СИСТЕМА ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ С ВОЗМОЖНОСТЬЮ ИХ ИЗВЛЕЧЕНИЯ ИЗ БУМАЖНЫХ КОПИЙ ЦИФРОВЫХ ДОКУМЕНТОВ

В.И. Коржик[1*], **Д.А. Флаксман**[1]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Санкт-Петербург, 193232, Российская Федерация
*Адрес для переписки: val-korzhik@yandex.ru

Информация о статье
УДК 004.056.5
Статья поступила в редакцию 12.04.2019

Ссылка для цитирования: Коржик В.И., Флаксман Д.А. Система цифровых водяных знаков с возможностью их извлечения из бумажных копий цифровых документов // Труды учебных заведений связи. 2019. Т. 5. № 3. С. 75–85. DOI:10.31854/1813-324X-2019-5-3-75-85

Аннотация: *В работе предлагается система ЦВЗ для цветных изображений, главной особенностью которой является возможность их извлечения даже после печати и последующего сканирования изображения со скрытым вложением. Дается описание алгоритмов вложения и извлечения дополнительной информации, основанных на использовании широкополосных сигналов в частотной области. Описаны алгоритмы коррекции искажений, возникающих при печати и последующем сканировании бумажных копий цифровых документов. Приводятся результаты экспериментального исследования предложенной системы по объему вложения и достоверности извлечения вложенных данных.*

Ключевые слова: *цифровые водяные знаки, широкополосные сигналы, геометрические преобразования, коррекция перспективных искажений.*

ВВЕДЕНИЕ

Система цифровых водяных знаков (ЦВЗ) – это способ защиты интеллектуальной собственности и авторских прав владельцев цифровой информации. ЦВЗ являются одним из двух основных разделов стеганографии – науки о скрытой передаче информации. Стеганографию можно разделить на собственно стеганографию (СГ) (в узком смысле) и на ЦВЗ [1]. Отличием СГ от ЦВЗ является то, то в стеганографии основной целью является скрытность передачи сообщений, а в ЦВЗ – невозможность устранения вложенного сообщения.

ЦВЗ по количеству вкладываемой информации делятся на нульбитовые и многобитовые. Многобитовые системы позволяют при извлечении получить скрытое сообщение, в том время как нульбитовые позволяют осуществить только проверку наличия или отсутствия самого факта вложения. С.О. Анфиногенов в своей диссертационной работе предлагает нульбитовую систему ЦВЗ, устойчивую к случайным и преднамеренным преобразованиям [2].

ЦВЗ чаще всего применяются для защиты изображений, звука, видео и других цифровых документов, однако, в настоящее время значительный интерес стал появляться и к использованию таких «аналоговых» носителей, как бумага, пленки и другие физические объекты. Все эти объекты хотя и обладают определенной степенью защиты, (например, физические водяные знаки, контрольные суммы и использование специальных типов бумаги и пленки), нуждаются в дополнительной защите. Так, например, фотографии в бумажных документах, идентифицирующих личность (паспорта, водительские права, пропуска и т. п.), нуждаются в дополнительной защите от подмены (переделки). В некоторых случаях целесообразно использовать скрытую (т. е. невидимую для нелегитимных пользователей), идентификацию личности или товара. Это свойство может упростить нахождение нарушителей процедур идентификации при выполнении необходимого контроля.

В диссертации Ю. Ткаченко [3] предлагается система ЦВЗ для графических QR-кодов, основанная на искажении формы отдельных блоков, входящих в состав бар-кода, однако данный метод требует изменения структуры самого бар-кода.

При разработке систем ЦВЗ часто используются различные способы погружения скрытой информации: дискретное преобразование Фурье, дискретное косинусное преобразование, дискретное пре-

образование Уолша и др. Так, в работе [4] предложена система ЦВЗ для проверки подлинности пластиковых карт, в основе которой лежит преобразование Адамара.

