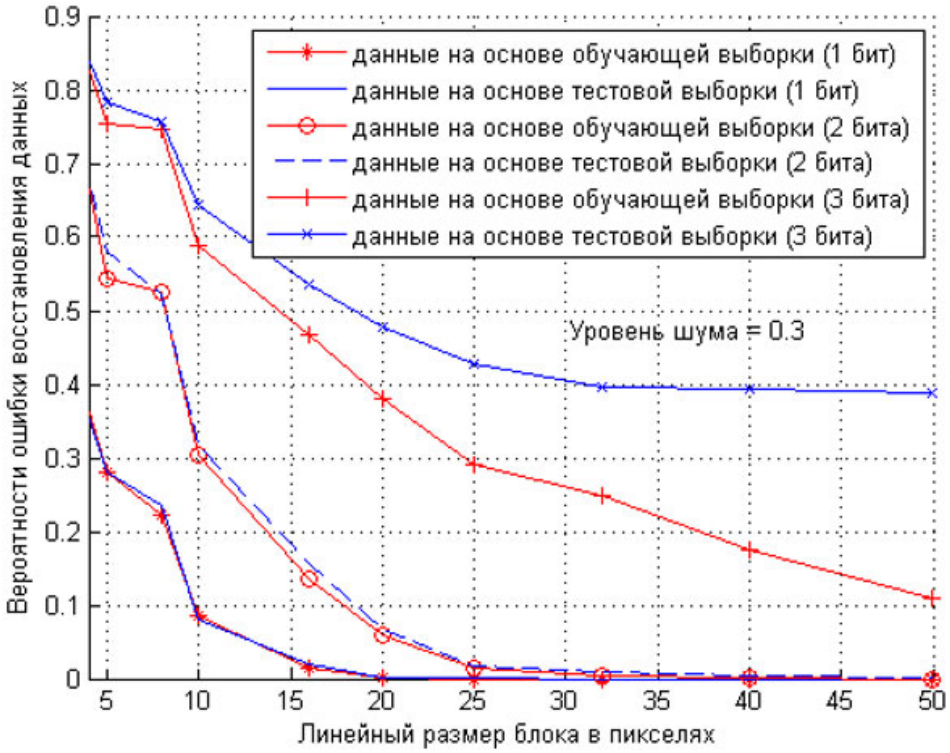

Рис. 8. Зависимость вероятности ошибки восстановления данных от размера блока изображения

ошибки. Полученные результаты при встраивании 1, 2 и 3 бит представлены на рис. 8 и в табл. 1. Как видно из рис. 8 нейронная сеть при СКО шума порядка 0.3 не реализует своих функций при внесении 3 бит информации. В этом случае для достижения лучшего результата необходимо изменить ее архитектуру, увеличив число слоев и нейронов в них, увеличив, одновременно, объем обучающей выборки.

Таблица 1

Зависимость линейного размера блока от СКО добавляемого шума и количества встраиваемых бит

Количество встраиваемых в один блок бит	СКО добавляемого шума			
	0	0.3	0.5	0.7
1	2	20	30	40
2	4	25	35	47
3	4	–	–	–

ЗАКЛЮЧЕНИЕ

В данной статье представлен алгоритм создания ЦВЗ с целью применения его для защиты электронных и бумажных документов и приведены результаты исследования алгоритма, в результате которого были получены зависимости вероятности ошибочного извлечения данных от амплитуды вносимой деформации, от величины маскирующего шума и от размера блока исходного изображения. Сравнение алгоритма с технологией маркеров подлинности показывает, что представленный алгоритм обеспечивает лучшую защищенность встроенных данных, но пока уступает в информационной емкости контейнера. Данный подход реализует высокую защищенность встроенных данных и может применяться для защиты корпоративных документов вне зависимости от его формата, а также позволяет обеспечить контроль использования и распространения каждой копии документа, что очень востребовано на сегодняшний день.

