

Метод скрытой передачи данных в оптическом канале видеокамеры 77-48211/543251

02, февраль 2013

Колесников М. В.

УДК 621.397+004.056

Россия, МГТУ им. Н.Э. Баумана

kolesnicov@gmail.com

Введение

В последнее десятилетие в связи с развитием компьютерной техники появился большой интерес к исследованиям в области стеганографии – науки о скрытой передаче или скрытом хранении информации. Основная задача стеганографии состоит в разработке методов встраивания специальных сообщений в основной цифровой сигнал (контейнер), таким образом, чтобы наличие этих сообщений не было заметно. Среди многочисленных методов стеганографической защиты изображений [1] выделяются оптические методы, в которых процесс встраивания или процесс извлечения скрытых сообщений может быть реализован аппаратно с использованием оптических средств.

Широко известны оптические методы [2,3], где процедура встраивания заключается в суммировании интенсивности, которая определяет изображение-контейнер, с интенсивностью, представляющей собой голограмму Фурье, в параметрах которой содержится скрываемое изображение. В результате каждая часть видимого изображения содержит информацию обо всём скрытом изображении. Незаметность голограммы на фоне изображения-контейнера обеспечивается низким уровнем аддитивного сигнала.

Использование голограммы Фурье позволяет встраивать данные в определенной полосе частот изображения-контейнера. Для успешного восстановления, как правило, используется область высоких частот, где собственные пространственно-частотные составляющие изображения-контейнера малы. Такой подход связан с направленностью существующих методов [4,5] на защиту изображений, находящихся на твердом носителе, однако его применение по отношению к цифровым изображениям приводит к разрушению скрытых данных в результате действия методов сжатия.

В настоящей работе представлен метод, позволяющий встраивать скрытые данные в средней полосе частот изображения, в котором процедура встраивания осуществляется аппаратно по схеме коррелятора совместного преобразования, а процедура извлечения – путем цифровой обработки изображений в соответствии с

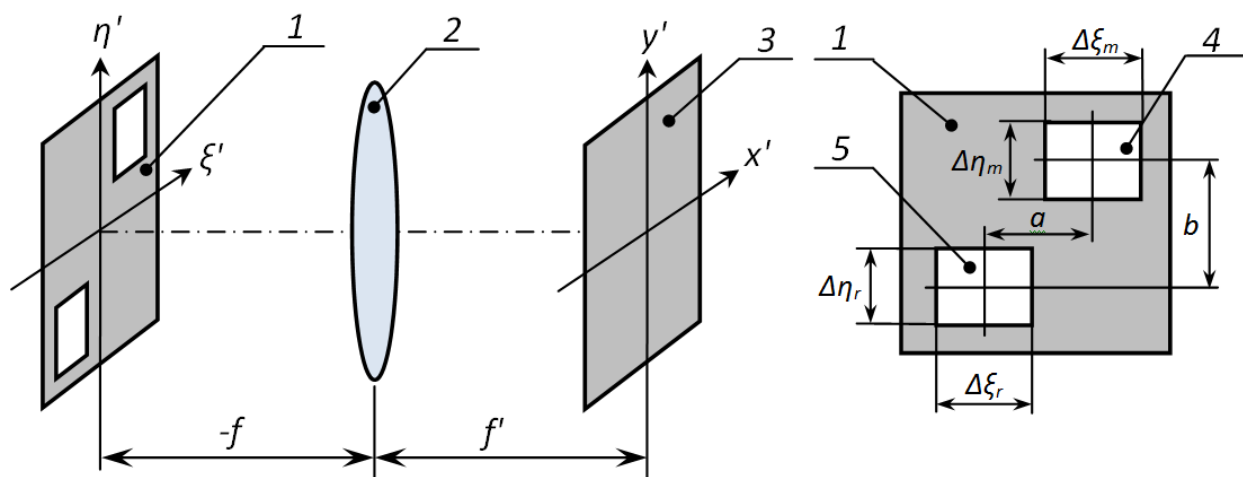
разработанным алгоритмом. Данный подход позволяет встраивать скрытые данные в оптическом канале параллельно с регистрацией основного изображения, и таким образом вынести процесс встраивания за пределы электронного тракта видеокамеры. Это дает возможность использовать для организации скрытого канала передачи информации практически любые системы регистрации видеоизображений.