Одним из направлений развития систем ЦВЗ является разработка систем целостности изображений. Например, на основе локальных особенностей может быть построена система хеширования изображений [5]. Однако создать систему ЦВЗ, устойчивую ко всем возможным «атакам» и преобразованиям покрывающих сообщений (ПС), достаточно сложно. Одним из решений данной проблемы является совместное использование нескольких систем ЦВЗ, устойчивых к различным наборам «атак». Такие системы называются «каскадными». В работе [6] предложена каскадная система ЦВЗ, совмещающая преимущества «нормализационного» метода [7], устойчивого к различным аффинным геометрическим атакам, и «голографического» [8], устойчивого к вырезанию фрагментов изображения.

В статье рассматривается система ЦВЗ, которая позволяет вкладывать информацию в цифровые изображения (в том числе бар-коды) и сохранять возможность достоверного извлечения вложенной информации даже после печати и последующего сканирования изображения с вложением.

В первом разделе подробно рассматривается алгоритм вложения и извлечения цифровой информации в изображение. Отдельное внимание уделяется способам устранения искажений, возникающих по время печати и последующего сканирования изображения с ЦВЗ. Во втором разделе представлены экспериментальные результаты работы предложенной системы ЦВЗ для цветных изображений. Третий раздел посвящен тем же вопросам, но применительно к изображениям в виде DataMatrix-кодов. Заключение суммирует результаты работы и формирует некоторые открытые проблемы.

1. ОПИСАНИЕ АЛГОРИТМА ВЛОЖЕНИЯ ЦИФРОВОЙ ИНФОРМАЦИИ В ПОКРЫВАЮЩЕЕ ИЗОБРАЖЕНИЕ И ЕЕ ИЗВЛЕЧЕНИЯ

Алгоритм вложения

Рассмотрим подробно алгоритм вложения скрытого сообщения в покрывающее изображение. Отметим, что сообщением может быть любая цифровая информация. Блок-схема работы алгоритма представлена на рисунке 1.

Для работы алгоритма вложения требуется одноканальное изображение, при этом оригинальное изображение может быть как в градациях серого, так и цветным (в формате RGB). В случае цветного изображения для вложения будет использоваться только синий канал изображения, так как человеческий глаз менее восприимчив к искажениям в нем.

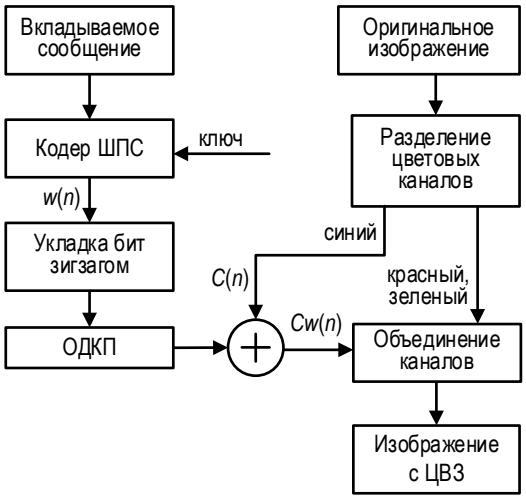


Рис.1. Блок-схема алгоритма вложения

Для вложения была выбрана область средних частот дискретно-косинусного преобразования (ДКП), что позволяет сделать вложение устойчивым не только к сжатию, но и к потере части покрывающего изображения. А для кодирования вкладываемого сообщения был выбран метод, основанный на использовании широкополосных сигналов (ШПС) [1], так как данный метод позволяет извлекать вложенные данные даже при больших искажениях и высоком уровне шума.

Для получения ШПС сначала необходимо подготовить псевдослучайную последовательность (ПСП), получить которую можно с помощью линейного рекуррентного регистра (ЛРР) [9]. Для работы ЛРР необходимо выбрать два числа и длину регистра. Первое число – это ключ, второе – начальное заполнение. Надо понимать, что чем больше длина ЛРР, тем больше будет период ПСП. Для большей стойкости вместо ЛРР может быть использован потоковый шифр [9].

