Доклады БГУИР
2004 *октябрь–декабрь* *№ 4*

ИНФОРМАТИКА

УДК 681.3:519.246

СИСТЕМА СКРЫТОЙ ПЕРЕДАЧИ ЦИФРОВЫХ ПОЛУТОНОВЫХ ИЗОБРАЖЕНИЙ НА БАЗЕ КОМПЛЕКСНОГО ПРЕОБРАЗОВАНИЯ BIFORE

И.А. РЕЗНИК, Р.Х. САДЫХОВ

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

Объединенный институт проблем информатики НАН Беларуси
Сурганова 6, Минск, 220072, Беларусь

Поступила в редакцию 16 августа 2004

В данной работе рассмотрена система скрытой передачи информации. Предложен модифицированный алгоритм сокрытия полутоновых изображений в полутоновых картинках. Стеганографическая система основана на модели двумерного пространственного коррелятора в базисе комплексного преобразования BIFORE. В качестве функции фильтра данного коррелятора используется секретный ключ. Рассмотрены вопросы эффективности, устойчивости, точности и быстродействия предложенного метода.

Ключевые слова: стеганография, сокрытие информации, комплексное преобразование BIFORE.

Введение

Одним из способов защиты от несанкционированного доступа к конфиденциальным данным является сокрытие информации.

В силу того что в последнее время резко возрос объем информации, передаваемой в глобальных сетях общего пользования и требующей авторизованного доступа, все большее развитие и распространение получают компьютерные стеганографические системы. Стеганография — наука о сокрытии самого факта наличия секретной информации. Достаточно активно ведутся работы в области цифровой стеганографии. Основные задачи цифровой стеганографии — изучение и разработка методов встраивания одних данных в другие с применением методов цифровой обработки сигналов. Основные направления стеганографии [2]: внедрение водяных знаков (*watermarking*), встраивание заголовков (*captioning*), идентификационных номеров, а также скрытая передача информации.

В данной работе предлагается система скрытой передачи полутоновых изображений в полутоновых цифровых картинках. Рассмотрим основные понятия предложенной стеганографической системы. Скрытое изображение — полутоновое изображение, требующее защиты от несанкционированного доступа к нему. Изображение-контейнер – полутоновое изображение, в которое встраивается скрытое. Стего-изображение – контейнер с внедренной в него скрытой картинкой. Секретный ключ — ключевая функция, при помощи которой встраивается и извлекается скрытое изображение. Стего-система должна позволять незаметно для невооруженного глаза встраивать скрываемую информацию в контейнер и извлекать ее оттуда. Из самого определения стего-системы следует, что стего-изображение должно незначительно отличаться

от изображения-контейнера. Для этого используется визуальная избыточность формата хранения графической информации.

Также следует отметить, что в последнее время в системах информационной безопасности активно внедряются методы и алгоритмы, заимствованные из оптических технологий [3, 7–9]. Использование оптических технологий предоставляет в основном два типа преимуществ: 1) возможность параллельной обработки информации; 2) сокрытие информации может осуществляться как в пространственном домене, так и в Фурье домене, что предоставляет отличные возможности для кодирования информации [6].

В силу всех вышеперечисленных факторов в качестве ядра нашей стеганографической системы выбрана цифровая модель двумерного пространственного коррелятора [1]. На основе данного коррелятора разработан метод, позволяющий внедрять скрытое изображение в изображение-контейнер и извлекать его из стего-изображения с минимальными потерями качества, затрачивая на эти операции достаточно мало времени. В отличие от классического пространственного коррелятора, вычисление корреляций в котором основаны на комплексном преобразовании Фурье (КПФ), в предлагаемой стего-системе используется пространственный коррелятор в базисе комплексного преобразования BIFORE (КПБ). Выбор данного комплексного преобразования обусловлен более высокой вычислительной скоростью по сравнению с КПФ.

В качестве пространственного фильтра рассматриваемого коррелятора используется ключевая функция (секретный ключ стего-системы).

Комплексное преобразование BIFORE

Понятие двоичного представления Фурье или BIFORE (BInary FOurier REpresentation) было введено в работе [10]. Также в литературе данное преобразование упоминается как преобразование Адамара или Уолша–Адамара.