1 Интерференционный метод формирования стеганнограммы

Рассмотрим процесс формирования аддитивного оптического сигнала (стеганнограммы) с общих позиций, как интерференцию двух волн: основной волны, в параметрах которой содержится неизвестное сообщение, и опорной волны, все параметры которой известны. Для аппаратной реализации данного процесса удобно использовать схему коррелятора совместного преобразования [6], представленную на рисунке 1. Транспарант 1 располагается в передней фокальной плоскости фурие-преобразующего объектива 2 и состоит из двух областей, смещённых относительно друг друга. Суммарный комплексный коэффициент пропускания транспаранта описывается выражением

$$\tau_{\Sigma}(\xi, \eta) = [\tau_M(\xi - a, \eta - b) + \tau_R(\xi, \eta)] \exp[i\varphi(\xi, \eta)], \quad (1)$$

где $\tau_M(\xi_m, \eta_m)$, $\tau_R(\xi_r, \eta_r)$ – комплексные коэффициенты пропускания в областях основной и опорной волны, соответственно; a, b – параметры смещения; $\varphi(\xi, \eta)$ – квазислучайная фазовая функция, предназначенная для выравнивания амплитуд в спектре входного сигнала, значения которой должны быть известны.



1 – амплитудно-фазовый транспарант; 2 – фурие-преобразующий объектив; 3 – плоскость регистрации; 4 – область основной волны; 5 – область опорной волны;

Рис. 1. Схема формирования стеганнограммы, основанная на корреляторе совместного преобразования

Комплексную амплитуду волны на входе фурье-преобразующего объектива 2 при подсветке транспаранта плоской волной с амплитудой A_0 можно представить как:

$$A(\xi, \eta) = A_M(\xi - a, \eta - b) + A_R(\xi, \eta), \quad (2)$$

где $A_M(\xi_m, \eta_m) = A_0 \tau_M(\xi_m, \eta_m) \exp[i\varphi(\xi_m, \eta_m)]$ – комплексная амплитуда основной волны,

$A_R(\xi_r, \eta_r) = A_0 \tau_R(\xi_r, \eta_r) \exp[i\varphi(\xi_r, \eta_r)]$ – комплексная амплитуда опорной волны.

Комплексная амплитуда в плоскости регистрации 3 представляет собой дифракционную картину Фраунгофера, полученную в результате дифракции на амплитудно-фазового транспаранта 1, и определяется с помощью преобразования Фурье следующим образом

$$A'(x', y') = \frac{1}{\lambda f'} \tilde{A}_M\left(\frac{x'}{\lambda f'}, \frac{y'}{\lambda f'}\right) \exp\left[-\frac{i2\pi}{\lambda f'}(ax' + by')\right] + \frac{1}{\lambda f'} \tilde{A}_R\left(\frac{x'}{\lambda f'}, \frac{y'}{\lambda f'}\right), \quad (3)$$

где $\tilde{A}_M(\nu_x, \nu_y)$, $\tilde{A}_R(\nu_x, \nu_y)$ – фурье-образы комплексных амплитуд основной и опорной волны, соответственно; λ – длина волны излучения, f' – фокусное расстояние фурье-преобразующего объектива.