На основе полученной ПСП и вкладываемых бит создается новая последовательность (ШПС), полученная по следующему правилу:

$$W(n) = \alpha(-1)^b \pi(n), \qquad n = 1, 2, \dots, N, \qquad (1)$$

где α – глубина вложения; N – длина ПСП, на которой вкладывается один бит (b = 1 или 0) информации; $\pi(n)$ – отсчет ПСП (±1); $b \in (0,1)$ – бит вкладываемого сообщения.

От параметра N зависят два важнейших свойства вложения. С одной стороны, чем больше N, тем надежнее будет извлекаться информация. С другой стороны, чем больше N, тем меньше бит можно будет вложить в изображение.

Далее из полученной ШПС-последовательности необходимо получить матрицу, размеры которой должны совпадать с размером оригинального изображения. Однако при этом надо учитывать, что следующим шагом будет обратное дискретно-косинусное преобразование (ОДКП), то есть полученная матрица является частотной матрицей. При

этом верхний левый угол – это область наиболее низких частот, а нижний правый – наиболее высоких. Оптимальной областью для укладки ШПС-последовательности является область средних частот, так как изменение низких частот сильно повлияет на качество полученного изображения с вложением, а область высоких частот больше всего подвержена искажениям. Укладывать последовательность необходимо зигзагом, начиная с верхнего левого угла, пропустив при этом область низких частот. Пример укладки бит зигзагом в область средних частот показан на рисунке 2.

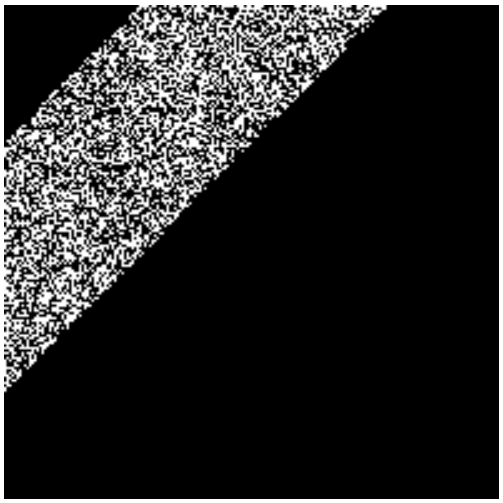


Рис. 2. Область средних частот при ДКП

Далее к полученной частотной матрице применяется ОДКП, которое описывается следующим уравнением:

$$p(x,y) = \sum_{u=0}^{W-1}\sum_{v=0}^{H-1} C(u)\cdot C(v)\cdot F(u,v)\times \\ \times \cos\left(\frac{\pi\cdot(2x+1)\cdot u}{2\cdot W}\right)\cdot\cos\left(\frac{\pi\cdot(2y+1)\cdot v}{2\cdot H}\right), \quad (2)$$

где

$$C(u) = \begin{cases} \frac{1}{\sqrt{W}}, & u = 0 \\ \sqrt{\frac{2}{W}}, & 1 \le u \le W-1 \end{cases};$$

$$C(v) = \begin{cases} \frac{1}{\sqrt{H}}, & v = 0 \\ \sqrt{\frac{2}{H}}, & 1 \le v \le H-1 \end{cases};$$

$F(u, v)$ – изображение; W – ширина изображения в точках; H – высота изображения в точках.

После ОДКП полученную матрицу необходимо сложить с выделенным ранее синим каналом оригинального изображения. Полученное в результате изображение готово к печати на физический носитель и последующему извлечению информации.

Алгоритм извлечения

Система ЦВЗ предполагает печать и последующее сканирование изображения, из-за чего возникают серьезные искажения. Для устойчивой работы алгоритма извлечения и устранения возникающих искажений необходимо добиться того, чтобы размер и геометрическое положение изображения, из которого будет осуществляться извлечение, и оригинала точно соответствовали друг другу. Блок-схема работы алгоритма извлечения представлена на рисунке 3. Стоит заметить, что процесс извлечения может быть осуществлен как при наличии оригинального изображения, так и при его отсутствии. В первом случае декодер называется информированным, во втором случае – слепым.