Комплексное преобразование BIFORE (КПБ) относится к семейству дискретных ортогональных преобразований [11]. В отличие от преобразования Фурье, базисом которого является набор синусоид с частотами гармоник, преобразование Адамара базируется на функциях Уолша [12]. Так как функции Уолша — прямоугольные колебания, они принимают только два значения "–1" и "+1". Сравнительная простота прямоугольных колебаний по отношению к синусоидам позволяет относительно легко обрабатывать информацию. КПБ наиболее пригодно для обработки комплексных информационных функций, а также обеспечивает определенные выгоды, связанные с методом вычислений [13]. В силу всех этих факторов выбор комплексного преобразования для вычисления корреляций в нашей работе был остановлен на КПБ.

Рассмотрим подробнее КПБ. Квантование функций Уолша, соответствующих синусоидам Фурье, в N выборочных точках на интервале $(0;1)$ дает в результате двумерный массив размера $N \times N$, состоящий из "–1" и "+1". Строки массива, полученного таким способом, могут быть перегруппированы к частному виду матрицы Адамара — $H(n)$, где $N = 2^n$ [12]. Например, для $n = 3$:

$$\left[H(3)\right] = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix}. \qquad (1)$$

Нетрудно заметить, что матрица Адамара любого порядка может быть рекурсивно сгенерирована следующим образом:

$$\begin{aligned}&[H(0)]=[1]\\&[H(k+1)]=\begin{bmatrix}[H(k)] & [H(k)]\\ [H(k)] & -[H(k)]\end{bmatrix}.\end{aligned} \quad (2)$$

Для комплексного случая матрицы преобразования генерируются следующим образом [14]:

$$\begin{aligned}&[M(0)]=1\\&[M(1)]=[H(1)]\\&[M(n)]=\begin{bmatrix}[M(n-1)] & [M(n-1)]\\ [L(1)]\otimes[H(n-2)] & -[L(1)]\otimes[H(n-2)]\end{bmatrix}\end{aligned}, \quad (3)$$

где $\otimes$ обозначает кронекеровское произведение, а $[L(1)]=\begin{bmatrix}1 & -i\\ 1 & i\end{bmatrix}$.

Таким образом, КПБ функции $x(n)$ и его обратное преобразование (ОКПБ) соответственно определяются как

$$\{X(n)\}=\frac{1}{N}[M(n)]\{x(n)\}, \quad (4)$$

$$\{x(n)\}=[M^*(n)]^T\{X(n)\}, \quad (5)$$

где операция * обозначает комплексное сопряжение матрицы, а T — транспонирование матрицы. Сигнальные графы КПБ и ОКПБ для случая $n=3$ приводятся на рис. 1 и 2 соответственно.

Для вычисления КПБ требуется выполнить $N\cdot log_2 N$ арифметических операций, причем каждая операция представляет собой комплексное сложение. Как известно, для вычисления КПФ также требуется $N\cdot log_2 N$ арифметических операций, но поскольку в качестве базиса преобразования используется набор синусоид Фурье, каждая арифметическая операция помимо комплексного сложения включает в себя еще и умножение, что значительно замедляет алгоритм быстрого преобразования Фурье по сравнению с быстрым преобразованием BIFORE.