Распределение интенсивности в плоскости регистрации определяется путем умножения функции $A'(x', y')$ на комплексно-сопряжённую и после преобразований имеет вид

$$\begin{aligned} I_w(x', y') = \frac{1}{(\lambda f')^2} & \left[\left| \tilde{A}_M\left(\frac{x'}{\lambda f'}, \frac{y'}{\lambda f'}\right) \right|^2 + \left| \tilde{A}_R\left(\frac{x'}{\lambda f'}, \frac{y'}{\lambda f'}\right) \right|^2 + \right. \\ & + \tilde{A}_M\left(\frac{x'}{\lambda f'}, \frac{y'}{\lambda f'}\right) \tilde{A}_R^*\left(\frac{x'}{\lambda f'}, \frac{y'}{\lambda f'}\right) \exp\left[-i2\pi(\nu_{x0}x' + \nu_{y0}y')\right] + \\ & \left. + \tilde{A}_M^*\left(\frac{x'}{\lambda f'}, \frac{y'}{\lambda f'}\right) \tilde{A}_R\left(\frac{x'}{\lambda f'}, \frac{y'}{\lambda f'}\right) \exp\left[i2\pi(\nu_{x0}x' + \nu_{y0}y')\right] \right], \quad (4) \end{aligned}$$

где введены обозначения $\nu_{x0} = a/\lambda f'$ и $\nu_{y0} = b/\lambda f'$.

Распределение, описываемое выражением (4) представляет собой интерференционную картину, полученную в результате сложения основной и опорной волны в плоскости регистрации, в параметрах которой содержится передаваемое сообщение. Спектр данного распределения имеет вид

$$\begin{aligned}\tilde{I}_w(v_x, v_y) = & (\lambda f')^2 \left[A_M(-\lambda f'v_x, -\lambda f'v_y) \otimes A_M^*(\lambda f'v_x, \lambda f'v_y) + \right. \\ & + A_R(-\lambda f'v_x, -\lambda f'v_y) \otimes A_R^*(\lambda f'v_x, \lambda f'v_y) + \\ & + A_M(-\lambda f'v_x, -\lambda f'v_y) \otimes A_R^*(\lambda f'v_x, \lambda f'v_y) \otimes \delta(v_x + v_{x0}, v_y + v_{y0}) + \\ & \left. + A_M^*(\lambda f'v_x, \lambda f'v_y) \otimes A_R(-\lambda f'v_x, -\lambda f'v_y) \otimes \delta(v_x - v_{x0}, v_y - v_{y0}) \right].\end{aligned}\quad (5)$$

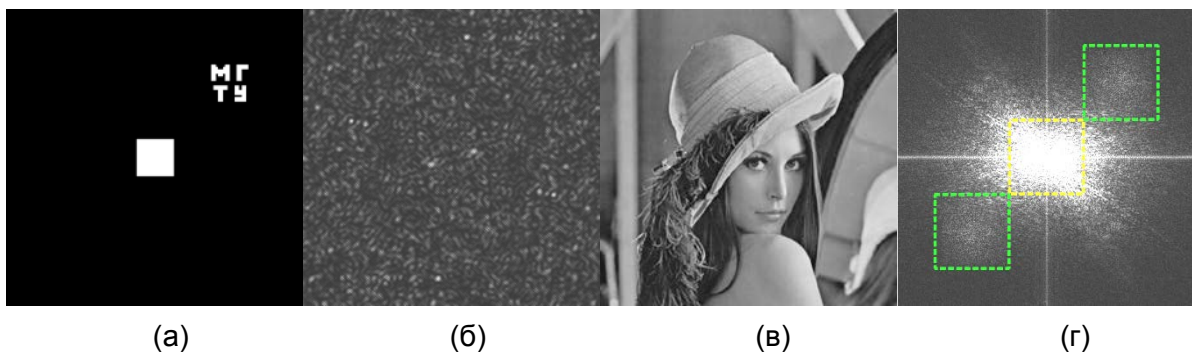
Анализ выражения (5) показывает, что спектр стего-изображения (изображения с наложенной стеганограммой) будет содержать два симметричных корреляционных «пики», смещенных относительно нулевого порядка на значения v_{x0} и v_{y0} (третье и четвертое слагаемое). Каждый из них представляет собой свертку функций, описывающих основную и опорную волну в плоскости транспаранта. Таким образом, при наложении интерференционной картины на произвольное изображение (контейнер) скрытые данные будут содержаться в определенной полосе частот шириной

$$\Delta v_x = \frac{\Delta \xi_m + \Delta \xi_r}{\lambda f'} \text{ и } \Delta v_y = \frac{\Delta \eta_m + \Delta \eta_r}{\lambda f'}, \quad (6)$$

где $\Delta \xi_m, \Delta \eta_m$ и $\Delta \xi_r, \Delta \eta_r$ – размеры областей основной и опорной волны.