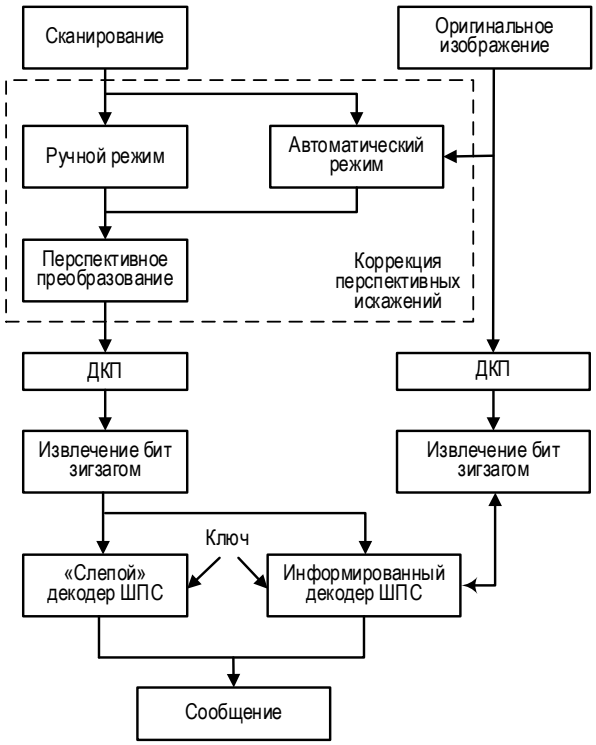


Рис. 3. Блок-схема алгоритма извлечения

Для извлечения вложения сначала нужно отсканировать распечатанное изображение с ЦВЗ, при этом следует выбирать такое разрешение сканирования, чтобы размер отсканированного изображения был больше, чем размер оригинального изображения. Иначе говоря, на одну точку оригинального изображения должно приходиться несколько точек на отсканированном изображении. Если не соблюдать данного правила, то произойдет ухудшение качества изображения и потеря части информации о нем, что негативно скажется на процессе извлечения вложенного сообщения.

После того как изображение было отсканировано, необходимо устранить возникшие геометрические искажения, основными из которых являются поворот, сдвиг и изменение масштаба. А если вместо сканера был применен фотоаппарат, то появятся «перспективные» искажения. Поэтому мы

будем рассматривать более общий случай – устранение «перспективных» искажений, используя перспективное преобразование.

Рассмотрим перспективное (проективное, гомографическое) преобразование подробнее. Важным аспектом перспективного преобразования является то, что при нем сохраняется коллинеарность точек, то есть три точки, лежащие на одной прямой (коллинеарные), останутся лежать на одной прямой и после преобразования, но при этом может не сохраниться параллельность линий, как это происходит при аффинном преобразовании (аффинное преобразование можно считать частным случаем перспективного преобразования). Перспективное преобразование описывается следующим матричным уравнением:

$$\begin{pmatrix} \bar{x}' \\ \bar{y}' \\ w \end{pmatrix} = \begin{pmatrix} t_{11} & t_{12} & t_{13} \\ t_{21} & t_{22} & t_{23} \\ t_{31} & t_{32} & t_{33} \end{pmatrix} \begin{pmatrix} \bar{x} \\ \bar{y} \\ 1 \end{pmatrix}, \quad (3)$$

где x', y' – новые координаты точки; x, y – старые координаты точки; $t_{i,j}$ – коэффициенты матрицы преобразования; w – глубина (масштаб).

Отсюда, после нормировки по масштабу получаем:

$$x'' = \frac{t_{11}x' + t_{12}y' + t_{13}}{t_{31}x' + t_{32}y' + t_{33}}, \qquad y'' = \frac{t_{21}x' + t_{22}y' + t_{23}}{t_{31}x' + t_{32}y' + t_{33}}. \quad (4)$$

Пример перспективного преобразования для тестового изображения представлен на рисунке 4.

а) б)

Рис. 4. Пример перспективного преобразования: а) тестовое изображение «Лена»; б) изображение после перспективного преобразования

При устранении перспективных искажений может возникнуть два варианта: первый – в наличии нет оригинального изображения (известен только размер изображения); второй – когда оно есть. В первом случае искажения устраняются с участием оператора (требуется визуальный поиск границ изображения), во втором – процесс может быть произведен в автоматическом режиме.

