АЛГОРИТМ СТЕГАНОГРАФИЧЕСКОГО СКРЫТИЯ ИНФОРМАЦИИ НА ОСНОВЕ ПРОСТРАНСТВЕННОЙ ДЕФОРМАЦИИ ФРАГМЕНТОВ ПОЛНОЦВЕТНЫХ ИЗОБРАЖЕНИЙ

Дрюченко М.А., Сирота А.А.
Воронежский государственный университет

Аннотация

Рассматривается алгоритм стеганографического скрытия информации, основанный на внесении относительно низкочастотных малозаметных деформирующих искажений во фрагменты полноцветных изображений-контейнеров и использовании свойства корреляции цветовых каналов изображений для последующего извлечения скрытых данных. Приводятся результаты применения алгоритма в части оценки искажающих изменений контейнера и достоверности восстановления скрытых данных.

Ключевые слова: стеганографическое скрытие информации, эластичная деформация, радиальные базисные функции.

Введение

Компьютерная стеганография представляет широкий набор методов скрытного встраивания защищаемых данных в структуру других данных, называемых контейнерами, которые могут храниться в открытом виде или передаваться по незащищённым каналам. Среди потенциальных областей практического применения методов стеганографического скрытия информации (ССИ) следует отметить их использование в DRM-системах при реализации технологий создания цифровых водяных знаков и «отпечатков пальцев» для защиты прав авторства и контроля за незаконным распространением защищаемого цифрового контента, скрытое аннотирование разнородной мультимедиа информации, а также возможность использования в системах аутентификации для подтверждения подлинности цифровых документов [1, 2].

К числу наиболее распространённых методов компьютерной стеганографии относятся методы, основанные на использовании свойств избыточности визуальной и аудио информации. Среди наиболее распространённых на сегодняшний день классов алгоритмов ССИ в контейнеры графических форматов необходимо выделить следующие:

– алгоритмы разделения битовых слоёв растровых изображений носителей на сегменты по уровню сложности с последующей заменой шумовых областей битами сообщения (BPCS-алгоритмы) [3];

– алгоритмы модификации младших бит цветовых значений пикселей, предусматривающие псевдослучайный выбор пикселей носителя, адаптивный выбор количества младших бит пикселей для модификации, а также коррекцию статистических характеристик результирующего контейнера [4, 5];

– алгоритмы модификации младших бит спектральных коэффициентов изображения-контейнера с псевдослучайным их выбором и коррекцией статистик заполненного контейнера для минимизации вероятности детектирования скрытых данных [6, 7];

– алгоритмы модификации таблиц квантования JPEG [8];

– алгоритмы модификации палитры цветов [9].

Следует отметить, что практически все рассмотренные алгоритмы при внесении скрываемой информации реализуют искажения контейнера, носящие аддитивный или мультипликативный характер. К числу основных недостатков приведенных алгоритмов ССИ в изображения можно отнести сравнительно низкую стойкость по отношению к типовым операциям преобразования маркированных файлов, «алгоритмический» характер процедуры встраивания информации, при котором реализуются логически определённые последовательности операций на заранее известном подмножестве элементов контейнера. Их применение зачастую приводит к изменению статистик заполненного контейнера и, как следствие, делает возможным успешное использование стегоаналитических атак. Применяемая в некоторых алгоритмах коррекция статистических характеристик контейнера требует дополнительных вычислительных затрат и не всегда позволяет обеспечить незаметность ССИ с точки зрения стегоанализа.

В данной работе описывается подход к ССИ, основанный на внесении относительно низкочастотных малозаметных деформирующих искажений во фрагменты полноцветных изображений-контейнеров и использовании свойства корреляции цветовых каналов изображений для последующего извлечения скрытых данных. Отличие предлагаемого алгоритма ССИ от известных, главным образом, заключается в реализации нестандартного способа внесения незначительных искажающих изменений графического контейнера, которые носят не аддитивно или мультипликативный характер, а основаны на плавной эластичной деформации непересекающихся фрагментов контейнера. При этом обеспечивается возможность осуществления «нецелочисленных» сдвигов координат опорных точек деформируемых областей изображения за счёт привлечения специальных процедур аппроксимации цифрового изображения и его представления в виде непрерывной функции пространственных координат. Как показали предварительные эксперименты, а также представленные ниже результаты, при реализации такого подхода факт ССИ не обнаруживается при первичном визуальном анализе, а также с привлечением известных статистических стеганографических атак, ориентированных на классические схемы стегоскрытия.

Процедура восстановления ранее скрытой информации, основанная на анализе нарушенной корреляции цветовых компонент фрагментов заполненного контейнера, в предлагаемом алгоритме реализуется с использованием аппарата искусственных нейронных сетей. Адаптивный характер, способность к дообучению для работы с графическими контейнерами, имеющими различные статистические характеристики, позволяет рассматривать нейронные сети в качестве универсального стеганографического декодера.

Следует отметить, что идея использования нейронных сетей в приложениях стеганографии на сегодняшний день является весьма актуальной. Анализ целого ряда публикаций позволяет сделать вывод, что нейронные сети используются в качестве декодеров, классификаторов и инструментов принятия решений о наличии в контейнере скрытой информации [10 – 12]. Однако следует отметить, что предложенный в статье вариант применения нейронных сетей для восстановления скрытой информации в известных работах не рассматривался.

1. Алгоритм встраивания информации

В общем виде задача стеганографического информационного скрытия формулируется следующим образом [1]. Требуется для множества возможных контейнеров *Z*, скрываемых сообщений *D* и стеганографических ключей *K* реализовать преобразования вида:

$$F_1 : Z \times D \times K \to \tilde{Z},\ \forall z \in Z, \tilde{z} \in \tilde{Z} :\ \left\| z - \tilde{z} \right\| \to \min,$$

$$F_2 : \tilde{Z} \times K \to \tilde{D},\ \forall d \in D, \tilde{d} \in \tilde{D} :\ \left\| d - \tilde{d} \right\| \to \min. \quad (1)$$

При построении прямого F_1 и обратного F_2 стеганографических преобразований обязательным условием является минимизация искажающих изменений заполненного контейнера $\tilde{z}$, а также минимизация ошибок при извлечении сообщения $\tilde{d}$. Также для систем создания и использования цифровых водяных знаков (ЦВЗ) выдвигается требование робастности встроенных сообщений к возможным искажениям ε маркированного контейнера: $\left\| d - F_2\left(z + \varepsilon, k\right) \right\| \to \min$.

В качестве сообщения d без ограничения общности всегда можно рассматривать двоичную (битовую) последовательность.

Как известно, любой алгоритм ССИ основан на внесении незначительных изменений в структуру файла-контейнера либо на изменении его статистических свойств таким образом, чтобы, зная характер вносимых изменений, можно было сформировать решающие правила (детекторы), позволяющие с той или иной степенью достоверности обнаруживать модификации, внесённые в процессе ССИ.

