

АНАЛИЗ УСТОЙЧИВОСТИ АЛГОРИТМОВ СОЗДАНИЯ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ С ИСПОЛЬЗОВАНИЕМ УНИВЕРСАЛЬНЫХ СЖИМАЮЩИХ ПРЕОБРАЗОВАНИЙ ПО ОТНОШЕНИЮ К НЕГАТИВНЫМ ВОЗДЕЙСТВИЯМ РАЗЛИЧНЫХ ВИДОВ

А. А. Сирота, Е. Ю. Митрофанова, М. А. Дрюченко

Воронежский государственный университет

Поступила в редакцию 29.07.2015 г.

Аннотация. Рассматриваются нейросетевые функциональные модели и алгоритмы преобразования информации, основанные на применении сжимающих преобразований универсального типа и обеспечивающие стеганографическое кодирования сообщений в форме цифровых водяных знаков (ЦВЗ) в произвольные объекты – контейнеры. Исследуется устойчивость алгоритмов создания цифровых водяных знаков при воздействии различных видов помех и преобразований, направленных на разрушение кодируемой информации.

Ключевые слова: нейронные сети, обработка изображений, стеганография, цифровые водяные знаки.

Annotation. The paper focuses on the functional neural network models and algorithms of data transformation based on the use of universal compression, performing steganographic message embedding in the form a digital watermark (DWM) into arbitrary objects – containers. The robustness of the digital watermarking algorithms to various transformations and distortions of the encoded information is considered.

Keywords: neural networks, image processing, steganography, digital watermarking.

ВВЕДЕНИЕ

Одной из ключевых проблем, возникающих при создании, хранении и передаче информации, является защита авторских прав на объекты цифрового (электронного) контента, обеспечение контроля их копирования, распространения и использования. В настоящее время для указанных целей могут использоваться технологии компьютерной стеганографии и, в частности, технологии цифровых водяных знаков (ЦВЗ) [1]. Для эффективного применения этих технологий необходимо выполнить ряд противоречивых требований, а именно: обеспечить аудио – и визуальную незаметность сообщений, отображаемых в ЦВЗ, сохранить исходное качество исходно-

го контейнера и, одновременно, обеспечить высокую достоверность извлечения ЦВЗ в условиях преднамеренных негативных воздействий – так называемых стеганографических атак. Указанные противоречия не снимаются в полной мере ни в одном из известных методов и алгоритмов создания ЦВЗ [1–4]. Одним из возможных подходов к дальнейшему развитию методов стеганографического скрытия информации (ССИ) является использование аппарата искусственных нейронных сетей (НС) [5–9]. При этом представляет интерес рассмотрение возможности построения алгоритмов создания ЦВЗ на основе универсальных нейросетевых функциональных моделей, реализующих сжимающие отображения информации и исследование их стойкости по отношению к типовым негативным воздействиям.

ОПИСАНИЕ АЛГОРИТМОВ СТЕГАНОГРАФИЧЕСКОГО СКРЫТИЯ ИНФОРМАЦИИ

Рассмотрим исходную постановку задачи. Пусть Z, D, K есть множества возможных контейнеров, скрываемых сообщений и ключей, тогда процедура встраивания и извлечения сообщения может быть представлена в виде отображений

$$F_* : Z \times D \times K \rightarrow Z,$$

$$\bar{z} = F_*(z, d, k), \quad z \in Z, \bar{z} \in Z, d \in D, k \in K,$$

$$\|z - \bar{z}\| \rightarrow \min,$$

$$F_{**} : Z \times K \rightarrow D,$$

$$\tilde{d} = F_{**}(\bar{z}, k), \quad \tilde{d} \in D, \|d - \tilde{d}\| \rightarrow \min,$$

где z, \bar{z} – исходный и заполненный контейнер; d, \tilde{d} – исходное и восстановленное сообщение. Далее в качестве контейнера без ограничения общности будем рассматривать реализацию случайного поля, заданного на двумерной дискретной сетке (как аналога изображения), а в качестве сообщения или ЦВЗ – двоичную последовательность $d^{(p)}$, $p = 1, P$, где $d^{(p)} \in \{-1, +1\}$ – скалярная величина, несущая один бит информации. Предполагается, что каждый элемент ЦВЗ $d^{(p)}$, $p = 1, P$ встраивается в собственный фрагмент контейнера $\Omega^{(p)}$, $p = 1, P$ произвольной формы, описываемый вектором $z^{(p)}$, $p = 1, P$. Совокупность фрагментов $\Omega^{(p)}$, $p = 1, P$ тем или иным способом покрывает контейнер.

Теоретические обоснования возможности построения этих отображений для ССИ на основе нейросетевых функциональных моделей и алгоритмов обработки информации основаны на результатах [9–11]. Применение нейросетевых функциональных моделей и

алгоритмов создания ЦВЗ связано с возможностью построения универсальных сжимающих отображений данных на основе линейных НС прямого распространения. При этом могут быть рассмотрены два типа преобразований: преобразования, реализующие гетероассоциативное сжимающее отображение, и преобразования, реализующие (как частный случай) автоассоциативное сжимающее отображение [12].

Архитектура нейронных сетей, которые могут быть использованы для сжатия данных, приведена на рис. 1а, где $z_1 \in R^{N_1}$ – входной вектор, $y = z_2 \in R^{N_2}$ – требуемый выходной целевой вектор. Особенностью архитектуры сети является использование сокращенного числа нейронов $M < N_1$, $M < N_2$ в скрытом слое по отношению к размерности входного и выходного векторов. При $z_1 \neq z_2$ сеть является гетероассоциативной, а при $z_1 = z_2$ – автоассоциативной [13].