Размер и смещение ковариационных «пигов» в спектре определяются заданными параметрами транспаранта, поэтому при известной опорной волне $A_R(\xi_r, \eta_r)$ встроенная информация может быть однозначно определена.

Результаты моделирования процесса встраивания скрытого сообщения по схеме коррелятора совместного преобразования представлены на рисунке 2. В качестве изображения-контейнера используется стандартное тестовое изображение “Lena” размером 512×512. Опорная волна задается прямоугольной областью, коэффициент пропускания в области основной волны $\tau_M(\xi_m, \eta_m)$ образует бинарное изображение в виде символов «МГТУ», а квазислучайная фазовая функция $\varphi(\xi, \eta)$ является бинарной и принимает значения 0 и π .



а – амплитудная составляющая транспаранта; б – стеганограмма;
в – стего-изображение; г – спектр амплитуд стего-изображения;

Рис. 2 – Результаты моделирования процесса встраивания скрытых данных.

Частный случай использования данного метода заключается в представлении комплексной амплитуды опорной волны на транспаранте в виде дельта-функции, что оправданно, когда размеры области опорной волны много меньше элементов информации в области основной волны. В этом случае опорная волна в плоскости регистрации – плоская, а стеганограмма представляет собой голограмму Фурье. Недостаток такого подхода заключается в том, что встраивание информации осуществляется в частотной области изображения-контейнера в явном виде.

2 Алгоритм извлечения скрытых данных

Для восстановления сообщения на первом этапе необходимо путем соответствующей частотной фильтрации оставить в спектре стего-изображения только ту область частот, в которой находится один из ковариационных «пику». После чего основная волна может быть восстановлена применением инверсной фильтрации [7], недостаток которой заключается в появлении искажений при наличии в исходном изображении шума. В нашем случае роль аддитивного шума играют пространственно-частотные составляющие изображения-контейнера в области частот, соответствующей ковариационному «пику». В случае если функция $\tilde{A}_R$ принимает нулевые или близкие к нулевым значения, то искажения принимают доминирующий характер. С учетом того, что фазовая составляющая фурье-спектра содержит определяющую информацию о пространственном распределении в изображении, для устранения указанного недостатка при восстановлении будем использовать алгоритм фазовой корреляции. На примере третьего слагаемого в выражении (4), восстановленная основная волна может быть получена как

$$A_M^r(\xi - a, \eta - b) = \mathfrak{F}^{-1} \left\{ \frac{I'_S(x', y') \tilde{A}_R(x'/\lambda f', y'/\lambda f')}{|I'_S(x', y') \tilde{A}_R(x'/\lambda f', y'/\lambda f')|} \right\}, \quad (7)$$

где $\mathfrak{F}^{-1}$ – оператор обратного преобразования Фурье, $I'_S(x', y')$ – стего-изображение после частотной фильтрации. Восстановленное распределение коэффициента пропускания в области основной волны с точностью до постоянного множителя находится путем умножения на комплексно-сопряженный коэффициент пропускания квазислучайной фазовой маски:

$$\tau_M^r(\xi_m, \eta_m) \sim A_M^r(\xi_m, \eta_m) \exp[-i\varphi(\xi_m, \eta_m)]. \quad (8)$$

Объем информации, передаваемый в пределах одного кадра, определяется количеством областей с размером $\Delta\xi_b \times \Delta\eta_b$ в пределах области основной волны, каждая из которых задает один бит информации путем амплитудной ($\tau_0 = 0$ и $\tau_1 = 1$) или фазовой ($\tau_0 = -1$ и $\tau_1 = 1$) модуляции излучения. Выбор размера элемента информации определяется путем компромисса между количеством элементов информации и отношением сигнал/шум μ в восстановленном распределении основной волны. Увеличивая размер, можно добиться необходимого отношения сигнал/шум путем усреднения сигнала по соответствующим областям, причем $\mu \sim \sqrt{\Delta\xi_b \Delta\eta_b}$.