В качестве вносимых изменений, кодирующих биты скрываемой информации (d), далее предлагается использовать пространственную деформацию фрагментов полноцветных растровых изображений (z), выполняемую для одной из цветовых компонент пространства RGB. Основная идея выполняемой обработки состоит в том, чтобы при извлечении на основе обучаемого решающего правила выявить наличие и параметры вносимых деформаций, и базируется на следующем. Характерной особенностью полноцветных изображений фотографического характера с глубиной цвета не менее 16 бит/пиксель является наличие локальной зависимости между составляющими градиента отдельных цветовых каналов. Так, в работе [13] отмечается, что объекты на цветных изображениях коррелируют между собой (совпадают по положению контуров и текстурным перепадам) в цветовых каналах. Незначительное локальное нарушение корреляции цветовых компонент пикселей (например, в цветовом пространстве RGB) можно использовать в интересах реализации стеганографических преобразований для встраивания и декодирования информации в контейнер-изображение.

В качестве базового метода искажения выбранных цветовых плоскостей двумерного изображения для реализации процедуры ССИ нами предлагается использовать метод эластичной деформации решётчатой функции с использованием аппроксимации на основе радиальных базисных функций (radial basis function, RBF) [14,15]. Среди преимуществ RBF-метода деформации перед известными сеточными методами [16,17] и методами многомерной интерполяции [18] следует отметить возможность точной плавной интерполяции участков растра, учёт изменения координат лишь заданных опорных точек (узлов) без привязки к сетке, возможность использования функций радиального базиса различной гладкости.

Математическая модель процесса внесения деформирующих искажений (ДИ) для исходной функции $f(x_1,...,x_n)$ n аргументов определяется следующим соотношением:

$$f(x_1 + r_1(x_1,..,x_n),..,x_n + r_n(x_1,..,x_n)) = \\ = f(u_1(x_1,..,x_n),..,u_n(x_1,..,x_n)) = f(u(x)) = g(x_1,..,x_n), \quad (2)$$

где $g(x_1,...,x_n)$ – результирующая деформированная функция; $r_i(x_1,...,x_n)$, $i = \overline{1,n}$ – функции вносимых деформирующих искажений по каждой координате, которые могут носить детерминированный или стохастический характер. Обозначив $r(x) = (r_1(x),...,r_n(x))^T$, перепишем (2) в виде:

$$f(x + r(x)) = f(u(x)) = g(x). \quad (3)$$

При реализации процесса внесения ДИ на основе (3) возникает ряд особенностей. Первая из них заключается в том, что область определения деформированной функции $g\left(x_1,\dots x_n\right)$ не должна выходить за пределы области определения исходной функции $f\left(x_1,\dots x_n\right)$. Данное условие исключает возможность возникновения артефактов при выходе аргументов в случае внесения ДИ за пределы области определения исходной функции. Для гарантированного обеспече-

ния выполнения этого условия можно использовать ограничивающие значения функции $u(x)$ по краям области определения исходной функции маски $u(x)=x+h(x)r(x)$. Функции $h(x)$ должны стремиться к нулю на границах области определения и к единице в её центре. В качестве них могут быть использованы гауссианы с соответствующим образом подобранными параметрами.

Вторая особенность реализации процесса внесения ДИ на основе (3) состоит в следующем. В случаях, когда исходная функция $f(x)$ является решётчатой функцией дискретных аргументов, т.е. задана на многомерной дискретной сетке (например, в случае деформации цифровых растровых изображений), прямое применение (3) невозможно. В данном случае для обеспечения возможности модификации аргументов $f(x)$ при внесении в них ДИ произвольного характера необходимо предварительно выполнять интерполяцию и её представление в виде функции $\tilde{f}(x)$ непрерывных аргументов. Далее вносятся деформирующие искажения путём подстановки $r(x)$ в аргументы $\tilde{f}(x)$. В результате получается деформированная функция непрерывнозначных аргументов $\tilde{g}(x)$, которая далее дискретизируется. В результате формируется новая решётчатая функция дискретных аргументов $\bar{g}(x)$.

При реализации предлагаемого алгоритма стеганографического скрытия данных осуществляется независимая деформация блоков изображения фиксированного размера. Для соседних блоков граничные пиксели являются общими. Для простоты набор пикселей, описывающих деформируемый блок изображения размерностью $w\times h$, запишем в виде вектора $P=(P_1,P_2,\dots P_n)$, где $P_j=(x_j,y_j)$, $j=\overline{1,n}$, $n=wh$. Для аппроксимации блока пикселей непрерывной функцией вычисляется интерполирующая функция в виде:

$$\tilde{f}(x,y)=\sum_{j=1}^{n} w_j U\left(\left\|P_j-(x,y)\right\|\right)+\phi(x,y), \qquad (4)$$

где w_j – неизвестные коэффициенты, которые требуется найти; $U(r_{ij})$ задаёт вид радиальных базисных функций, $r_{ij}=\left\|P_i-P_j\right\|=\sqrt{\left(x_i-x_j\right)^2+\left(y_i-y_j\right)^2}$ – расстояние между точками с координатами (x_i,y_i) и (x_j,y_j), $i,j=\overline{1,n}$; $\phi(x,y)=\phi_1+\phi_x x+\phi_y y$ – полином, вводимый в (4) в случае использования в качестве U сплайнов «тонкой пластины» или мультиквадратичных RBF-функций [19, 20]. На практике в качестве U часто применяются функции вида гауссиана ($U(r)=e^{-\alpha r^2}$, $\alpha>0$), мультиквадратичные и обратные мультиквадратичные функции ($U(r)=\sqrt{1+r^2}$, $U(r)=\left(\sqrt{1+r^2}\right)^{-1}$), сплайны «тонкой пластины» ($U(r)=r^2\log(r)$), ядра Вендланда. При реализации алгоритма стеганографического встраивания данных рассматривались два варианта RBF-функций: $U(r)=e^{-r^2/2\sigma^2}$, где σ – параметр влияния RBF-функций, и $U(r)=r^2\ln(r)$.

Элементам суммы (4) соответствуют центры RBF-функций с координатами x_j,y_j. При наличии в (4) полинома ϕ коэффициенты w_j должны подчиняться условиям:

$$\sum_{j=1}^{n} w_j=0,\ \sum_{j=1}^{n} w_j x_j=0,\ \sum_{j=1}^{n} w_j y_j=0.$$

Вектор $W=(w_1,\dots w_n)$ и коэффициенты полинома (ϕ_1,ϕ_x,ϕ_y) определяются из системы уравнений, записываемой в матричной форме в виде

$$A=L^{-1}Y, \qquad (5)$$

где

$$A=\left(W \mid \phi_1 \quad \phi_x \quad \phi_y\right)^T,\ L=\left(\begin{array}{c|c} K & B \\ \hline B^T & O \end{array}\right),$$

$$K=\begin{pmatrix} 0 & U(r_{12}) & \dots & U(r_{1n}) \\ U(r_{21}) & 0 & \dots & U(r_{2n}) \\ \dots & \dots & \dots & \dots \\ U(r_{n1}) & U(r_{n2}) & \dots & 0 \end{pmatrix},$$

$$B=\begin{pmatrix} 1 & x_1 & y_1 \\ 1 & x_2 & y_2 \\ \dots & \dots & \dots \\ 1 & x_n & y_n \end{pmatrix},$$

O – нулевая матрица размером 3×3; $Y=(V|0\ 0\ 0)^T$, $V=(v_1,\dots,v_n)$, v_i – значения решётчатой функции дискретных аргументов в координатах (x_i,y_i).