Наиболее простым является способ ручного устранения перспективных искажений, неизбежно возникающих при печати и сканировании изображения. При этом необходимо знать только размер оригинального изображения. Сначала необходимо визуально найти четыре угловые точки изображения на отсканированном образце. По положению найденных четырех точек можно рассчитать коэффициенты перспективного преобразования, описывающего преобразование между полученным четырехугольником и прямоугольником, характеризующим размеры оригинального изображения. Для этого необходимо подставить координаты найденных четырех точек в уравнение (4). В результате подстановки получится восемь уравнений: четыре уравнения для «x» и четыре – для «y», при этом коэффициент t_{33} следует принять равным 1. В результате решения получившейся системы из восьми уравнений получится матрица искомого перспективного преобразования.

Затем необходимо применить перспективное преобразование (3) с найденными коэффициентами к отсканированному изображению с ЦВЗ, одновременно обрезав полученное изображение по размерам оригинального. Весь процесс, за исключением визуального поиска, может быть легко автоматизирован. На рисунке 5а приведено отсканированное изображение, а на рисунке 5б – то же самое изображение, но после устранения перспективных искажений. Видно, что отсканированное изображение отличается масштабом и повернуто на небольшой угол.

Имея оригинальное изображение, можно использовать другой метод, и тогда все операции могут быть произведены полностью автоматически и при этом надежнее, чем при ручной коррекции.

а) б)

Рис. 5. Устранение перспективных искажений: а) отсканированное изображение; б) восстановленное изображение

Основным принципом является поиск оригинального изображения на отсканированном, для чего используются хорошо зарекомендовавшие себя методы, применяемые в «компьютером зрении». Алгоритм поиска оригинала на отсканированном изображении можно разбить на четыре этапа.

Этап 1. Поиск локальных особенностей (ЛО) и расчет их дескрипторов с использованием алгоритма обнаружения устойчивых признаков изображения SURF (*от англ.* Speeded Up Robust Features) [10].

ЛО – это хорошо различимая область изображения, соответствующая следующим требованиям: повторяемость (не изменяет своего положения при разном освещении и угле обзора); локальность (занимает малую часть изображения); значимость (каждую ЛО можно уникально описать); компактность и эффективность (количество ЛО невелико по сравнению с количеством точек изображения). Примером ЛО могут служить углы, а наиболее распространенный детектор углов – это детектор Харриса [11]. Дескриптор ЛО – это математическая характеристика, описывающая геометрию локальной окрестности вокруг точки. Поиск ЛО выполняется отдельно для оригинального изображения и изображения, полученного от сканера.

Этап 2. Сравнение ЛО оригинального изображения и изображения, полученного от сканера. Для этого используется алгоритм быстрого сравнения FLANN (*от англ.* Fast Approximate Nearest Neighbors Search) [12]. Результатом работы данного алгоритма являются пары соответствующих друг другу дескрипторов на оригинальном и отсканированном изображении.

Этап 3. Поиск коэффициентов наиболее вероятного перспективного преобразования, описывающего трансформацию первого изображения во второе, с использованием алгоритма оценки параметров на основе случайных выборок RANSAC (*от англ.* RANdom SAmple Consensus), предложенного в 1981 г. Фишлером и Боллесом [13].

Алгоритм RANSAC в данном случае работает следующим образом. По четырем случайно выбранным парам строится гипотеза – перспективное преобразование, описывающее трансформацию отсканированного изображения, к геометрическому положению оригинального изображения. Оставшиеся пары дескрипторов проверяются на соответствие гипотезы (сочетается ли данная пара дескрипторов с предложенным преобразованием). После многократного случайного построения различных гипотез выбирается та, которой удовлетворяет наибольшее число пар дескрипторов.

Этап 4. Применение найденного перспективного преобразования к отсканированному изображению.