На рисунке 3 представлена схема алгоритма извлечения информации. Ввиду того, что часть функций принимают комплексные значения, на рисунке 3 изображены их модули.

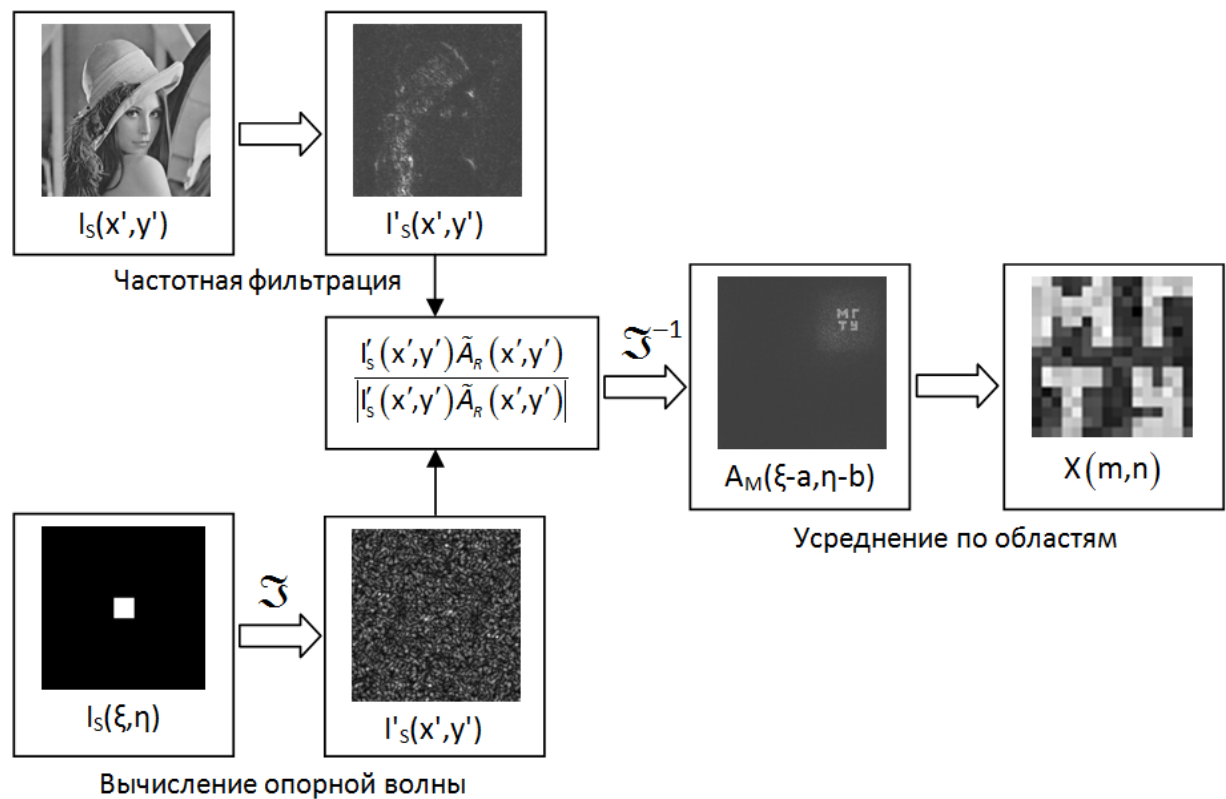


Рис. 3. Схема алгоритма извлечения информации.