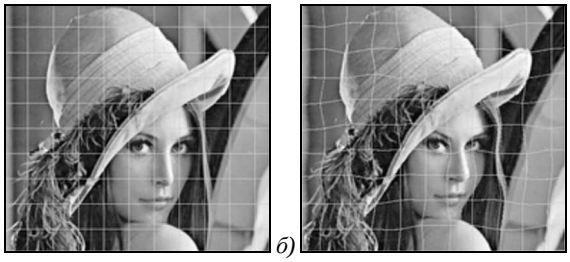
На практике получаемые в (5) системы уравнений не всегда могут иметь стандартное решение из-за плохой обусловленности невырожденной матрицы L [20]. В этих случаях применяются методы регуляризации. Например, используют расчёт псевдообратной матрицы $A=L^{+}Y$ (где L^{+} – псевдообратная матрица к L) или регуляризацию по А.Н. Тихонову [21]. В последнем случае решение имеет вид

$$A=\left(\lambda I+L^T L\right)^{-1}L^T\left(Y-LA_0\right),$$

где I – единичная матрица размером $(n+3)\times(n+3)$; λ – параметр регуляризации, A_0 – априорное решение. При регуляризации чем больше λ, тем лучше обусловленность и ближе решение к априорной оценке A_0, но дальше от решения исходной некорректной задачи. Исходя из этих соображений, параметр λ должен принимать промежуточные значения, определяемые эмпирическим путём или при помощи дополнительного анализа. Если в качестве A_0 использовать

нулевую матрицу, то регуляризация будет проводиться без учёта априорного решения [15].

В простейшем случае искажения контейнера выполняются путём внесения плавной сдвиговой деформации центральной части каждого фрагмента вдоль одной из осей или по диагонали на заданное значение амплитуды сдвига Δ, измеряемой в единицах пикселей. Необходимо отметить, что предлагаемый подход позволяет вносить деформирующие искажения при любых значениях амплитуды искажений Δ, в том числе нецелочисленных. Пример деформации фрагмента изображения «Lena.bmp» с использованием в качестве RBF-функции сплайнов «тонкой пластины» приведен на рис. 1*а*, *б*. На исходном и искажённом изображениях дополнительно показана сетка, в координатах узлов которой задавались опорные точки, относительно которых производилась деформация (задают решётчатую функцию дискретных аргументов). Для каждого узла сетки деформация представляла из себя односторонний сдвиг в случайном направлении (вертикально-горизонтальном или диагональном) с максимальной амплитудой $\Delta_{\max}=3$ пикселя. Следует отметить, что вносимые в процессе деформации растра искажения носят низкочастотный характер, что является важным аспектом при реализации стегоалгоритмов, потенциально устойчивых к высокочастотным искажениям контейнера-изображения. Что касается требования минимизации искажающих изменений стеганографического контейнера, то при амплитуде деформации $\Delta_{\max}\le 1$ на изображениях с невыраженной регулярной структурой визуально определить наличие модификаций достаточно сложно.



а) *б)*

Рис. 1. Фрагмент исходного изображения «Lena.bmp» (а); фрагмент «деформированного» изображения, максимальная амплитуда деформации $\Delta_{max}=3$ (б)

Далее с учётом особенностей предлагаемого алгоритма внесения ДИ для реализации ССИ использовались непересекающиеся блоки контейнера, а не изображение целиком, и проводилась независимая деформация отдельных цветовых компонент в рамках каждого блока в различных направлениях, соответствующих значениям элементов битовой последовательности. Информационная ёмкость предложенного алгоритма, определяемая отношением объёма доступного пространства стегоскрытия к общему объёму контейнера, невелика. В случае встраивания одного бита информации в каждый деформируемый блок контейнера, информационная ёмкость будет определяться отношением числа модифицируемых блоков контейнера к его объёму в битах. Так, для несжатого полноцветного растрового изображения размером 1600×1200 пикселей, содержащего 30000 непересекающихся блоков размерностью 8×8 пикселей, каждый из которых используется для встраивания одного бита сообщения, информационная ёмкость алгоритма составит $6{,}51\cdot10^{-4}$.

При реализации «блочного» варианта алгоритма скрывающее информацию преобразование F_1 можно записать в виде:

$$F_1\left(z^{(i)},d_i\right)=\begin{cases}z^{(i)}, & d_i=0\\ \tilde{z}^{(i)}, & d_i=1\end{cases},\ i=\overline{1,N},$$

где N – длина встраиваемой последовательности в битах, $z^{(i)}=\left(z_R^{(i)}\mid z_G^{(i)}\mid z_B^{(i)}\right)\in z,\tilde{z}$ – непересекающиеся блоки пикселей заданного размера $w\times h$, которые не подвергаются модификации,

$\tilde{z}^{(i)}=\left(z_R^{(i)}\mid z_G^{(i)}\mid \tilde{z}_B^{(i)}\right)\in\tilde{z}$, $i=\overline{1,N}$ – блоки пикселей, полученные в результате пространственной деформации их синих цветовых плоскостей $z_B^{(i)}$. Выбор для модификации синих цветовых плоскостей блоков обусловлен физиологическими свойствами человеческого зрения и направлен на минимизацию визуальных искажений маркированного контейнера. По аналогии с алгоритмом JPEG рассматривались квадратные блоки пикселей размерностью 8×8 пикселей. Для простоты длина встраиваемого сообщения выбиралась не больше доступного пространства стегоскрытия, определяемого общим количеством непересекающихся блоков заданного размера на изображении.

В общем случае деформация синей цветовой плоскости в блоке изображения выполняется путём сдвига синей компоненты блока на заданный шаг Δ вдоль одной или нескольких осей фрагмента контейнера $z_B^{(i)}$ в низкочастотном спектре. Преобразования производятся над элементами контейнера, представленными в вещественной форме. После деформации значения пикселей дискретизируются.

Пример результатов работы алгоритма встраивания в виде увеличенных фрагментов «поблочно» деформированной синей цветовой плоскости тестового изображения «Lena.bmp» для максимальных значений амплитуды деформации $\Delta_{\max}=0{,}5$, $\Delta_{\max}=1$ и $\Delta_{\max}=2$ приведен на рис. 2*б-г*.

При увеличении модифицированных изображений цветовых плоскостей на контрастных областях растра можно наблюдать артефакты встраивания – незначительные изломы границ объектов. В то же время при объединении цветовых плоскостей и рассмотрении полноцветного растра (рис. 2*г*) визуально определить факт деформации (для малых $\Delta_{\max}\le 1$) практически невозможно.