Для проведения экспериментов была разработана программа на языке C++ с использованием библиотек компьютерного зрения «OpenCV», в которых уже реализованы вышеприведенные алгоритмы. Иллюстрация результата работы алгоритма представлена на рисунке 6. Слева находится оригинальное изображение, справа – отсканированное. На отсканированном изображении рамкой выделено найденное изображение. Линиями сопоставлены пары наиболее явно совпадающих ЛО, по которым найдено искомое перспективное преобразование. Можно заметить, что среди пар ЛО есть также и явные выбросы. Правда, на результате это никак не сказывается, так как выбросы отсеиваются алгоритмом RANSAC [13].

После того, как отсканированное изображение приведено к размерам оригинала, можно приступать к извлечению вложенных данных. Сначала, так же, как и при вложении, необходимо выделить рабочий канал. Если изображение было цветным, то рабочим является синий, если же изображение было в градациях серого, то дальнейшие шаги будут осуществляться непосредственно с самим изображением.

Рис. 6. Автоматическая коррекция перспективных искажений

Далее, так как вложение осуществлялось в частотную область, необходимо провести ДКП. ДКП – это ортогональное преобразование, в результате которого изображение представляется в виде суммы двумерных синусов различной амплитуды и частоты. ДКП описывается следующим уравнением:

$$F(u,v) = C(u)\cdot C(v)\cdot \sum_{x=0}^{W}\sum_{y=0}^{H} p(x,y)\times \\ \times \cos\left(\frac{\pi\cdot(2x+1)\cdot u}{2\cdot W}\right)\cdot\cos\left(\frac{\pi\cdot(2y+1)\cdot v}{2\cdot H}\right), \quad (5)$$

где

$$C(u) = \begin{cases} \frac{1}{\sqrt{W}}, & u = 0 \\ \sqrt{\frac{2}{W}}, & 1 \le u \le W-1 \end{cases};$$

$$C(v) = \begin{cases} \frac{1}{\sqrt{H}}, & v = 0 \\ \sqrt{\frac{2}{H}}, & 1 \le v \le H-1 \end{cases};$$

$p(x,y)$ – изображение; W – ширина изображения в точках; H – высота изображения в точках.

На рисунке 7 представлен синий канал (отображен в градациях серого) и соответствующая ему частотная матрица. Затем из полученной частотной матрицы необходимо получить последовательность бит. Для этого необходимо применить сканирование зигзагом. При этом следует выбирать именно ту область матрицы, в которую осуществлялось вложение.

Заключительным шагом является извлечение вложенных бит. Здесь может быть два варианта в зависимости от наличия или отсутствия ПС. Если его нет, то будет использоваться «слепой» декодер, а если ПС присутствует, то будет использоваться информированный декодер, при этом для оригинального изображения необходимо будет произвести ДКП и извлечение «зигзагом».

И наконец, необходимо сгенерировать ПСП бит (если использовался ЛРР, то необходимо знать ключ и начальное заполнение).

а) б)

Рис. 7. ДКП: а) тестовое изображение; б) частотная матрица (черный – наибольшая амплитуда, белый – наименьшая)

После этого нужно провести извлечение бит с помощью корреляционного приемника [1], который работает следующим образом: для каждых N бит последовательности, отвечающих за один вложенный бит, рассчитывается следующий коэффициент:

$$\Lambda = \sum_{n=1}^{N} (C'_w(n) - C(n)) \cdot \pi(n), \qquad n = 1,2, \dots, N, \quad (6)$$

где $C'_W(n)$ – отчет последовательности отсканированного изображения; $C(n)$ – отчет последовательности оригинального изображения; $\pi(n)$ – ПСП; N – длина ПСП, на которой вкладывается один бит.

В случае «слепого» декодера, $C(n)$ принимается всегда равным «0». Определение значения бита осуществляется следующим образом:

$$b = \begin{cases} 1, \Lambda < 0 \\ 0, \Lambda \geq 0 \end{cases}. \quad (7)$$

2. ЭКСПЕРИМЕНТАЛЬНЫЕ РЕЗУЛЬТАТЫ

Для проверки работы алгоритма была разработана программа на языке C++ с использованием библиотек компьютерного зрения «OpenCV» и проведена серия экспериментов. В ходе экспериментов, которые проводились как на изображениях в градациях серого, так и на цветных, были подобраны оптимальные параметры длины и глубины ШПС.