Идея применения универсальных сжимающих отображений для встраивания ЦВЗ состоит в следующем. При использовании гетероассоциативного сжимающего отображения, как более общего случая, каждый фрагмент контейнера $\Omega^{(p)}$, используемый для встраивания элемента двоичной последовательности, разбивается на входную и выходную части. Соответственно, на вход нейронной сети, имеющей архитектуру, представленную на рисунке 1а и выполняющей сжатие, подаются данные из одной части фрагмента контейнера; при этом на выходе формируется оценка данных другой части фрагмента, которые затем и подвергаются модификации путем изменения амплитуды высокочастотной составляющей – собственного вектора, соответствующего минимальному собственному числу в

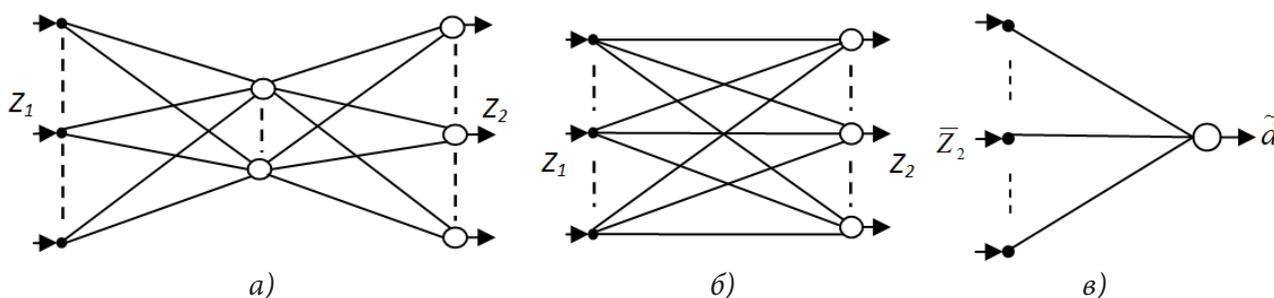


Рис. 1. Архитектура нейронных сетей

разложении оценки $\tilde{z}_{2/1}$. Это обеспечивает маскирование процесса встраивания, но требует использования дополнительно обученной нейронной сети, архитектура которой дана на рисунке 1б, определяющей корреляционные связи частей фрагмента для оценки (прогноза) значений данных выходной части фрагмента при известных значениях входной.

Область определения Ω (форма каждого фрагмента контейнера) при выполнении сжимающих отображений для изображений может быть произвольной конфигурации. На рис. 2 представлены примеры отображения конфигурации фрагментов, подвергаемых модификации: это области прямоугольной формы, решетки случайной конфигурации внутри области прямоугольной формы и т.п. Серым цветом выделены пиксели входной части фрагмента Ω_1 , белым цветом выделены пиксели выходной части фрагмента Ω_2 , в которой происходит встраивание элементов ЦВЗ.

На основе приведенных обоснований определена универсальная схема преобразования данных для встраивания и восстановления ЦВЗ в контейнерах графических и звуковых форматов данных. Требуется с использованием функциональных возможностей нейронных сетей для каждого фрагмента контейнера, представленного вектором $z \in R^N$, и встраиваемой последовательности данных $d \in R^1$ построить отображения

$$\begin{aligned} \tilde{z}_{2/1} &= F_c(z_1), \quad \tilde{z}_{2/1} = F_e(z_1), \\ \bar{z}_2 &= F_m(\tilde{z}_{2/1}, \tilde{z}_{2/1}, d) + (z_2 - \tilde{z}_{2/1}), \\ \|\bar{z}_2 - z_2\| &\rightarrow \min, \\ \tilde{d} &= F_d(\bar{z}_2), \quad \tilde{d} \in D, \quad \|d - \tilde{d}\| \rightarrow \min, \end{aligned} \quad (1)$$

где оператор F_c реализует приближенную

оценку (прогноз) значений данных выходной части фрагмента на основе сжимающего отображения при известной входной части; оператор F_e – оптимальную выборочную оценку значений данных выходной части фрагмента при известных значениях входной части и обеспечивает подготовку вектора-контейнера к встраиванию данных; оператор F_m – реализует модификацию выходной части при встраивании элементов ЦВЗ, состоящую в манипуляции амплитуды высокочастотной составляющей по закону, определяемому последовательностью $d^{(p)}$, $p = 1, P$; оператор F_d – выполняет декодирование (восстановление) ранее скрытого сообщения на основе классификации предъявляемого фрагмента контейнера для двух гипотез $H_1: d^{(p)} = -1$, $H_2: d^{(p)} = +1$.

Операторы F_c , F_e в общем случае могут быть реализованы на основе обучения нейронных сетей, архитектура которых приведена на рис. 1а, б. Обучение НС проводится по совокупности реализаций входного и целевого вектора $\{z_1^{(p)}, z_2^{(p)}\}$, $p = 1, P$, полученных от всех фрагментов контейнера. После обучения нейронных сетей, представленных на рис 1а, б, на их входы для каждого фрагмента подается вектор $z_1^{(p)}$, $p = 1, P$. Применение первой сети (оператор F_c , рис. 1а) обеспечивает выполнение индивидуального для данного набора данных сжимающее отображение с минимальной дисперсией ошибки. Вторая сеть (оператор F_e , рис. 1б) используется для точного прогнозирования выходной части фрагментов контейнера на основе соседних фрагментов контейнера в виде оценки $\tilde{z}_{2/1}^{(p)}$ и для определения стохастической составляющей прогноза.