2. Алгоритм извлечения информации

Для реализации восстанавливающего скрытые данные преобразования F_2 использовалась однослойная нейронная сеть (НС) прямого распространения с линейной передаточной функцией (рис. 3), реализующая двухальтернативное решающее правило (на выходе сети восстанавливается двоичная последовательность данных $\tilde{d}$).

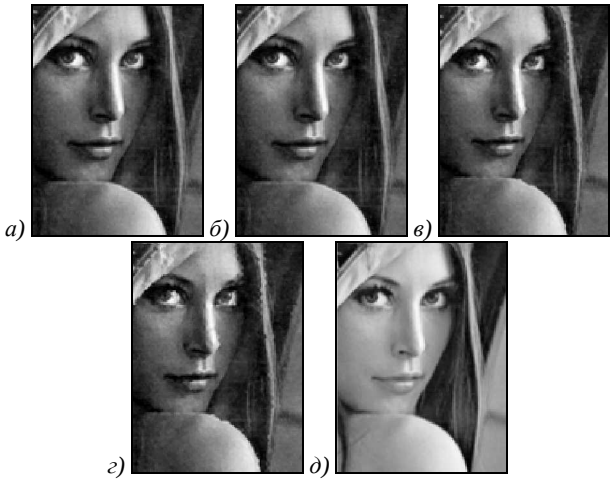


Рис. 2. Увеличенный фрагмент исходного изображения «Lena.bmp» (синий цветовой канал) (а); фрагменты «блочно» деформированного изображения (синий цветовой канал) с амплитудой деформации $\Delta_{\max} = 0{,}5$ (б), $\Delta_{\max} = 1$ (в) и $\Delta_{\max} = 2$ пикселя (в), размер блоков 8×8; фрагмент изображения, сформированного в результате объединения деформированного синего цветового канала с исходными (красным и зелёным) при $\Delta_{\max} = 1$

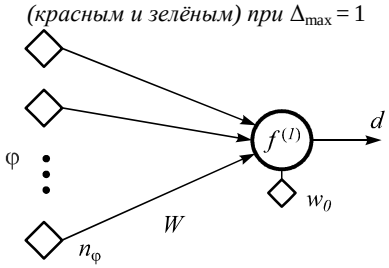


Рис. 3. Нейронная сеть, реализующая восстановление скрытой информации

Результаты предварительных экспериментов показали, что для формирования обучающей выборки, в максимальной степени отражающей корреляционные связи нетронутых (R,G) и деформированных (B) цветовых плоскостей, целесообразно использовать разности их градиентов. Дополнительно для уменьшения артефактов стеганографического кодирования эмпирически задаётся порог $10 \le \tau \le 120$, определяющий допустимые максимальные значения уровня градиента для немодифицируемых R и G цветовых компонент блока. В этом случае очередной *i*-й блок контейнера выбирается для модификации, если выполняется условие $\max\left(\max\left(\nabla z_R^{(i)}\right), \max\left(\nabla z_G^{(i)}\right)\right) \le \tau$.

Матрица обучающих данных НС определялась в виде $\Phi = \{\varphi_1, \varphi_2, ..., \varphi_M\}$, где

$$\varphi_i = \left(\varphi_R^{(i)}(0,0)\ \varphi_G^{(i)}(0,0) ... \varphi_R^{(i)}(w-1,h-1)\ \varphi_G^{(i)}(w-1,h-1)\right),$$

$i = \overline{1,M}$, M – объём обучающей выборки, определяемый числом блоков, в которые производится встраивание информации. Элементами вектора ϕ_i являются выписанные по столбцам элементы матриц разности градиентов (с центрированием) цветовых плоскостей *i*-го блока:

$$\phi_R^{(i)} = \nabla\hat{z}_R^{(i)} - \nabla\hat{z}_B^{(i)},\quad \phi_G^{(i)} = \nabla\hat{z}_G^{(i)} - \nabla\hat{z}_B^{(i)},$$

$$\nabla\hat{z}_R^{(i)}(j,l) = \nabla z_R^{(i)}(j,l) - m_R^{(i)},$$

$$\nabla\hat{z}_G^{(i)}(j,l) = \nabla z_G^{(i)}(j,l) - m_G^{(i)},$$

$$\nabla\hat{z}_B^{(i)}(j,l) = \nabla z_B^{(i)}(j,l) - m_B^{(i)},$$

$$\nabla z_R^{(i)} = \sqrt{\left(s_x * z_R^{(i)} / 255\right)^2 + \left(s_x * z_R^{(i)} / 255\right)^2},$$

$$\nabla z_G^{(i)} = \sqrt{\left(s_x * z_G^{(i)} / 255\right)^2 + \left(s_x * z_G^{(i)} / 255\right)^2},$$

$$\nabla z_B^{(i)} = \sqrt{\left(s_x * \tilde{z}_B^{(i)} / 255\right)^2 + \left(s_x * \tilde{z}_B^{(i)} / 255\right)^2}$$

($*$ обозначает двумерную операцию свертки),

$$m_R^{(i)} = (wh)^{-1} \sum_{j=1}^{w} \sum_{l=1}^{h} \nabla z_R^{(i)}(j,l),$$

$$m_G^{(i)} = (wh)^{-1} \sum_{j=1}^{w} \sum_{l=1}^{h} \nabla z_G^{(i)}(j,l),$$

$$m_B^{(i)} = (wh)^{-1} \sum_{j=1}^{w} \sum_{l=1}^{h} \nabla z_B^{(i)}(j,l).$$

Для вычисления градиента использовались стандартные ядра дискретного дифференциального оператора Собеля размером 3×3 s_x, s_y. Количество входных контактов сети $n_\varphi = 2wh$ определялось как удвоенное число пикселей обрабатываемого блока изображения. Ожидаемые на выходе сети значения определялись компонентами целевого двоичного вектора-сообщения $d = (d_1, d_2, ... d_M)$, где $d_i = \{-1, +1\}$, $i = \overline{1,M}$.

Матрица входных данных для тестирования обученной НС формировалась в виде $\bar{\Phi} = \{\bar{\varphi}_1, \bar{\varphi}_2, ... \bar{\varphi}_Q\}$, где векторы $\bar{\varphi}_i$, $i = \overline{1,Q}$ содержат элементы матриц разности градиентов цветовых плоскостей блоков тестового изображения, Q – объём тестовой выборки, определяемый числом блоков контейнера, в которые производилось встраивание информации. Получаемые на выходе сети данные обозначались как $\tilde{d} = (\tilde{d}_1, \tilde{d}_2, ... \tilde{d}_Q)$, где $\tilde{d}_i = \{-1, +1\}$, $i = \overline{1,Q}$.

При практическом использовании НС для реализации правила восстановления ранее скрытых данных по возможности следует исключать случаи переобучения сети. Эффект переобучения наблюдается при «индивидуальном» (контентно-зависимом) обучении НС – с использованием выборки обучающих данных малого размера, сформированной на основе фрагментов одного графического контейнера. При последующем использовании такой сети для восстановления информации, скрытой в контейнеры с отличающимися характеристиками, возможно значительное снижение достоверности процедуры восстановления данных и получение некорректных результатов. Следует, однако, отметить, что это лишь возможный частный случай практического использования алгоритма для конкретного контейнера. С целью улучшения репрезентативности приводимых в статье результатов при проведении тестирования обучающая выборка для НС, реализующей восстановление ранее скрытой

информации, формировалась на основе фрагментов нескольких различных изображений из тестовых наборов [22, 23]. Впоследствии обученная сеть использовалась для извлечения данных из других изображений, не участвовавших в обучении.