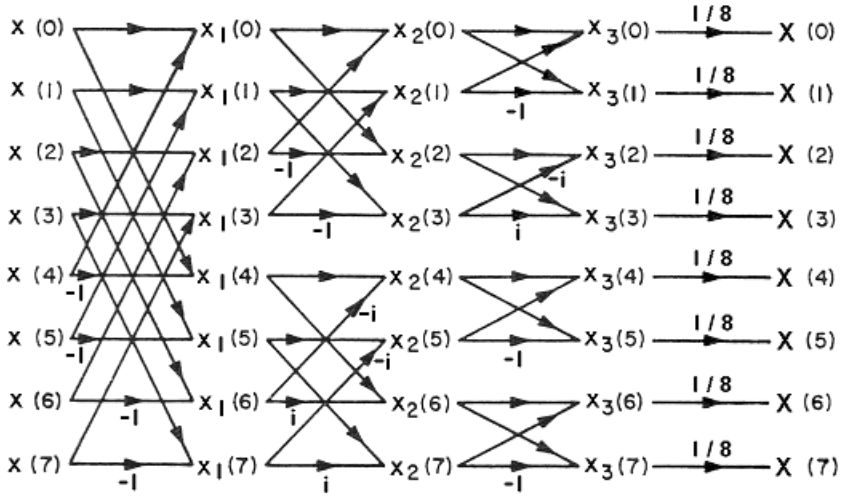

Рис. 1. Сигнальный граф, отображающий КПБ для $n = 3$

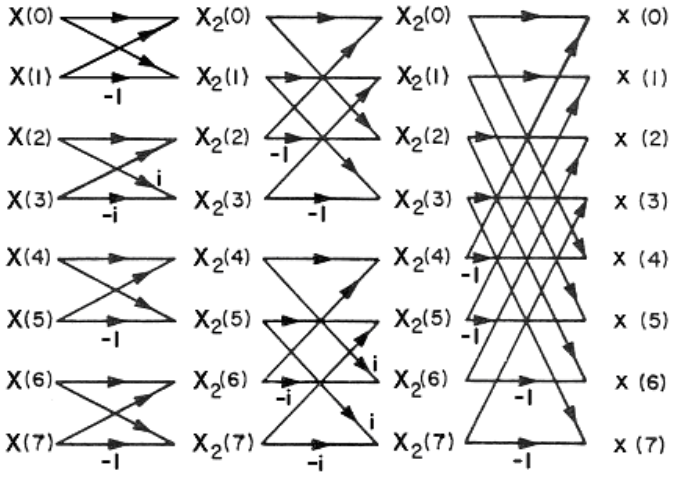

Рис. 2. Сигнальный граф, отображающий ОКПБ для $n = 3$

Двумерный пространственный коррелятор в базисе КПБ

Двумерный пространственный коррелятор описывается тремя плоскостями: входной, пространственно-частотной и выходной. Изображение-контейнер обозначается $c(x, y)$ и рассматривается во входной плоскости коррелятора. Скрываемое изображение обозначается $h(x, y)$ и рассматривается в выходной плоскости. Также определяется функция фильтра $K(u,v)$, которая ссылается на ключевую функцию и отображается в пространственно-частотной плоскости. В целях стабильности алгоритма $K(u,v)$ — чисто-фазовая функция вида $K(u,v) = e^{i\phi(u,v)}$, где $\phi(u,v)$ — случайная функция, равномерно распределенная на интервале $(-\pi, \pi)$ [4].

Входная плоскость коррелятора описывается комплексной функцией $a(x, y)$, амплитуда которой равна функции контейнера $c(x, y)$, а фаза обозначается функцией $\theta(x, y)$, т.е. $a(x, y) = c(x, y)e^{i\theta(x,y)}$. Требуется найти такую функцию $\theta(x, y)$, чтобы, пропустив через коррелятор функцию $a(x, y)$, получить на выходе комплексную функцию с амплитудой, равной скрытому изображению $h(x, y)$.

Обозначим комплексную функцию, описывающую выходную плоскость коррелятора $b(x,y)$, тогда $b(x,y)=h(x,y)e^{i\varphi(x,y)}$, где $\varphi(x,y)$ — фаза выходной функции. Следовательно, выходную корреляционную функцию можно представить в виде

$$b(x,y)=\hat{I}\hat{E}\ddot{I}\acute{A}\quad\left[\hat{E}\ddot{I}\acute{A}\ \{a(x,y)\}K(u,v)\right], \tag{6}$$

где *КПБ* и *ОКПБ* – операторы комплексного преобразования BIFORE и обратного комплексного преобразования BIFORE соответственно. Из уравнения (6) входная функция выражается как

$$a(x,y)=\hat{I}\hat{E}\ddot{I}\acute{A}\quad\left[\hat{E}\ddot{I}\acute{A}\ \{b(x,y)\}K^{*}(u,v)\right], \tag{7}$$

где $K^{*}(u,v)$ — комплексно-сопряженное $K(u,v)$.

Для вычисления фазовой функции $\theta(x,y)$ применяется алгоритм ПНМО "проекция на множество ограничений". В работе [4] описана его версия, оптимизированная для работы с корреляциями. Указанный итеративный алгоритм основан на преобразовании между двумя доменами.