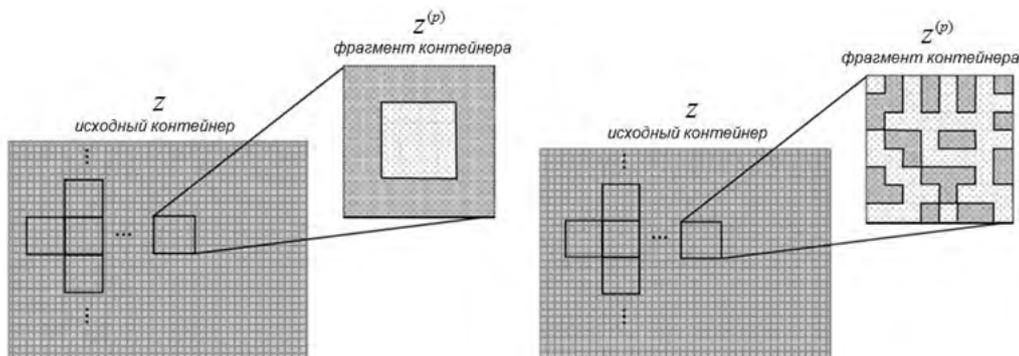


Рис. 2. Примеры конфигурации фрагментов, подвергаемых модификации

Для декодирования ЦВЗ используется оператор F_d , который может быть реализован на основе НС, архитектура которой показана на рис. 1в. Такая сеть обучается для решения задачи классификации входного для нее вектора с целью выделения значения ранее скрытого в нем элемента последовательности ЦВЗ. Можно показать, что для гауссовских случайных векторов в результате обучения однослойной линейной НС по совокупности $\{\bar{z}_2^{(p)}, d^{(p)}, p=1, P\}$ при $P \rightarrow \infty$ формируется преобразование входных данных в выходные, реализующее структуру оптимального решающего правила [12].

ИССЛЕДОВАНИЯ УСТОЙЧИВОСТИ АЛГОРИТМОВ

В [14, 15] показано, что разработанные нейросетевые модели и алгоритмы могут достаточно эффективно применяться для реализации универсальных схем скрытого встраивания пользовательской информации (допускающей незначительный процент возможных ошибок при ее восстановлении) в различные объекты цифрового контента, например, в цифровые изображения или аудиофайлы. На рис. 3а представлен пример исходного файла-контейнера, на рис. 3б представлен результирующий файл-контейнер, содержащий встроенный ЦВЗ, а на рис. 3в показана разность между исходным и заполненным контейнером с коэффициентом умножения 100 для обеспечения наглядности отображения.



Рис. 3. Исходный контейнер (а) и результирующий контейнер, содержащий встроенную последовательность ЦВЗ (б)

На рис. 4 представлена зависимость показателя уровня искажения контейнера от амплитуды встраиваемой последовательности в единицах уровня. На графике используются следующие обозначения: MseB-learn – показатель искажения при встраивании ЦВЗ для данных, используемых для обучения НС; MseB-test – показатель искажения при встраивании ЦВЗ на данных, не участвовавших в обучении НС. В данном случае для полноцветного изображения размером 1024×1024 использовался алгоритм, основанный на преобразовании автоассоциативного типа, с исходным размером фрагмента контейнера $N_1 = 8 \times 8$, имеющего прямоугольную форму. Вероятность правильного декодирования ЦВЗ для данного примера практически равна нулю. В качестве показателя уровня искажения контейнера использовался критерий Бовика [16] (Q_R, Q_G, Q_B), рассчитываемый для каждой из трех цветовых компонент исходного и результирующего изображения RGB на основе соотношения:

$$Q_R(Q_G, Q_B) = \frac{4 * \sigma_{xy} * \bar{x} * \bar{y}}{(\sigma_x^2 + \sigma_y^2) \left| (\bar{x})^2 + (\bar{y})^2 \right|}, \quad (2)$$

Результирующий показатель Q_{RGB} определялся как среднее геометрическое Q_R, Q_G, Q_B

$$Q_{RGB} = \sqrt[3]{Q_R Q_G Q_B}. \quad (3)$$

Полученные результаты, показывают эффективность рассмотренных алгоритмов. Однако до сих пор открытым оставался вопрос об их устойчивости в смысле возможности восстановления ранее скрытого ЦВЗ по отношению к негативным воздействиям на



Рис. 4. Зависимость показателя уровня искажения контейнера от амплитуды встраиваемой последовательности в единицах уровня

контейнер – стеганографическим атакам, направленным на разрушение ЦВЗ. Рассмотрим следующие типовые негативные воздействия, оказываемые на контейнер:

- центрированный белый гауссовский шум с фиксированной или относительной от уровня яркости дисперсией ν ;
- импульсный шум, реализующий подавление пикселей исходного изображения («соль и перец»);
- низкочастотная фильтрация на основе скользящего фильтра заданной апертуры;
- высокочастотная фильтрация на основе скользящего фильтра заданной апертуры;
- применение сжатия изображений на основе преобразование JPEG.

Оценка устойчивости рассмотренных алгоритмов создания ЦВЗ к различным негативным воздействиям, проводилась с использованием реальных объектов цифрового контента, при этом в качестве показателей устойчивости использовалась вероятность ошибки при восстановлении встроеного ЦВЗ в условиях воздействия на контейнер стеганографической атаки. При использовании алгоритма, основанного на применении автоассоциативного преобразования задавались: исходный размер фрагмента контейнера $N_1 = 8 \times 8$, имеющего прямоугольную форму. В случае использования алгоритма, основанного на применении гетероассоциативного преобразования задавались: исход-