3. Экспериментальные исследования уровня искажения контейнера и достоверности восстановления скрытых данных

Экспериментальный анализ разработанного алгоритма в части оценки искажающих изменений контейнера и достоверности восстановления скрытых данных проводился с использованием полноцветных несжатых изображений из известных наборов Kodak Lossless True Color Image Suite [22] и TESTIMAGES [23]. Разрешение тестовых изображений варьировалось от 300×300 до 1200×1200 пикселей. Тестирование стегоалгоритма проводилось как по изображениям, фрагменты которых содержались в обучающем множестве восстанавливающей данные НС, так и по изображениям, не участвовавшим в обучении НС. Основным критерием предварительной оценки уровня искажений контейнера являлась среднеквадратическая ошибка (СКО)

$$MSE_{X,Y} = (wh)^{-1} \sum_{i=1,\,j=1}^{w,h} \left(X_{i,j} - Y_{i,j}\right)^2 ,$$

где X – исходное изображение, Y – изображение, содержащее скрытно встроенную информацию, w и h – ширина и высота изображения. Вероятность ошибки при извлечении информации определялась как $P_{err} = n_{err}/M$, где n_{err} – количество ошибочно восстановленных НС бит.

На рис. 4 приведены зависимости среднеквадратической ошибки искажения контейнера и вероятности ошибки восстановления скрытой информации от значений амплитуды деформации в блоках изображения для RBF-функций $U(r) = r^{-r^2/2\sigma^2}$, параметр влияния RBF-функции $\sigma = 0{,}85$ (рис. 4*а*, *б*) и $U(r) = r^2 \ln(r)$ (рис. 4*в*, *г*).

Соотношения были получены для следующих условий: размер обрабатываемых блоков контейнера – 8×8 пикселей, амплитуда деформации – $0{,}5 \le \Delta \le 3$, объём выборки для обучения нейронных сетей $P_1 = 4000$, объём тестирующей выборки $P_2 = 10000$, число эпох обучения $T = 5000$, порог для уровня градиента, при превышении которого встраивание информации не производится, $\tau = 30$. Для извлечения данных использовалась однослойная НС с линейной передаточной функцией, реализующая двухальтернативное решающее правило. На графиках используются следующие обозначения: $\text{mse\_train}_{1,2}$ – СКО искажения контейнера при тестировании алгоритма на данных, используемых для обучения НС, $\text{mse\_test}_{1,2}$ – СКО искажения контейнера при тестировании на данных, не участвовавших в обучении НС, $\text{perr\_train}_{1,2}$, $\text{perr\_test}_{1,2}$ – вероятности ошибки восстановления скрытой информации при тестировании на данных используемых и не используемых для обучения НС соответственно. Индексы в обозначениях характеризуют варианты деформации: 1 – деформацию содержимого блока по двум направлениям (симметричное растяжение по оси OX или OY), 2 – деформацию в одном направлении (сдвиг на заданный шаг Δ по одной из осей).

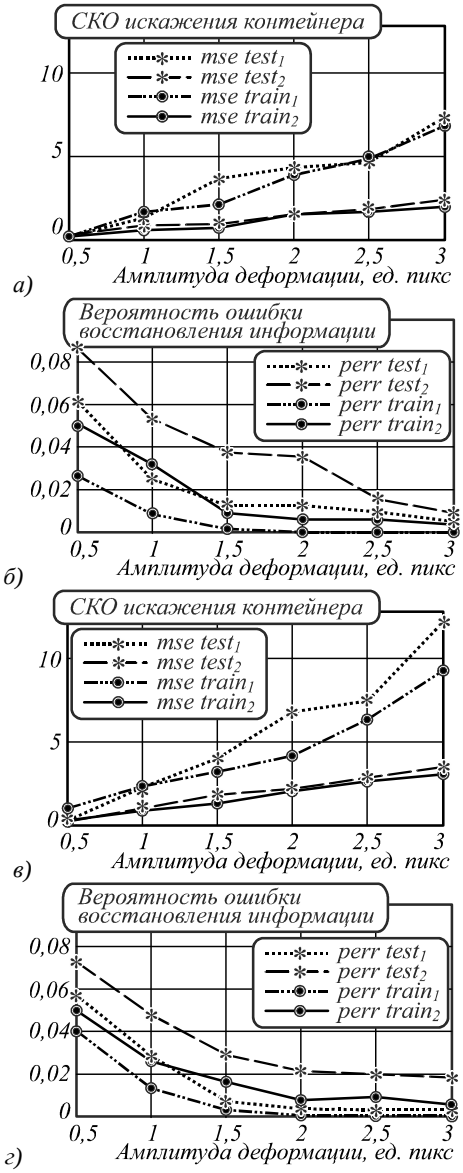


Рис. 4. Зависимости среднеквадратической ошибки искажения контейнера (а, в) и вероятности ошибки восстановления скрытых данных (б, г) от значения амплитуды деформации для RBF-функций двух видов

Как показали результаты экспериментов, с увеличением амплитуды деформации вероятность ошибки восстановления скрытой информации убывает до 0,5 % для первого и до 1 % для второго варианта деформации (для RBF-функции вида Гауссиана) и до 0,3 % и 2% (для сплайнов «тонкой пластины») при проведении тестирования на данных, не участвовавших в обучении сети и значении амплитуды $\Delta = 3$. Одновременно с этим СКО искажения маркированного контейнера возрастает до 2 и 7,5 соответственно (для Гауссовых RBF-функций) и до 3,5 и 12 (для сплайнов «тонкой пластины»). Следует

отметить, что критерий предварительной оценки ошибок – СКО (впрочем, как и все остальные математические критерии) не может соответствовать всем аспектам восприятия искажений человеком и не отражает наличие возможных структурных артефактов, возникающих в результате стеганографического скрытия информации, поэтому после внесения деформации в блоки контейнера желательно всегда визуально оценивать результат.

Существенно повысить достоверность восстановления информации возможно за счёт обучения и использования НС, реализующих оператор F_2, индивидуально для каждого маркируемого контейнера. В этом случае параметры обученной сети будут являться стеганографическим ключом. При тестировании стегоалгоритма на данных, используемых для предварительного обучения НС, независимо от вида функции U в (4) вероятность ошибок извлечения информации не превышает 1 % для значений $\Delta \ge 1,5$.

4. Экпериментальные исследования устойчивости скрытых данных к возможным искажениям заполненного контейнера, а также к некоторым статистическим стегоатакам

Для исследования устойчивости предложенного алгоритма стеганографического информационного скрытия были проведены эксперименты в части оценки вероятности восстановления ранее скрытых данных из заполненных контейнеров, подвергшихся искажениям в виде искусственного зашумления импульсным шумом (плотностью η от 5 до 30 %), медианной и сглаживающей фильтрации, преобразованиям яркости.