3 Исследование устойчивости к компрессии

Под устойчивостью понимается возможность восстановления скрытой информации после предполагаемых преобразований стего-изображения. Применительно к цифровым изображениям и видеозаписям такими преобразованиями являются методы компрессии по стандартам JPEG и H.264, соответственно.

Алгоритм JPEG в настоящее время представляет собой наиболее распространенный алгоритм сжатия цифровых изображений. JPEG сжатие основано на удалении данных из визуально не значимых областей изображения, которые, в свою

очередь, используются для встраивания скрытых данных. Уровень потерь, вызванных сжатием, принято характеризовать коэффициентом качества q , который принимает значения от 0 до 100.

Исследуем устойчивость к алгоритму сжатия JPEG, при встраивании скрытых данных объемом 64 бита в пределах полутоновых изображений размером 512×512 , в качестве которых будем использовать стандартные тестовые изображения: “Peppers”, “Lena”, “Barbara”, “Goldhill”, “Baboon” (рис. 4). В качестве скрытых данных будем использовать сгенерированные случайным образом битовые последовательности. Оценку показателя устойчивости будем производить с помощью коэффициента ошибочных битов BER (Bit Error Rate), определяемого как отношение количества ошибочных битов к общему количеству переданных битов.



а – “Peppers”, б – “Lena”, в – “Barbara”, г – “Goldhill”, д – “Baboon”

Рис. 4. Стандартные тестовые изображения

Для простоты анализа примем, что основная и опорная волны задаются квадратными областями равных размеров, расположенными таким образом, что скрытые данные будут содержаться в средней полосе частот изображения-контейнера шириной $\Delta \nu_x = 0,5\nu_{Nx}$ и $\Delta \nu_y = 0,5\nu_{Ny}$ со средними частотами $\nu_{x0} = 0$ и $\nu_{y0} = 0,5\nu_{Nx}$, где ν_{Nx} и ν_{Ny} – частоты Найквиста по соответствующим направлениям. При использовании области средних частот встроенный сигнал, с одной стороны, более устойчив к сжатию, чем при встраивании в области высоких частот, с другой стороны, не так заметен на фоне изображения контейнера, как при встраивании в области низких частот.

С целью обеспечения визуальной незаметности накладываемого сигнала примем, что среднеквадратическое отклонение флуктуаций интенсивности соответствует одному уровню квантования.

На рисунке 5 представлены полученные графики зависимости коэффициента ошибочных битов, от коэффициента качества JPEG. Для однозначного определения принадлежности элемента информации к “0” или “1” в распределении $X(m, n)$, полученного путем усреднения по соответствующим областям восстановленного сигнала $\tau_M^r(\xi_m, \eta_m)$, использовалась кластеризация методом k -средних [8].

Как следует из полученных результатов, использование фазовой модуляции при задании элементов информации приводит к появлению меньшего числа ошибочных битов

по сравнению с амплитудной модуляцией. Это объясняется тем, что данные, содержащиеся в фазе, в меньшей степени подвергается влиянию пространственно-частотных составляющих спектра изображения-контейнера. Высокий процент ошибочных битов при использовании изображений “Goldhill” и “Baboon” объясняется слишком большими значениями амплитуд фурье-спектра этих изображений в средней полосе частот при данном уровне накладываемого сигнала.