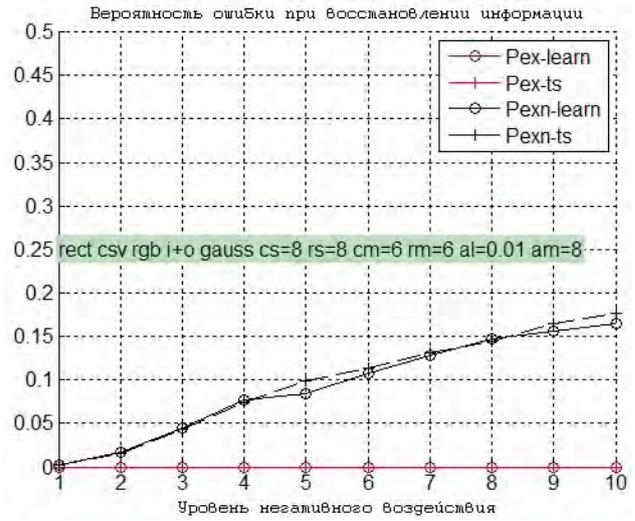
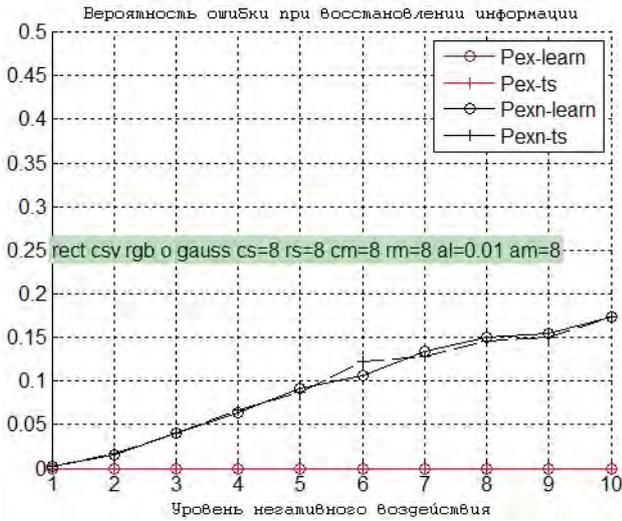
ный размер фрагмента контейнера $N_1 = 8 \times 8$, размер фрагмента, используемого для встраивания одного элемента последовательности ЦВЗ $N_2 = 6 \times 6$. На приведенных ниже графиках используются следующие обозначения: $P_{ex-learn}$ – оценка вероятности ошибки при восстановлении ЦВЗ (элемента двоичной последовательности ЦВЗ), при тестировании на данных, используемых для обучения, при отсутствии негативного воздействия; P_{ex-ts} – оценка вероятности ошибки при восстановлении ЦВЗ при тестировании на данных, не участвовавших в обучении, при отсутствии негативного воздействия; $P_{exn-learn}$ – оценка вероятности ошибки при восстановлении ЦВЗ, при тестировании на данных, используемых для обучения, после негативного воздействия; P_{exn-ts} – оценка вероятности ошибки при восстановлении ЦВЗ при тестировании на данных, не участвовавших в обучении, после негативного воздействия.

Центрированный белый гауссовский шум с фиксированной или относительной от уровня яркости дисперсией ν . Для проверки устойчивости к зашумлению в контейнер вносился центрированный белый гауссовский шум с нулевым средним значением и фиксированной дисперсией. В данном случае заполненный файл-контейнер $\bar{z}^{(p)}$, $p = \overline{1, P}$ модифицируется на основе следующего соотношения:

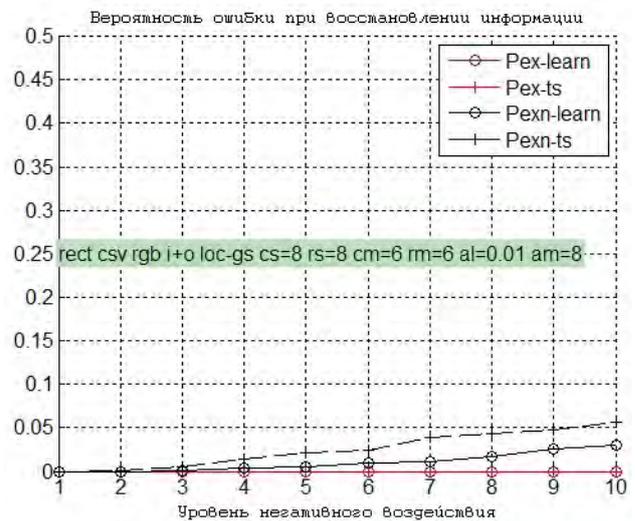
$$\bar{z}^{(p)} = \bar{z}^{(p)} + \sqrt{\nu} * N^{(p)}, \quad p = \overline{1, P}, \quad (4)$$

где $N^{(p)}$ – массив, элементами которого являются случайные величины, распределенные по нормальному закону с нулевым математическим ожиданием и среднеквадратическим отклонением, равным единице; ν – значение дисперсии шума; $\bar{z}^{(p)}$ – результирующий файл-контейнер после негативного воздействия. Под уровнем негативного воздействия в данном случае понимается значение варьируемого показателя K , определяющего градации значений используемой абсолютной или относительной дисперсии $\nu = K * 10^{-4}$.

На рис. 5 представлена зависимость вероятности ошибки восстановления элемента последовательности ЦВЗ от уровня негативного воздействия для преобразований автоассоциативного типа (а) и гетероассоциативного типа (б).



а) б)
Рис. 5. Вероятность ошибки при восстановлении ЦВЗ



а) б)
Рис. 6. Вероятность ошибки при восстановлении ЦВЗ

На рис. 6 представлены аналогичного вида зависимости вероятности ошибки при восстановлении ЦВЗ от уровня негативного воздействия для преобразований автоассоциативного типа (а) и гетероассоциативного типа (б) при задании относительной от уровня яркости I исходного контейнера (файл графического формата) дисперсии зашумления каждого пикселя $\nu = K * 10^{-4} * I$.

Анализ полученных зависимостей показывает весьма высокую стойкость предложенных алгоритмов ССИ по отношению к видам подобных шумовых воздействий.

Импульсный шум, реализующий подавление пикселей исходного изображения («соль и перец»). Под импульсным шумом

понимается искажение сигнала импульсами, т. е. выбросами с очень большими положительными или отрицательными значениями и малой длительностью. Выбросы шума особенно заметны на очень темных или очень светлых участках изображений. Существует две основные модели импульсного шума. В наиболее часто используемой модели «соль-перец» («salt-and-pepper») все выбросы шума имеют фиксированное значение. При этом данный тип шума представляет собой совокупность выбросов светлых и темных импульсов на изображении, его часто называют шумом типа Заполненный файл-контейнер $\bar{z}^{(p)}$, $p=1, P$ модифицируется на основе следующих соотношений:

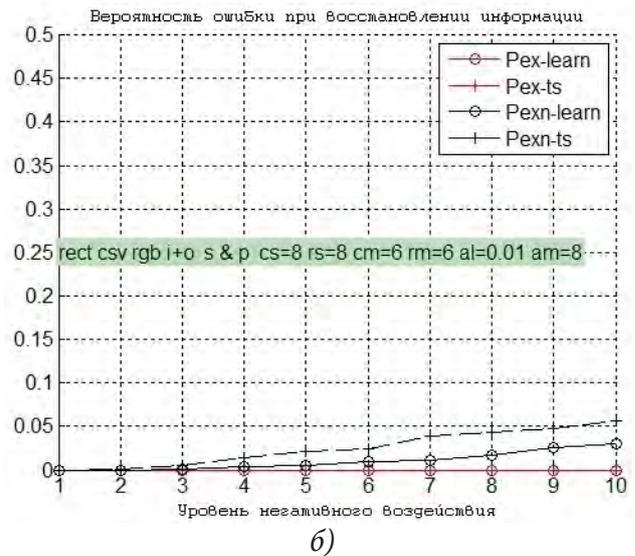
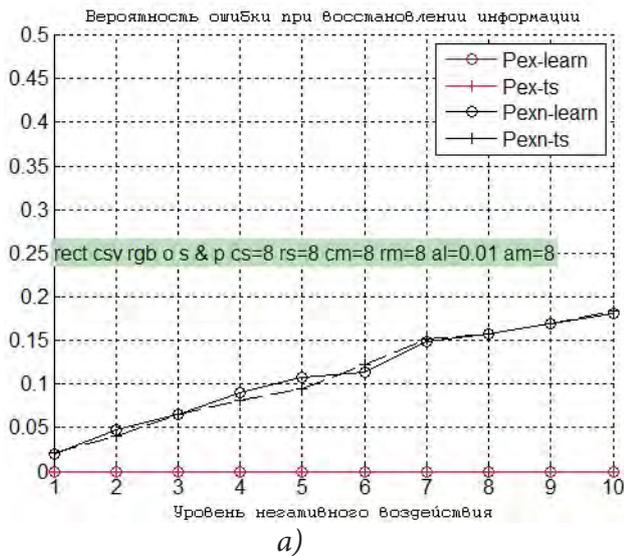


Рис. 7. Зависимость вероятности ошибки при восстановлении ЦВЗ

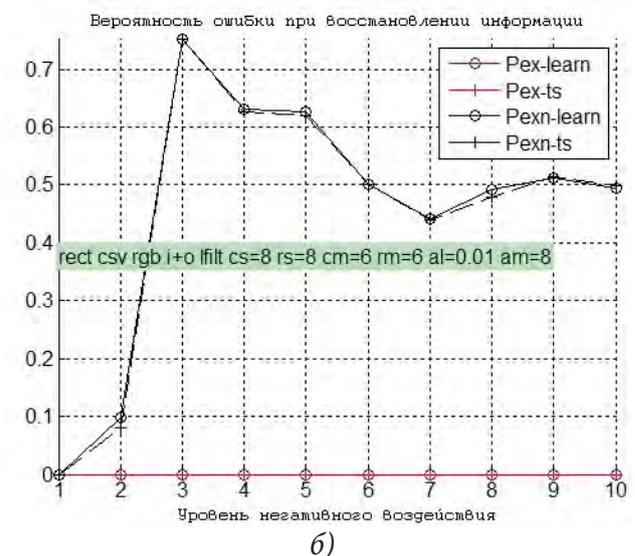
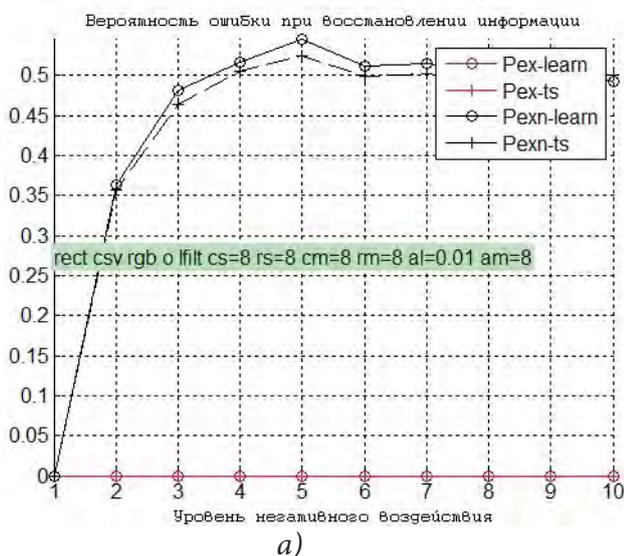


Рис. 8. Зависимость вероятности ошибки при восстановлении ЦВЗ

$$\bar{z}^{(p)} = \bar{z}^{(p)},$$

$$\begin{cases} R_{ij}^{(p)} < \nu/2, & \bar{z}_{ij}^{(p)} = 0, \\ R_{ij}^{(p)} \geq \nu/2, R_{ij}^{(p)} < \nu, & \bar{z}_{ij}^{(p)} = 1, \end{cases} \quad p = \overline{1, P}, \quad (5)$$

где $R^{(p)}$ – массив, элементами которого являются случайные величины, распределенные по равномерному закону в интервале (0, 1); ν плотность шума (относительная доля искаженных пикселей); $\bar{z}^{(p)}$ – результирующий файл-контейнер после негативного воздействия. При этом уровень негативного воздействия K , определяет плотность шума $\nu = K * 10^{-3}$ и соответственно долю искаженных пикселей $d = \nu * 100 \%$.

На рис. 7 представлена зависимость вероятности ошибки при восстановлении ЦВЗ

от уровня негативного воздействия для преобразований автоассоциативного типа (а) и гетероассоциативного типа (б). Анализ полученных зависимостей показывает весьма высокую стойкость предложенных алгоритмов ССИ по отношению ко всем видам шумовых воздействий.