В начале алгоритма функция $\theta(x,y)$ инициализируется случайным образом. На каждой итерации $a(x,y)$ преобразуется, согласно корреляции, описанной в (6), в выходную функцию $b(x,y)$, а затем обратно, согласно корреляции, описанной в (7). На каждой итерации в каждом из доменов полученные функции проецируются на множество ограничений. Во входном домене множество ограничений выражает вероятность получения изображения-контейнера $c(x,y)$, в выходном — скрываемого изображения $h(x,y)$.

В выходной плоскости проекция P_1 на множество ограничений на *j*-й итерации выражается как

$$P_1\left[b_j(x,y)\right]=\begin{cases}h(x,y)e^{i\varphi_j(x,y)}, \text{åñëè}\,(x,y)\in W\\ b_j(x,y), \text{èíà÷å},\end{cases} \tag{8}$$

где *W* — окно, содержащее скрытое изображение (оно должно быть меньше размера контейнера [6]). Проекция P_2 на множество ограничений на *j*-й итерации выражается как

$$P_2\left[a_j(x,y)\right]=c(x,y)e^{i\theta_j(x,y)}. \tag{9}$$

Сходимость алгоритма оценивается среднеквадратичными ошибками, вычисляемыми на каждой итерации при проецировании в обоих доменах [5]. Для выходного домена, согласно (8):

$$e_{b_j}=\frac{1}{D_W{}^2}\sum_x\sum_y\left|h(x,y)-\left|b_j(x,y)\right\|^2. \tag{10}$$

Для входного домена, согласно (9):

$$e_{a_j}=\frac{1}{D^2}\sum_x\sum_y\left|c(x,y)-\left|a_j(x,y)\right\|^2, \tag{11}$$

где $D\times D$ — размер изображения-контейнера, $D_W\times D_W$ — размер скрытого изображения.

Алгоритм продолжает повторяться до тех пор, пока ошибки e_{b_j} и e_{a_j} не станут достаточно малы. Необходимые условия сходимости этих ошибок следующие:

Коррелятор должен быть энергетически стабильным.

Из всех функций множества ограничений на *j*-й итерации P_1 и P_2 наиболее точно описывают b_j и a_j соответственно.

Доказательство выполнения обоих этих условий представлено в работе [4].

Следует заметить, что функция $K(u,v)$ генерируется один раз в начале итерационного процесса и далее не изменяется. Она является частью коррелятора и никоим образом не зависит от кодируемых изображений. Более того, $K(u,v)$ можно рассматривать как обобщенное среднее между функциями b_j и a_j.

Алгоритм заканчивается на *n*-й итерации, когда среднеквадратичные ошибки (10) и (11) снизятся по отношению к среднеквадратичным значениям исходных изображений до некоторого порога (%), Данный порог должен обеспечивать достаточное приближение амплитуды $|b_n(x,y)|$ к скрываемому изображению $h(x,y)$, и амплитуды $|a_n(x,y)|$ к $c(x,y)$. Среднеквадратичные значения исходных изображений рассчитываются соответственно как

$$c_{\text{ñð}} = \frac{1}{D^2}\sum_x\sum_y \tilde{n}^2(x,y), \tag{12}$$

$$h_{\text{ñð}} = \frac{1}{D_W{}^2}\sum_x\sum_y h^2(x,y). \tag{13}$$

Схема алгоритма ПНМО представлена на рис. 3.