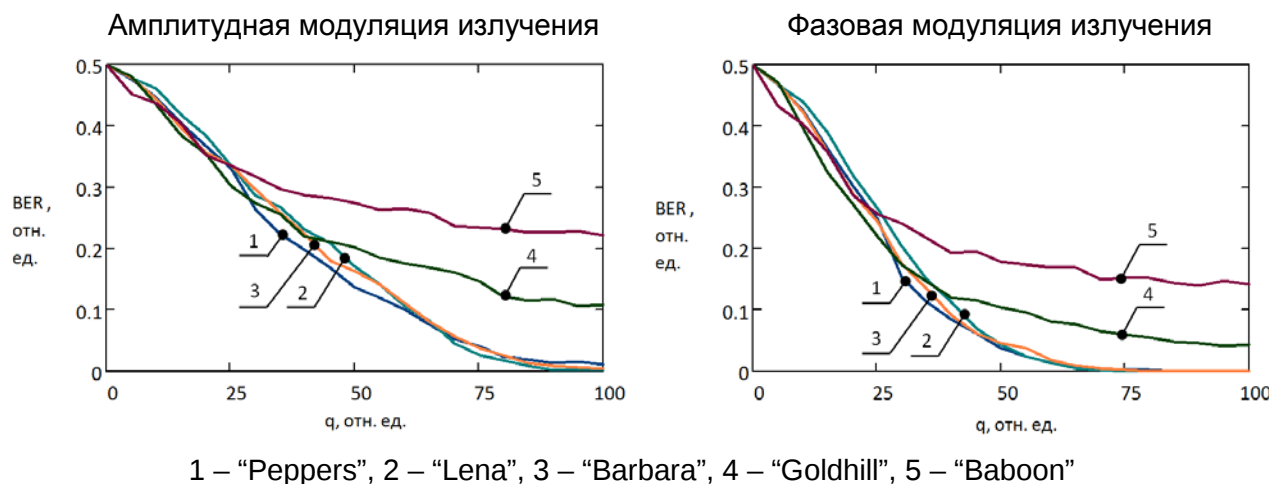


Рис. 5. Зависимость коэффициента ошибочных битов от коэффициента качества JPEG

Исследуем путем численного моделирования устойчивость к применению сжатия при встраивании обновляемых скрытых данных в последовательность видеок кадров. Для этого будем использовать сжатие по стандарту H.264 кодером x264. Сжатие осуществляется варьированием качества отдельных кадров для достижения наилучшего качества всей последовательности при заданной скорости видеопотока и частоте 30 кадров в секунду.

В качестве видеозаписей будем использовать стандартные тестовые видеопоследовательности (рис. 3.12), состоящие из 300 кадров размером 352×288 : “Akiyo”, “Crew”, “Hall monitor”, “Foreman”, “City”. Объем скрытых данных в пределах одного кадра при встраивании в средней полосе частот ($\Delta \nu_x = 0,5\nu_{Nx}$, $\Delta \nu_y = 0,5\nu_{Ny}$, $\nu_{x0} = 0$, $\nu_{y0} = 0,5\nu_{Nx}$) составляет 25 бита. Встраиваемые данные для каждого кадра представляют собой сгенерированные случайным образом битовые последовательности.

В таблице 3 представлены результаты вычисления коэффициента ошибочных битов, усредненного по серии из 300 кадров, для пяти видеопоследовательностей с применением различной степени сжатия.

Таблица 1 – Зависимость коэффициента ошибочных битов от скорости видеопотока.

	Akiyo	Crew	Hall monitor	Foreman	City
1 Мбит/с	0,015	0,15	0,08	0,127	0,208
2 Мбит/с	0,002	0,008	0,005	0,025	0,07
3 Мбит/с	0	0,0003	0,0004	0,01	0,03
4 Мбит/с	0	0	0	0,006	0,017

Используемые при моделировании видеопоследовательности можно разделить на две категории: снятые неподвижной камерой (“Akiyo”, “Hall monitor”) и снятые подвижной камерой (“Crew”, “Foreman”, “City”). Видеозаписи, относящиеся ко второй категории, содержат большое количество меняющихся во времени объектов, поэтому при одной и той же степени сжатия уровень искажений, как самих изображений, так и встроенных скрытых данных выше, чем у видеозаписей, относящихся к первой группе.

Для большей наглядности рассмотрим искажения, возникающие при встраивании конкретной информации, представляющей собой бинарное изображение размером 86×86 в виде знака “Copyright”. С учетом того, что в пределах одного кадра передаётся 25 битов скрытых данных, для передачи всего изображения потребуется 295 кадров. В качестве контейнера будем использовать видеозапись “Hall monitor” с частотой 30 кадров в секунду. Восстановленные изображения представлены на рисунке 6.