Низкочастотная фильтрация на основе скользящего фильтра заданной апертуры. Низкочастотная фильтрация осуществляется путем двумерной свертки матрицы изображения с весовой маской фильтра. Негативное воздействие усредняющим низкочастотным фильтром, с заданным размером апертуры (маски) $[m, n]$, предназначенным для фильтрации высокочастотного шума сопровожда-

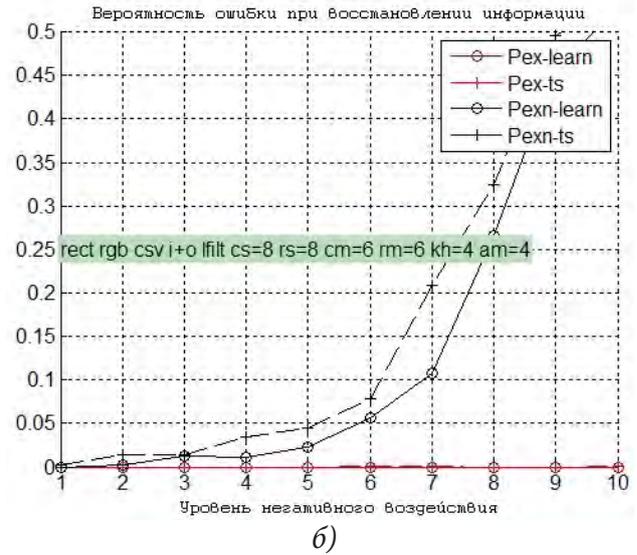
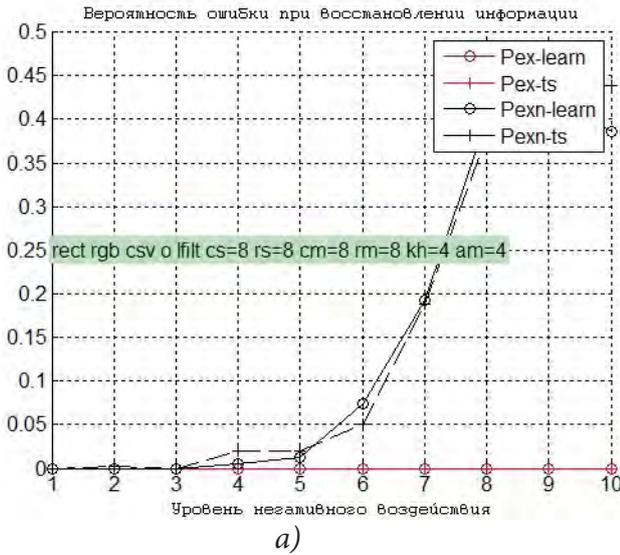


Рис. 9. Зависимость вероятности ошибки при восстановлении ЦВЗ

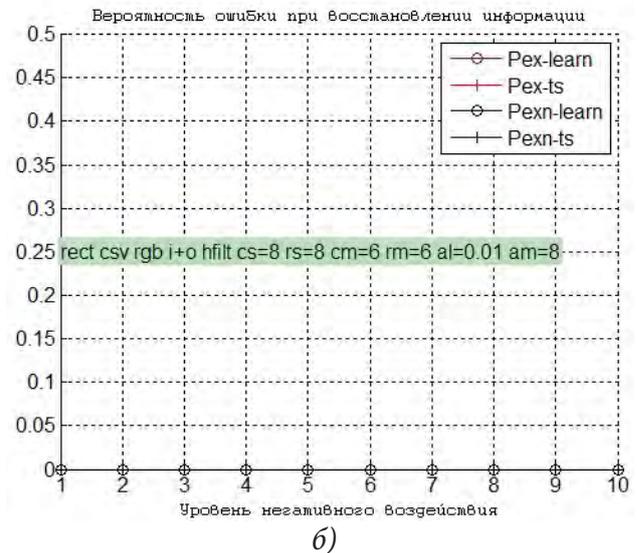
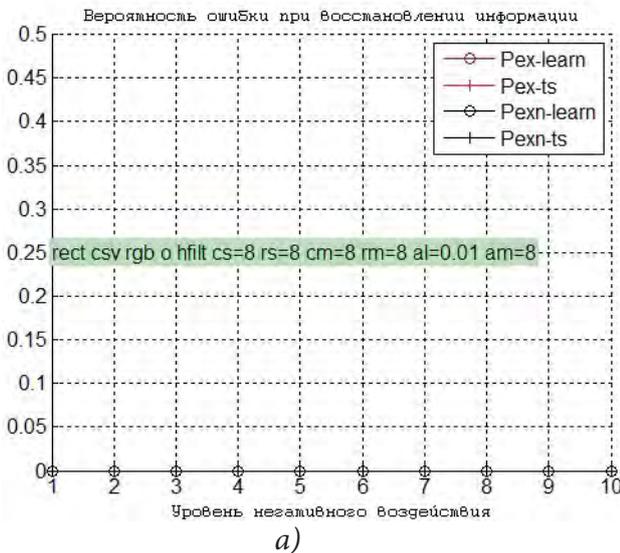


Рис. 10. Зависимость вероятности ошибки при восстановлении ЦВЗ

ется размыванием исходного изображения $z^{(p)}$, $p = 1, P$ (файла-контейнера). При этом каждый элемент маски равен $1/m * n$, где m и n размеры маски (количество строк и столбцов). При этом уровень негативного воздействия определяет размер маски фильтра $K = \max(m, n)$.

На рис. 8 представлена зависимость вероятности ошибки при восстановлении ЦВЗ от уровня негативного воздействия для преобразований автоассоциативного типа (а) и гетероассоциативного типа (б). Здесь, очевидно, мы видим существенное снижение вероятности восстановления ЦВЗ при осуществлении низкочастотного сглаживания изображения, ранее встроенные ЦВЗ при воздействии на

заполненный контейнер низкочастотным фильтром с размером маски более 3 пикселей разрушаются.