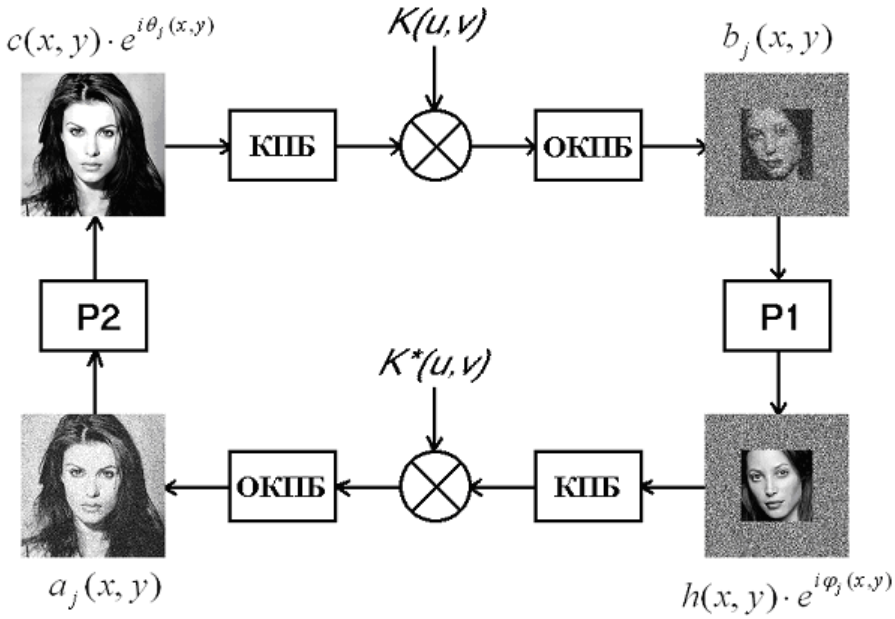

Рис. 3. Схема алгоритма ПНМО

Внедрение скрываемого изображения в контейнер

На первом этапе работы алгоритма производится нормировка размеров, положения и содержимого скрываемого изображения и изображения-контейнера.

Далее скрываемое изображение помещается в выходную плоскость коррелятора, описанного выше, а изображение-контейнер — во входную плоскость. Производится обучение коррелятора. На выходе процесса обучения мы получаем комплексную функцию $a_n(x,y)$, описываемую двумя линейными функциями $c(x,y)$ и $\theta_n(x,y)$, где n — количество итераций, затраченных на обучение. Теперь требуется сформировать на основе этих двух функций стего-изображение.

Пусть m — число бит, требуемых для задания уровня яркости каждого пикселя полутонового изображения. Обозначим $Ph(x,y)$ аппроксимацию функции $\theta_n(x,y)$, полученную квантованием по 2^r уровням $(r<m)$, где r — число бит, отводимых на хранение фазы $\theta_n(x,y)$.

Далее стего-изображение $S(x,y)$ формируется по следующему алгоритму. Величина яркости каждого пикселя совпадает с величиной яркости полутонового изображения контейнера, за исключением r младших бит. Эти r младших бит заменяются значением функции $Ph(x,y)$ для пикселя с координатами (x,y). Данное допущение приемлемо, поскольку изменение нескольких младших бит каждого пикселя не вносит заметных искажений в общую картину изображения. Человеческий глаз не может, например, распознать изменение 8-битного тона (256 оттенков), если изменился только самый младший бит. Очевидно, что r должно быть не больше половины m. Количество бит, отводимых на хранение фазы, прямо пропорционально влияет на качество извлекаемого скрытого изображения, но, с другой стороны, обратно пропорционально качеству передаваемого изображения. Следовательно, целесообразно выбирать r пропорционально количеству оттенков, реально используемых в скрытом изображении, и тогда стего-изображение $S(x,y)$ может передаваться по открытым каналам связи.

Извлечение скрытого изображения из стего-изображения

На приемной стороне сначала производится выделение аппроксимированной входной комплексной корреляционной функции. Для этого на основе стего-изображения $S(x,y)$ формируются две функции: $Ph(x,y)$ и $c'(x,y)$. $Ph(x,y)$ — описывается r младшими битами $S(x,y)$, а $c'(x,y)$ — $(m–r)$ старшими. Далее после нормировки $Ph(x,y)$ и $c'(x,y)$, согласно формуле (6), вычисляется выходная корреляционная функция на основе входной функции и ключа:

$$b(x,y) = \hat{I}\hat{E}\ddot{I}\acute{A}\ \left[\hat{E}\ddot{I}\acute{A}\ \left\{c'(x,y)e^{iPh(x,y)}\right\}K(u,v)\right]. \qquad (14)$$

На заключительном этапе производится нормировка амплитуды функции $b(x,y)$ и выделение окна, содержащего скрытое изображение.