Относительная устойчивость встроенной информации была показана при добавлении к заполненным контейнерам импульсного шума небольшой плотности. Для зашумлённых носителей из тестовых наборов, имеющих 100 % заполнение и сформированных при использовании оптимальной с точки зрения минимизации визуальных искажений значений амплитуды деформации $\Delta_{\max} \le 2$ для блоков контейнера размером 8×8 пикселей, деформируемых по двум направлениям, Гауссовых RBF-функций и порогового значения уровня градиента $\tau = 30$ были получены следующие усреднённые по реализациям (разным контейнерам) значения вероятности ошибок восстановления данных. Вероятность ошибки извлечения информации для контейнеров, участвовавших в обучении составила $\text{perr\_train}_1 \approx 4{,}5\,\%$ при $\eta = 0,05$, $\text{perr\_train}_1 \approx 1\,1\%$ при $\eta = 0,1$, $\text{perr\_train}_1 \approx 26{,}5\,\%$ при $\eta = 0,3$. Для тестовых контейнеров, не участвовавших в обучении НС $\text{perr\_test}_1 \approx 6{,}5\,\%$ при $\eta = 0,05$, $\text{perr\_test}_1 \approx 16\,\%$ при $\eta = 0,1$, $\text{perr\_test} \approx 29\,\%$ при $\eta = 0,3$. Полученные значения показывают возможность уверенного восстановления встроенной информации (с незначительными ошибками) при небольшой плотности вносимого импульсного шума ($< 0,15$). При большей доле искажённых шумом пикселей ошибки восстановления информации можно считать неприемлемыми.

Устойчивость встроенных данных к изменению яркости и нормализации цветовых гистограмм (автоуровни) заполненного контейнера была показана для больших значений амплитуды деформируемых блоков $\Delta \le 2$ (размер блока – 8×8, Гауссовая RBF-функция, τ=30). Вероятности ошибки восстановления для протестированного множества изображений с изменённой яркостью или прошедших нормализацию в среднем соответствовали представленным на рис. 4*б*, *г* значениям, вычисленным для неискажённых контейнеров. Следует отметить, что при малых значениях амплитуды деформации $\Delta \le 1$ после применения яркостной коррекции вероятность ошибочного восстановления устойчиво возрастала до 30 % и более.

Встроенные предложенным способом данные оказались неустойчивы к медианной фильтрации. Так, корректно восстановить встроенную информацию не удаётся ($\text{perr\_test}_{1,2} \approx 50\%$), после применения медианного фильтра со скользящей апертурой размером 3×3 пикселя к типовым контейнерам из тестовых наборов, имеющих 100% заполнение и сформированных для значений амплитуды деформации $\Delta_{\max} \le 2$, блоков размером 8×8 пикселей, Гауссовых RBF-функций, порога уровня градиента $\tau = 30$. Аналогичные результаты наблюдаются после применения низкочастотной пространственной фильтрации, реализуемой с помощью операции сглаживания. Даже в случае выбора малой размерности скользящей апертуры (3×3) незначительное размытие границ объектов на изображении приводит к нарушению локальной зависимости между составляющими градиента отдельных цветовых каналов в деформированных блоках контейнера, что делает невозможным дальнейшее корректное восстановление скрытых данных. Средние значения ошибки восстановления бинарного сообщения для «сглаженных» контейнеров, не участвовавших в обучении НС, с параметрами алгоритма: $\Delta_{\max} \le 2$, размером блока 8×8 пикселей, порогом уровня градиента $\tau = 30$, составили $\text{perr\_test}_{1,2} \approx 50\,\%$. Следует отметить, что увеличение размеров деформируемых блоков с одновременным увеличением значения амплитуды $\Delta_{\max}$ (в качестве возможного сценария повышения устойчивости к медианной и усредняющей фильтрации), на наш взгляд, не имеет практической ценности, поскольку получаемые в результате изображения будут иметь видимые артефакты на границах контрастных объектов, что противоречит базовым принципам стеганографии о визуальной незаметности скрытой информации.

Одним из основных ранее заявленных достоинств предложенной схемы ССИ является сохранение после встраивания информации большинства статистических характеристик контейнера, традиционно нарушаемых классическими стегоалгоритмами (распределения младших бит, частоты переходов битовых значений и т.п.). Для демонстрации устойчивости пред-

ложенного алгоритма к статистическим атакам, направленным на анализ классических алгоритмов ССИ, использовались критерий хи-квадрат [1], определяющий схожесть теоретических и эмпирических гистограмм цветовых компонент исследуемого контейнера, и разностный стегоанализ на основе двойной статистики (RS-метод) [24], оценивающий пространственные корреляции пикселей.

Для эксперимента были выбраны 15 тестовых контейнеров из [22, 23], в которые производилось встраивание случайных битовых последовательностей из расчёта 100 % их заполнения скрытыми данными. Рассматривались две реализации заполненных контейнеров, соответствующих двум вариантами значения амплитуды деформации $\Delta = 1$, $\Delta = 2$. Прочие параметры алгоритма скрытия: размер блока – 8×8, Гауссова RBF-функция, $\tau = 30$. В результате статистического стегоанализа тридцати полученных заполненных контейнеров критерий хи-квадрат и RS-метод не выявили присутствие скрытой информации. Для заполненных контейнеров эмпирические значения статистики хи-квадрат во всех случаях значительно превосходили теоретические для соответствующего числа степеней свободы и уровня значимости, что ошибочно подтверждает гипотезу об отсутствии ССИ. Для всех тестовых заполненных контейнеров в RS-методе вычисленные значения количества регулярных и сингулярных групп для отрицательной (R_{-M}, S_{-M}) и неотрицательной (R_M, S_M) маски отличались незначительно $R_{-M} \approx R_M$, $S_{-M} \approx S_M$ (примерно соответствовали значениям, вычисленным для незаполненных контейнеров), т.о. ошибочно подтверждая гипотезу о незаполненности.

На основании полученных результатов можно сделать вывод о том, что предложенный алгоритм ССИ является устойчивым к широко распространённым статистическим стегоаналитическим критериям, однако следует ожидать, что в перспективе можно будет предложить критерий, выявляющий нарушение корреляции цветовых компонент при определённых амплитудах деформации.

Заключение

Тестирование стегоалгоритма на разных изображениях показало, что практическая его применимость в значительной мере определяется типами и характером содержимого используемых графических контейнеров. Наилучшие результаты фиксируются для естественных полноцветных фотографических изображений. Подобные изображения в общем случае предполагают отсутствие искусственных влияний и артефактов, нарушающих линейную зависимость цветовых компонент в малых локальных областях. Безусловно, естественные шумы, например, вносимые матрицей фотоаппарата, будут иметь место, но, как показали эксперименты, принципиального влияния на качество алгоритма они не оказывают. Следует отметить, что реализация стеганографического скрытия в изображения векторной графики и прочие синтетические изображения (с нарушенной корреляцией цветовых каналов) в рамках предложенного подхода нецелесообразно.