Для борьбы с подобными воздействиями предложена следующая модификация алгоритма. Она основана на переходе от модификации значений отдельных пикселей фрагмента к модификации средних яркости групп рядом стоящих пикселей фрагментов файла-контейнера, образующих блоки размером $kh \times kh$ ($kh = 4, kh = 8$). При этом исходный файл-контейнер $z^{(p)}$ $p = 1, P$ последовательно разбивается на блоки $b_{ij}^{(r,g,b)}$ размером $kh \times kh$ по каждой из трех цветовой компонент. Исходное изображение представляется в виде матриц таких блоков $B^{(r,g,b)} = \left\| b_{ij}^{(r,g,b)} \right\|$,

$i = \overline{1, I}, j = \overline{1, J}$ для каждой из цветовой компонент, где I, J – количества полученных блоков по оси OX и по оси OY . Далее по отношению к полученному таким образом изображению реализуется стандартный алгоритм встраивания и восстановления ЦВЗ.

На рис. 9 представлены полученные зависимости вероятности ошибки при восстановлении информации для преобразований автоассоциативного (а) и гетероассоциативного (б) типа для блока размером $kh \times kh$ при $kh = 4$. Полученные результаты свидетельствуют о возможности применения рассмотренной модификации алгоритма встраивания ЦВЗ для эффективной борьбы с низкочастотной фильтрацией.

Высокочастотная фильтрация на основе скользящего фильтра заданной апертуры. В случае воздействия высокочастотной фильтрацией на исходный файл контейнер, используется маска фильтра, повышающая резкость изображения, и определяется следующим соотношением:

$$h = \frac{1}{(1+\alpha)} \begin{bmatrix} -\alpha & \alpha-1 & -\alpha \\ \alpha-1 & \alpha+5 & \alpha-1 \\ -\alpha & \alpha-1 & -\alpha \end{bmatrix}, \quad (6)$$

где α – параметр в диапазоне $[0,1]$, управляющий соотношением между центральным и граничным элементами маски (размер маски 3×3). При этом под уровнем негативного воздействия понимается размер маски фильтра. На рис. 10 представлена зависимость вероятности ошибки при восстановлении одного бита встраиваемой информации от уровня негативного воздействия для преобразований автоассоциативного (а) и гетероассоциативного типа (б).

Полученные результаты показали, что воздействие высокочастотной фильтрации не оказывает влияния на достоверность восстановления ранее скрытых данных.

Применение сжатия изображений на основе преобразование JPEG. Представляет интерес и исследование устойчивости ЦВЗ при воздействии сжатием в стандарте JPEG. При сжатии изображений по стандарту JPEG отмечается появление на восстановленных изображениях при высоких степенях сжатия

характерных артефактов: изображение рассыпается на блоки размером 8×8 пикселей (этот эффект особенно заметен на областях изображения с плавными изменениями яркости), в областях с высокой пространственной частотой (например, на контрастных контурах и границах изображения) возникают артефакты в виде шумовых ореолов. При применении преобразования JPEG, также как и при борьбе с низкочастотной фильтрацией, используется ранее описанный модифицированный алгоритм встраивания ЦВЗ, основанный на усреднении групп пикселей; при этом размер фрагмента файла-контейнера задается кратным 8 ($kh = 8, kh = 16$). Кроме того, для обеспечения устойчивости ЦВЗ предварительно необходимо выполнить линейное преобразование, переводящее исходное полноцветное изображение из формата RGB в формат YCbCr:

$$\begin{bmatrix} Y \\ Cb \\ Cr \end{bmatrix} = \begin{bmatrix} 16 \\ 128 \\ 128 \end{bmatrix} + \begin{bmatrix} 65.481 & 128.553 & 24.966 \\ -37.797 & -74.203 & 112.0 \\ 112.0 & -93.784 & -18.214 \end{bmatrix} \times \begin{bmatrix} R \\ G \\ B \end{bmatrix}. \quad (7)$$

В данном случае под уровнем негативного воздействия понимается значение показателя K , определяющего уровень качества изображения после сжатия на основе преобразования JPEG $q = 100 - 10 * (K - 1)$. Значение $q = 100$ соответствует самому высокому качеству при отсутствии сжатия. Значение $q < 75$ т. е. $K > 4$ свидетельствует о существенной потере качества изображения при сжатии.

На рис. 11 представлены зависимости вероятности ошибки при восстановлении одного бита встраиваемой информации от уровня негативного воздействия для преобразований автоассоциативного типа (а) и гетероассоциативного типа (б).

В целом, полученные результаты свидетельствуют об устойчивости разработанных алгоритмов в смысле возможности восстановления ранее скрытого ЦВЗ по отношению к негативным воздействиям на контейнер, в том числе, при определенных модификациях, и к преобразованиям низкочастотной фильтрации и сжатия с высокой степенью потери качества изображения.