Амплитуда полученной функции $|b(x,y)|$ в определенном приближении совпадает с функцией скрытого изображения $h(x,y)$.

Экспериментальные результаты

Тестирование системы проводилось для трех пар изображений (скрываемое и изображение-контейнер). В качестве контейнера для всех трех случаев использовались полутоновые изображения с 256 уровнями серого ($m=8$) размером 256×256 пикселей. В качестве скрытого изображения использовались полутоновые изображения с 256 уровнями серого ($m=8$) размером 128×128 пикселей.

Обучение коррелятора прекращалось в тот момент, когда суммарная среднеквадратичная ошибка составляла менее 0,1% среднего значения изображения для обеих картинок (12), (13). Алгоритм обучения длился в среднем 10 итераций.

Тестирование проводилось для различного количества бит, отводимых на хранение фазы (параметр r — см. выше). Результаты эксперимента изображены на рис. 4.

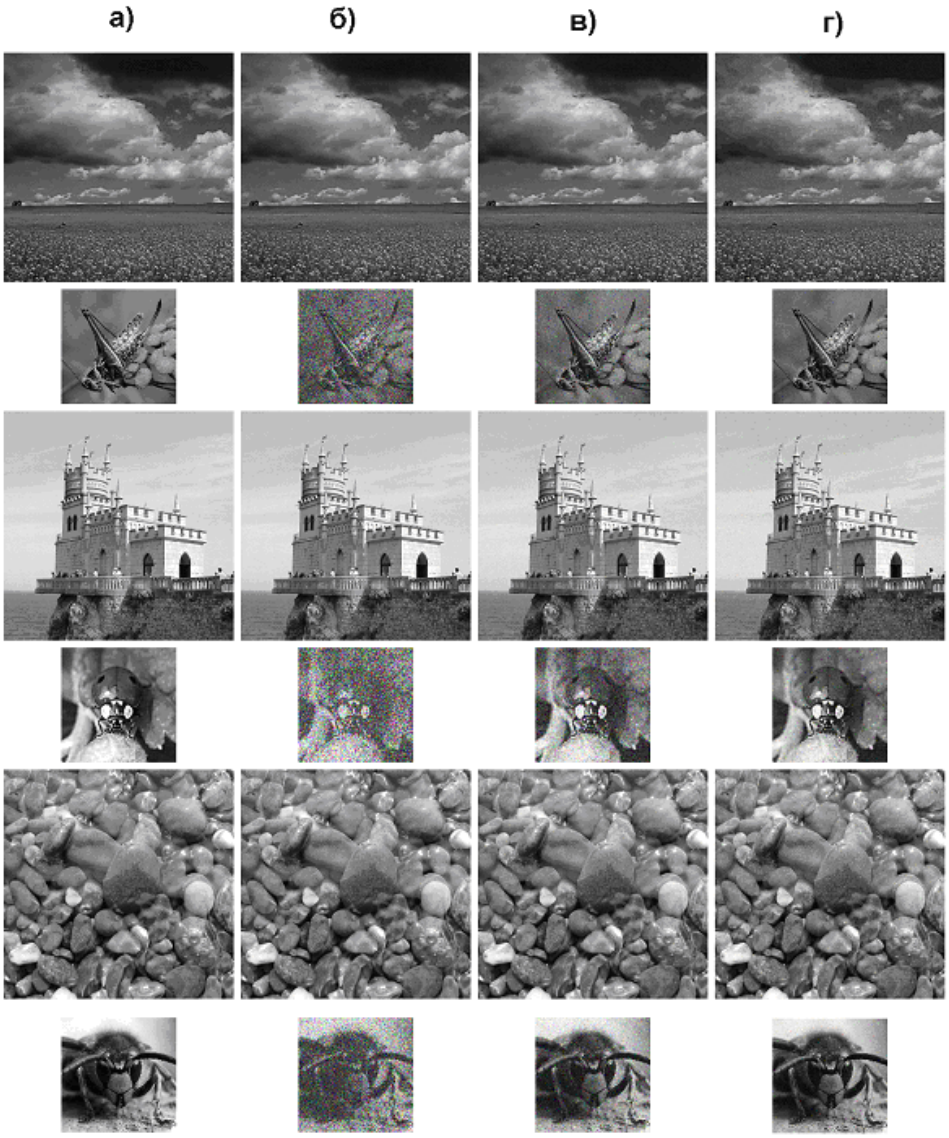

Рис. 4. *а* — исходные изображения-контейнеры и скрываемые изображения; *б* — стего-изображения и извлеченные скрытые изображения $(r = 2)$; *в* — стего-изображения и извлеченные скрытые изображения $(r = 3)$; *г* — стего-изображения и извлеченные скрытые изображения $(r = 4)$