СПИСОК ЛИТЕРАТУРЫ

1. *Грибунин В. Г.* Цифровая стеганография / В. Г. Грибунин, И. Н. Оков, И. В.Туринцев. – М. : Солон-Пресс, 2002. – 272 с.

2. *Конахович Г. Ф.* Компьютерная стеганография. Теория и практика / Г. Ф. Конахович,

А. Ю. Пузыренко. – М. : МК-Пресс, 2006. – 288 с.

3. *Барсуков В. С.* Еще раз о стенографии – самой современной из древнейших наук / В. С. Барсуков, А. В. Шувалов // Специальная техника. – 2004. – № 2. – С. 51–65.

4. *Теренин А. А.* Использование цифровых водяных знаков для борьбы с инсайдерами / А. А.Теренин, Ю. Н. Мельников, В. В. Погуляев // Специальная техника. – 2008. – № 1.

5. *Дубина Н. Н.* Полиграфические методы защиты // КомпьюАрт. – 2002. – № 1. – С. 73–102.

6. *Митекин В. А.* Модели стеганографической системы и обобщенного алгоритма встраивания ЦВЗ в полиграфические изделия / В. А. Митекин, А. В. Сергеев, В. А. Федосеев, Д. М. Богомолов // Компьютерная оптика. – 2007. – Т. 31. – № 4.

7. Watermarked image generator and method of embedding watermarks into an input image – US Patent 7,006,256.

8. Digital watermarking system for making a digital watermark with few colors of input image – US Patent 6,268,866.

9. Halftone patterns for trusted printing – US Patent 5,946,103.

10. Protected document bearing watermark and method of making – US Patent 4,210,346.

11. Anti-counterfeiting method and apparatus using digital screening – US Patent 6,104,812.

12. *Глумов Н. И.* Алгоритм извлечения скрытой информации из отсканированных полиграфических изделий / Н. И. Глумов, В. А. Митекин, А. В. Сергеев, В. А. Федосеев // Вестник СГАУ. – 2008. – № 2 (15).

13. *Сагайдак Д. А.* Способ формирования цифрового водяного знака для физических и электронных документов / Д. А. Сагайдак, Р. Т. Файзуллин // Компьютерная оптика. – 2014. – Т. 38. – № 1. – С. 94–104.

14. *Балакин А. В.* Использование стеганографических методов для защиты текстовой информации / А. В. Балакин, А. С. Елисеев, А. Ю. Гуфан // T-Comm. –2009. – № S. – DSPA. – С. 42–50.

15. Технология маркеров подлинности / genkey Режим доступа : http://www.genkey.ru/newsite/products_markers.php?mn=15

16. *Акимов А. В.* Модели и алгоритмы внесения деформирующих искажений на изображениях с использованием радиально-базисных функций / А. В. Акимов, М. А. Дрюченко, А. А. Сирота // Вестник Воронеж. гос. ун-та. Сер. Системный анализ и информационные технологии. – 2013. – № 2. – С. 9–19.

17. *Сизиков В. С.* Устойчивые методы обработки результатов измерений. Учебное пособие / В. С. Сизиков. – СПб. : «СпецЛит», 1999. – 240 с.

Сирота А. А. – д-р техн. наук, профессор, заведующий кафедрой Технологий обработки и защиты информации, факультет компьютерных наук, Воронежский государственный университет.
E-mail: sir@cs.vsu.ru

Швырева А. В. – бакалавр технических наук, магистрант кафедры Технологий обработки и защиты информации, факультет компьютерных наук, Воронежский государственный университет.
E-mail: shvyreva@cs.vsu.ru

Sirota A. A. – Doctor of Technical Sciencies, Professor, Department of Processing Technology and Information Security, Computer Sciences Faculty, Voronezh State University.
E mail: sir@cs.vsu.ru

Shvyreva A. V. – Bachelor of Technical Sciencies, student of the Department of Processing Technology and Information Security, Computer Science Faculty, Voronezh State University.
E-mail: shvyreva@cs.vsu.ru