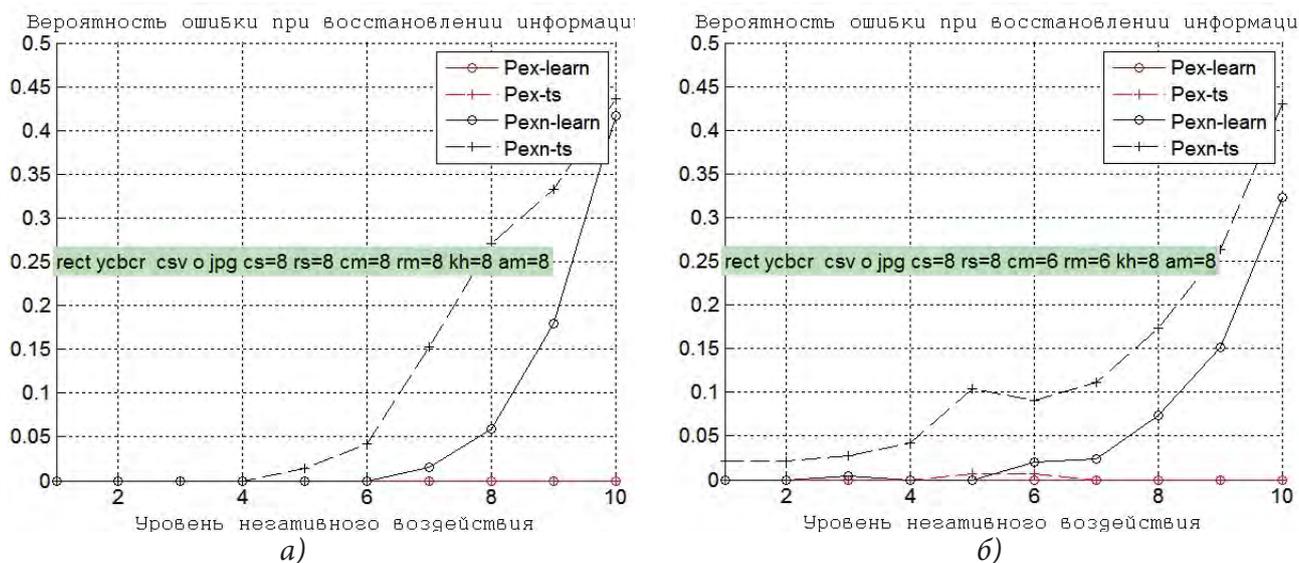


Рис. 11. Зависимость вероятности ошибки при восстановлении ЦВЗ

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

СПИСОК ЛИТЕРАТУРЫ

1. Бахрушин А. П. Спектральный анализ видеокадров на основе системы импульсных функций с целью синхронизации процессов внедрения и поиск цифровых водяных знаков / А. П. Бахрушин // Вестник Тихоокеанского государственного университета. – 2008. – № 4. – С. 225–238.
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. Хорошко В. А. Методы и средства защиты информации / В. А. Хорошко, А. А. Чекатов. – К. : Юниор, 2003. – 504 с.
5. Kavitha V. Neural based steganography / V. Kavithal, K. S.Easwarakumar // PRICAI 2004 : Trends in Artificial Intelligence, 8th Pacific Rim International Conference on Artificial Intelligence. – 2004. – Vol. 3157. – P. 429–435.
6. Chang C. Using Counter-propagation neural network for robust digital audio watermarking in DWT domain / C. Chang, W. Shen, H. Wang //

Systems, Man and Cybernetics (SMC). IEEE International Conference on . – 2006. – Vol. 2. – P. 1214–1219.

7. Сирота А. А. Нейросетевые модели и алгоритмы стеганографического скрывания информации / А. А. Сирота, М. А. Дрюченко // Информационные технологии. – 2011. – № 3. – С.41–49.

8. Сирота А. А. Нейросетевые технологии создания скрытых цифровых водяных знаков / А. А. Сирота, М. А. Дрюченко, Е. Ю. Митрофанова // Нейрокомпьютеры: разработка и применение. – 2012. – № 10. – С. 13–20.

9. Сирота А. А. Сходимость весов двухслойной линейной нейронной сети при построении оптимальных оценок случайных векторов / А. А. Сирота, Е. Ю. Митрофанова // Нейрокомпьютеры: разработка и применение. – 2011. – № 7. – С. 39–48.

10. Сирота А. А. Восстановление регрессионных моделей случайных процессов и полей с использованием нейронных сетей / А. А. Сирота, М. А. Дрюченко, Е. В. Воронова // Вестник Воронежского государственного университета. Системный анализ и информационные технологии. – 2009. № 1. – С. 109–119.

11. Кирсанов Э. А. Обработка информации в пространственно-распределенных системах радио мониторинга: статистический и нейросетевой подход / Э. А. Кирсанов, А. А. Сирота. – М. : Физматлит, 2012. – 344 с.

12. *Сирота А. А.* Нейросетевые функциональные модели и алгоритмы преобразования информации для создания цифровых водяных знаков / А. А. Сирота, Д. А. Дрюченко, Е. Ю. Митрофанова // Известия вузов. Радиэлектроника. – 2015. – Т. 1. № 1. – С. 3–16.

13. *Осовский С.* Нейронные сети для обработки информации / С. Осовский. – М. : Финансы и статистика, 2002. – 344 с.

14. *Сирота А. А.* Нейросетевые алгоритмы создания цифровых водяных знаков на основе гетероассоциативных сжимающих преобразование / А. А. Сирота, Д. А. Дрюченко, Е. Ю. Митрофанова // Сборник трудов Международной научно-технической конференции «Кибернетика и технологии XXI

века (С&Т 2014г.). – Воронеж, 2014. – Т. 1. – С. 68–78.

15. *Сирота А. А.* Анализ стойкости алгоритмов создания цифровых водяных знаков на основе универсальных сжимающих преобразований по отношению к типовым стеганографическим атакам / А. А. Сирота, Д. А. Дрюченко, Е. Ю. Митрофанова // Сборник трудов Международной научно-технической конференции «Кибернетика и технологии XXI века (С&Т 2015г.). – Воронеж, 2015. – С. 57–68.

16. *Приоров А. Л.* Цифровая обработка изображений: учебное пособие /А. Л. Приоров, И. В. Апальков, В. В. Хрящев; Яросл. гос. ун-т. – Ярославль : ЯрГУ, 2007. – 235 с.

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

Митрофанова Е. Ю. – к.т.н., ассистент кафедры Технологий обработки и защиты информации, факультет компьютерных наук, Воронежский государственный университет. E-mail: mitrofanova@cs.vsu.ru

Дрюченко М.А. – к.т.н., доцент кафедры Технологий обработки и защиты информации, факультет компьютерных наук, Воронежский государственный университет. E-mail: mitrofanova@cs.vsu.ru

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

Mitrofanova E. Yu. – Candidate of Technical Sciences, Assistant of Department of Processing Technology and Information Security, Computer Sciences Faculty, Voronezh State University. E-mail: mitrofanova@cs.vsu.ru

Dryuchenko M. A. – Candidate of Technical Sciences, Associate Professor at the Department of Processing Technology and Information Security, Computer Sciences Faculty, Voronezh State University. E-mail: dryuchenko@cs.vsu.ru