Помимо основного эксперимента проводилось тестирование системы на устойчивость к потерям или преднамеренному искажению злоумышленником части информации при передаче стего-изображения. Устойчивость системы проверялась следующим образом: в передаваемом изображении были сымитированы потери части (15 %, 30 % и 45 %) пикселей — область с нулевой интенсивностью. Результат опыта представлен на рис. 5, на котором показаны стего-изображения с потерей части пикселей и извлеченные из них скрытые изображения (количество бит отводимых на хранение фазы $r = 4$).

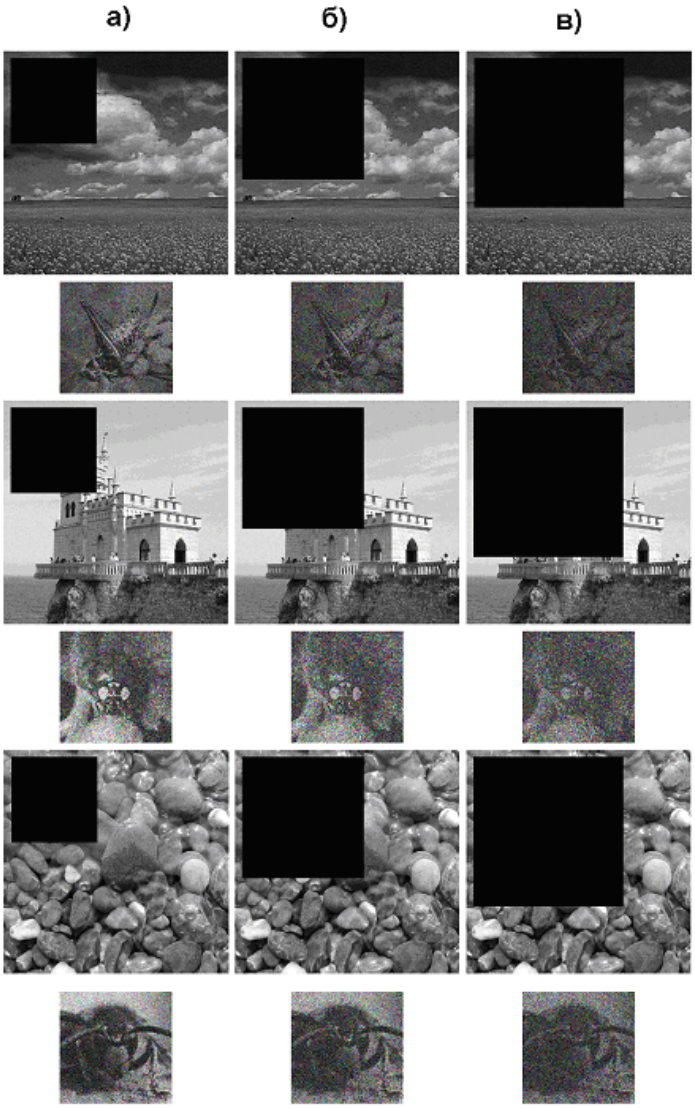

Рис. 5. Стего-изображения и извлеченные скрытые изображения: *а* — потеря 15 % пикселей; *б* — потеря 30 % пикселей; *в* — потеря 45 % пикселей

Также был проведен сравнительный анализ использования для вычисления корреляций КПБ и КПФ. Оба коррелятора обучались до одинакового порога суммарных среднеквадратичных ошибок, равного 0,1 % среднеквадратичных значений изображений. Обучение обоих корреляторов до одинакового порога означает то, что стего-изображения получаются одинакового качества. На обучение коррелятора, основанного на КПБ, было затрачено на 40 % меньше времени, чем на обучение коррелятора, основанного на КПФ.