С учётом проведённых предварительных экспериментов по исследованию устойчивости скрытой информации предлагаемый стегоалгоритм можно условно отнести к классу полухрупких. Необходимо также отметить обеспечиваемую за счёт нестандартной (не аддитивной или мультипликативной) природы стеганографического скрывающего преобразования устойчивость к специализированным статистическим стеганографическим атакам.

В качестве прочих достоинств предложенного в статье стегоалгоритма можно отметить сравнительно невысокую сложность процедур внедрения и детектирования, адаптируемость алгоритма под изображения-носители разного характера, возможность гибкой настройки параметров для уменьшения визуальной заметности результатов скрытия или повышения устойчивости встроенных данных к возможным трансформациям контейнера. К возможным недостаткам предложенного алгоритма следует отнести трудоёмкость процедуры предварительного обучения восстанавливающей информацию нейронной сети, невозможность корректной работы с некоторыми классами изображений (с явно невыраженной корреляцией цветовых компонент), а также неустойчивость скрытой информации к отдельным преобразованиям контейнера.

Благодарности

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 13-01-97507 р_центр_а.

Литература

1. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков. – М.: Солон-пресс, 2002. – 272 с. – ISBN / ISSN: 5-98003-011-5.
2. **Глумов, Н.И.** Алгоритм встраивания полухрупких цифровых водяных знаков для задач аутентификации изображений и скрытой передачи информации / Н.И. Глумов, В.А. Митекин // Компьютерная оптика. – 2011. – Т. 35, № 2. – С. 262-267. – ISSN 0134-2452.
3. Robust steganography using bit plane complexity segmentation / S.T. Maya, M.N. Miyatake, R.V. Medina // 1st International Conference on Electrical and Electronics Engineering, Mexico. – 2004. – P. 40-43.
4. A new steganography approach for image encryption exchange by using the least significant bit insertion / M.A.B. Younes, A. Jantan // International Journal of Computer Science and Network Security. – 2008. – P. 247-254.
5. Steganographic technique based on minimum deviation of fidelity (STMDF) / J.K. Mandal, M. Sengupta // 2nd International Conference on Emerging Applications of Information Technology (EAIT), Kolkata. – 2011. – P. 298-301.
6. Hide and seek: An introduction to steganography / N. Provos, P. Honeyman // IEEE Security Privacy. – 2003. – P. 32-44.
7. F5 – A steganographic algorithm: High capacity despite better steganalysis / A. Westfeld // Proceedings of 4th International Workshop Information Hiding, Springer-Verlag. – 2001. – P. 289-302.
8. A steganographic method based upon JPEG and particle swarm optimisation algorithm / X. Li, J. Wang // Information Sciences. – 2007. – Vol. 177(3). – P. 99-109.

9. Reversible image hiding algorithm based on pixels difference / H. Ren, C. Chang, J. Zhang // In the IEEE International Conference on Automation & Logistics, ICAL'09, Shenyang. – 2009. – P. 847-850.
10. Digital Watermarking Based on Neural Network Technology for Grayscale Images / J. Chen, Tung-Shou Chen, Keh-Jian Ma, Pin-Hsin Wang // Encyclopedia of Multimedia Technology and Networking. – 2005. – Vol. 29. – P. 204-212.
11. Digital watermarking based on neural networks for color images / Pao-Ta Yu, Hung-Hsu Tsai, Jyh-Shyan Lin // Signal Processing. – 2001. – Vol. 81(3). – P. 663-671.
12. Разработка методов обеспечения безопасности использования информационных технологий, базирующихся на идеях стеганографии: автореф. дис. канд. техн. наук : 05.13.17 / И.В. Нечта. – Новосибирск, 2012. – 21 с.
13. **Самойлин, Е.А.** Метод межканальной градиентной реконструкции / Е.А. Самойлин, В.В. Шипко // Цифровая обработка сигналов. – 2013. – № 3. – С. 13-16. – ISSN 1684-2634.
14. Mesh deformation based on radial basis function interpolation / A. de Boer, M.S. van der Schoot, H. Bijl // Computer and Structures. – 2007. – P. 784-795. – ISSN:0045-7949.
15. **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 ВГУ (системный анализ и информационные технологии). – 2013. – № 2. – С. 9-19. – ISSN 0234-5439. – ISSN 1995-5499.
16. Image metamorphosis using snakes and free-form deformations / S.Y. Lee, K.Y. Chwa, S.Y. Shin // SIGGRAPH '95: Proceedings of the 22nd annual conference on Computer graphics and interactive techniques, ACM Press, New York, NY, USA. – 1995. – P. 439-448.
17. Free-form deformation of solid geometric models / T.W. Sederberg, S.R. Parry // Proceedings of ACM SIGGRAPH 1986, ACM Press. – 1986. – P 151-160.
18. A two-dimensional interpolation function for irregularly-spaced data / D. Shepard // Proceedings of the 1968 23rd ACM National Conference. – 1968. – P. 517-524.
19. Principal warps: thin-plate splines and decomposition of deformations / F.L. Bookstein // IEEE Transactions on Pattern Analysis and Machine Intelligence. – 1986. – Vol. 11(6). – P. 567-585. – ISSN:0162-8828.
20. A thin plate spline method for mapping curves into curves in two dimensions / M.J.D. Powell // Computational Techniques and Applications (CTAC95), Melbourne, Australia. – 1995.
21. **Сизиков, В.С.** Устойчивые методы обработки результатов измерений. Учеб. пособие / В.С. Сизиков. – СПб.: СпецЛит, 1999. – 240 с.
22. Набор тестовых изображений «Kodak Lossless True Color Image Suite» [Электронный ресурс]. – URL: http://r0k.us/graphics/kodak/ (дата обращения 19.11.2014).
23. Набор тестовых изображений «TESTIMAGES» Электронный ресурс]. – URL: http://testimages.tecnick.com (дата обращения 19.11.2014).
24. Reliable detection of LSB steganography in color and grayscale images / J. Fridrich, M. Goljan, R. Du // Proc. of the ACM Workshop on Multimedia and Security, Ottawa, Canada. – 2001. – P. 27-30.