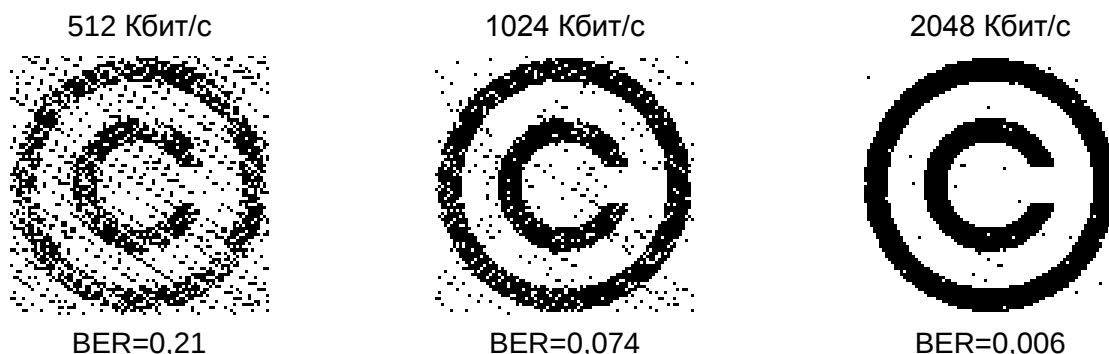


Рис.6. Восстановленные скрытые данные при различных скоростях видеопотока.

Заключение

Применение фазовой модуляции при задании элементов информации позволяет добиться существенно меньшего количества ошибочных битов в извлеченных данных по сравнению с амплитудной модуляцией. Компромисс между объемом передаваемой информации и количеством ошибочных битов может быть достигнут за счет варьирования размеров элементов информации на амплитудно-фазовом транспоранте.

Использование полосы средних частот при встраивании скрытых данных в изображение по схеме коррелятора совместного преобразования позволяет успешно противостоять такому виду искажений, как сжатие по стандарту JPEG. Например, при

встраивании скрытых данных объемом 64 бита в естественное изображение размером 512×512 и последующем сжатии по стандарту JPEG с коэффициентом качества 60 вероятность появления ошибочных битов не превышает 0,05.

Показана устойчивость к сжатию по стандарту H.264 при встраивании скрытых данных в видеопоток. При высокой скорости видеопотока, соответствующего современным каналам передачи информации, предложенный метод можно использовать для скрытой передачи данных.

Список литературы

1. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. К.: «МК-Пресс», 2006. 288 с.
2. N. Takai, Y. Mifune, Digital watermarking by a holographic technique // Appl. Opt. 41. 2002. pp. 865-873. DOI:10.1364/AO.41.000865
3. М. В. Смирнов, Голографический подход к встраиванию скрытых водяных знаков в фотоизображение // Оптический журнал. 2005. том 72. № 6. с. 51-56.
4. L. J. Sun and S. L. Zhuang, Watermarking by encrypted Fourier holography // Opt. Eng. vol. 46. no.8. 2007. pp. 0858011-0858014. DOI:10.1117/1.2769366
5. S. Wang, S. Huang, X. Zhang, and W. Wu, Hologram-Based Watermarking Capable of Surviving Print-Scan Process // Applied Optics, 49(7). 2010. pp. 1170-1178. DOI: 10.1364/AO.49.001170
6. C. S. Weaver, J. W. Goodman, A technique for optically convolving two functions // Appl. Opt. 5. 1966. pp. 1248-1249. DOI: 10.1364/AO.5.001248
7. Гонсалес Р., Вудс Р. Цифровая обработка изображений. М.: Техносфера, 2005. 1072 с.
8. MacQueen J., Some methods for classification and analysis of multivariate observations // In Proc. 5th Berkeley Symp. on Math. Statistics and Probability. 1967. pp. 281-297.