В ходе экспериментов была определена степень отличия передаваемого стего-изображения от изображения-контейнера и извлекаемого на приемной стороне скрытого изображения от исходного скрываемого изображения. Мера отличия определялась как среднее суммарное различие между всеми пикселями пары изображений. Результаты отображены в таблице.

Степень отличия пар изображений

Пары изображений	Количество бит, отводимых на хранение фазы		
	r=2	*r*=3	*r*=4
Стего-изображение и изображение-контейнер	0,8 %	1,2 %	2,1 %
Извлеченное изображение и исходное изображение	19,4 %	8,7 %	5,1 %

Выводы

В работе предложена оптимизированная по вычислительной сложности стеганографическая система скрытой передачи полутоновых изображений. Алгоритм внедрения и извлечения основан на модифицированной модели двумерного пространственного коррелятора. Цифровые корреляции основаны на комплексном преобразовании BIFORE. Секретный ключ стегосистемы внедрен в коррелятор в виде пространственного фильтра.

Проведены эксперименты для трех пар изображений и различных значений параметра r (количество бит, отводимых на хранение фазы в передаваемом стего-изображении).

Проверена устойчивость алгоритма к потерям или преднамеренной порче части передаваемой информации. Установлено, что изображения распознаваемы даже при потере 30% пикселей стего-изображения.

В результате сравнения КПФ и КПБ показана более высокая скорость обучения коррелятора при использовании КПБ (качество изображений одинаковое).

Рассчитаны такие важные качественные характеристики системы, как степень отличия передаваемого стего-изображения от исходного изображения-контейнера и степень отличия извлеченного скрытого изображения от исходного скрываемого, для различных параметров r. Оптимальное соотношение "качество передаваемого изображения \ качество извлеченного изображения" показано для случая, когда количество бит, отводимых на хранения фазы $r = 4$.

Таким образом, предлагаемая стеганографическая система позволяет устойчиво, надежно и незаметно для невооруженного глаза передавать полутоновые изображения, причем в качестве контейнера также используется полутоновое изображение.

THE SYSTEM, BASED ON THE COMPLEX BIFORE TRANSFORM, OF HIDDEN TRANSFER OF THE HALFTONE IMAGES

I.A. REZNIK, R.KH. SADYKHOV

Abstract

In the given work the system of the hidden transfer of the information is considered. The modified algorithm of hiding half-tone images in grayscale pictures is offered. The steganografic system is based on model of the two-dimensional spatial correlator in basis of the complex BIFORE transform. As filter function of the given correlator the secret key is used. The problems of efficiency, robustness, accuracy and performance of the suggested method are considered.

Литература

1. *Гудмен Дж.* Введение в Фурье-оптику. М, 1970.
2. *Грибунин В.Г.* Цифровая стеганография. СПб., 2002.
3. *Javidi B.* // Phys. Today. 1997. Vol. 50, N. 3. P. 27–32.
4. *Rosen J.* // Opt. Lett. 1993. Vol. 18. P. 1183–1185.
5. *Rosen J., Javidi B.* // Appl. Opt. 2001. Vol. 40, N. 20.
6. *Li Y., Kreske K., Rosen J.* // Appl. Opt. 2000. Vol. 39. P. 5295–5301.
7. *Javidi B., Ahouzi E.* // Appl. Opt. 1998. Vol. 37. P. 6247–6255.
8. *Javidi B., Bernard L., Towghi N.* // Opt. Eng. 1999. Vol. 38/ P. 9–19.
9. *Kishk S., Javidi B.* // Applied Optics. 2002. Vol. 41, No. 26.
10. *Ohnsorg F.R.* // Spectrum Analysis Techniques Symp., Honeywell Res. Cen., Hopkins, Minn., Sept. 20–21, 1966.
11. *Ахмед Н., Рао К.Р., Шульц,* // ТИИЭР. 1971. Т. 59, № 9. С. 93–95.
12. *Ahmed N., Rao K.R., Abdussattar A.L.* // IEEE Trans. Audio Electroacoust. 1971. Vol. AU-19. P. 225–234.
13. *Рао К.Р., Ахмед Н.* // ТИИЭР. 1972. № 8. С. 106–109.