References

1. Digital steganography / V.G. Gribunin, I.N. Okov. – Moscow. "Solon-press" Publisher, 2002. – 272 p. – ISBN / ISSN: 5-98003-011-5. – (In Russian).
2. **Glumov, N.I.** Algorithm for embedding semi-fragile digital watermarks for the purpose of images authentication and secure communication / N.I. Glumov, V.A. Mitekin // Computer Optics. – 2011. – Vol. 35(2). – P. 262-267. – ISSN 0134-2452. – (In Russian).
3. Robust steganography using bit plane complexity segmentation / S.T. Maya, M.N. Miyatake, R.V. Medina // 1st International Conference on Electrical and Electronics Engineering, Mexico. – 2004. – P. 40-43.
4. A new steganography approach for image encryption exchange by using the least significant bit insertion / M.A.B. Younes, A. Jantan // International Journal of Computer Science and Network Security. – 2008. – P. 247-254.
5. Steganographic technique based on minimum deviation of fidelity (STMDF) / J.K. Mandal, M. Sengupta // 2nd International Conference on Emerging Applications of Information Technology (EAIT), Kolkata. – 2011. – P. 298-301.
6. Hide and seek: An introduction to steganography / N. Provos, P. Honeyman // IEEE Security Privacy. – 2003. – P. 32-44.
7. F5 – A steganographic algorithm: High capacity despite better steganalysis / A. Westfeld // Proceedings of 4th International Workshop Information Hiding, Springer-Verlag. – 2001. – P. 289-302.
8. A steganographic method based upon JPEG and particle swarm optimisation algorithm / X. Li, J. Wang // Information Sciences. – 2007. – Vol. 177(3). – P. 99-109.
9. Reversible image hiding algorithm based on pixels difference / H. Ren, C. Chang, J. Zhang // IEEE International Conference on Automation & Logistics, ICAL'09, Shenyang. – 2009. – P. 847-850.
10. Digital Watermarking Based on Neural Network Technology for Grayscale Images / J. Chen, Tung-Shou Chen, Keh-Jian Ma, Pin-Hsin Wang // Encyclopedia of Multimedia Technology and Networking. – 2005. – Vol. 29. – P. 204-212.
11. Digital watermarking based on neural networks for color images / Pao-Ta Yu, Hung-Hsu Tsai, Jyh-Shyan Lin // Signal Processing. – 2001. – Vol. 81(3). – P. 663-671.
12. Development of methods for the safe use of information technology, based on the ideas of steganography: technics dissertation abstract : 05.13.17 / I.V. Nechta. – Novosibirsk, 2012. – 21 P. – (In Russian).
13. **Samoilin, E.A.** Method of inter-channel gradient reconstruction / E.A. Samoilin, V.V. Shipko // Digital signal processing. – 2013. – Vol. 3. – P. 13-16. – ISSN 1684-2634. – (In Russian).
14. Mesh deformation based on radial basis function interpolation / A. de Boer, M.S. van der Schoot, H. Bijl // Computer and Structures. – 2007. – P. 784-795. – ISSN:0045-7949.
15. **Akimov, A.V.** Models and algorithms for image deformation using radial basis functions / A.V. Akimov, M.A. Dryuchenko, A.A. Sirota // Vestnik VSU (System Analysis and Information Technology). – 2013. – Vol. 2. – P. 9-19. – ISSN 0234-5439. – ISSN 1995-5499. – (In Russian).
16. Image metamorphosis using snakes and free-form deformations / S.Y. Lee, K.Y. Chwa, S.Y. Shin // SIGGRAPH '95: Proceedings of the 22nd annual conference on Computer graphics and interactive techniques, ACM Press, New York, NY, USA. – 1995. – P. 439-448.
17. Free-form deformation of solid geometric models / T.W. Sederberg, S.R. Parry // Proceedings of ACM SIGGRAPH 1986, ACM Press. – 1986. – P 151-160.
18. A two-dimensional interpolation function for irregularly-spaced data / D. Shepard // In Proceedings of the 1968 23rd ACM National Conference. – 1968. – P. 517-524.
19. Principal warps: thin-plate splines and decomposition of deformations / F.L. Bookstein // IEEE Transactions on Pattern Analysis and Machine Intelligence. – 1986. – Vol. 11(6). – P. 567-585. – ISSN:0162-8828.

20. A thin plate spline method for mapping curves into curves in two dimensions / M.J.D. Powell // Computational Techniques and Applications (CTAC95), Melbourne, Australia. – 1995.
21. Steady methods of processing measurements results / V.S. Sizikov. − Saint Peterburg: “SpecLit” Publisher, 1999. – 240 p. – (In Russian).
22. A set of test images «Kodak Lossless True Color Image Suite» [Electronic resource]. – URL: http://r0k.us/graphics/kodak/ (request date 19.11.2014).
23. A set of test images «TESTIMAGES» [Electronic resource]. – URL: http://testimages.tecnick.com (request date 19.11.2014).
24. Reliable detection of LSB steganography in color and gray-scale images / J. Fridrich, M. Goljan, R. Du // Proc. of the ACM Workshop on Multimedia and Security, Ottawa, Canada. – 2001. – P. 27-30.

STEGANOGRAPHY ALGORITHM FOR INFORMATION HIDING BASED ON SPATIAL DEFORMATION OF FULL-COLOR IMAGE FRAGMENTS

M.A. Dryuchenko, A.A. Sirota
Voronezh State University

Abstract

A steganography algorithm based on a relatively low-frequency spatial deformation of full color image fragments is considered. Correlation properties for the color channels of images are used for extraction of hidden data. Results of the algorithm application are presented.

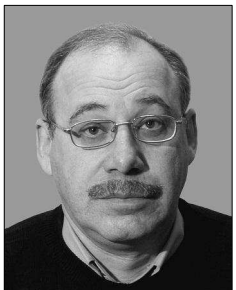
Key words: steganography information hiding, elastic deformation, radial basis functions.

Сведения об авторах

Дрюченко Михаил Анатольевич, 1985 года рождения, в 2007 году окончил Воронежский государственный университет по специальности «Прикладная математика и информатика». Доцент кафедры технологий обработки и защиты информации Воронежского государственного университета. Область научных интересов: компьютерная стеганография и стегоанализ, компьютерная обработка изображений, программирование.

E-mail: *m_dryuchenko@mail.ru* .

Mikhail Anatolievich Dryuchenko (1985) graduated from Voronezh State University in 2007, majoring in Applied Mathematics and Informatics. Currently docent of Information Processing and Security Technologies department of Voronezh State University. Research interests: steganography and steganalysis, computer graphics processing, programming.



Сирота Александр Анатольевич, 1954 года рождения, в 1976 году окончил Воронежский государственный университет по специальности «Радиофизика и электроника». Доктор технических наук (1995 год), профессор, заведует кафедрой технологий обработки и защиты информации Воронежского государственного университета. Область научных интересов: синтез и анализ систем сбора и обработки информации, методы и технологии компьютерного моделирования информационных процессов и систем, системный анализ в сфере информационной безопасности, компьютерная обработка изображений, нейронные сети и нейросетевые технологии в системах принятия решений.

Страница в интернете:
https://sites.google.com/a/sc.vsu.ru/tozi/sotrudniki-kafedry/sotrudniki-kafedry-tozi/sirota .

E-mail: *sir@cs.vsu.ru* .

Alexander Anatolievich Sirota (1954) graduated from Voronezh State University in 1976 majoring in “Radiophysics and Electronics”. Professor, Doctor of Technical Sciences (since 1995). Currently head of the Chair of Information Processing and Security Technologies department of Voronezh State University. Research interests: analysis and design of information collection and processing systems, methods and techniques of information processes and systems computer modeling, system analysis in information security, digital image processing, neural networks and neural network technologies in decision-making systems.

Поступила в редакцию 16 июля 2014 г.