От длины ШПС зависит надежность и количество информации, вкладываемой в изображение. Если она окажется малой, то в процессе извлечения может оказаться слишком много ошибок, однако при ее увеличении будет уменьшаться количество вкладываемых в изображение бит. От глубины ШПС зависит визуальное качество изображения.

Сначала, для подбора длины ШПС, для изображений в градациях серого было выбрано тестовое изображение «Лена» в градациях серого» (см. рисунок 4а): размер изображения – 512×512 точек, физический размер напечатанного изображения – 9×9 см, глубина вложения ШПС – 4. Печать осуществлялась на лазерном принтере «Kyocera Ecosys P6021cdn». Сканирование осуществлялось «Canon LiDE 220» с разрешением 1200 dpi.

Результаты эксперимента представлены в таблице 1. По горизонтали изменяется длина ШПС используемая при вложении, а по вертикали откладывается количество бит, используемых для вложения. При этом приведены результаты как для «информированного» декодера, так и для «слепого». По результатам эксперимента можно сделать вывод, что для изображений оптимальной является длина ШПС в диапазоне от 300 до 700, при которой достигается оптимальное соотношение надежности и количества вложенной информации.

Для цветных изображений был проведен аналогичный эксперимент. Эксперимент проводился на цветном изображении «Лена». Размер изображения 512×512 точек. Физический размер напечатанного изображения: 9×9 см. Глубина вложения ШПС: 6. Печать осуществлялась на лазерном принтере «Kyocera Ecosys P6021cdn». Сканирование осуществлялось «Canon LiDE 220» с разрешением 1200 dpi.

Результаты эксперимента представлены в таблице 2. По представленным результатам можно сделать вывод, что для цветных изображений, так же, как и для изображений в градациях серого, оптимальной длинной ШПС является значение в диапазоне от 300 до 700.

Затем был проведен эксперимент по подбору оптимальной глубины вложения ШПС для цветных изображений. Длина ШПС была выбрана равной 500. Остальные параметры остались неизменными (таблица 3).

По результатам видно, что минимальной глубиной вложения является значение, равное 5. Стоит заметить, что увеличение глубины вложения влечет за собой чрезмерное ухудшение качества изображения, поэтому оптимальным диапазоном значений глубины ШПС можно считать значения в диапазоне от 6 до 7.

Далее была проведена серия экспериментов на трех других изображениях. Все эти изображения были напечатаны струйным принтером на бумаге размером 10×15 см. Результаты экспериментов приведены в таблице 4: «Изображение 1» – изображение в градациях серого, размером 1154×904 пикселя. «Изображение 2» – цветное изображение, размером 1154×904 пикселя. «Изображение 3» – цветное изображение, размером 412×530 пикселей.

По результатам экспериментов видно, что при печати изображения важную роль играет соотношение разрешения изображения и его физического размера (разрешение печати). Так, печать изображения с ЦВЗ большого размера на маленький лист может повлечь за собой уменьшение реальной скорости вложения и увеличение вероятности ошибки.

Можно заметить, что в сериях экспериментов присутствует заметный разброс вероятности ошибок, который обусловлен тем, что при проведении каждого эксперимента производилась печать и сканирование изображения, а также поиск и устранение перспективных искажений, из-за чего может возникнуть некоторая вариативность в точности устранения возникших искажений.

ТАБЛИЦА 1. Результаты эксперимента по подбору длины ШПС для изображений в градациях серого

Декодер	Вложение, бит	Длина ШПС				
		200	300	500	700	900
		Количество ошибочных бит (красным – в %)				
Информированный / Слепой	64	12 / 14	7 / 1	3 / 6	1 / 0	2 / 1
		18 / 21	10 / 1,5	4 / 9	1,5 / 0	3 / 1,5
	128	16 / 14	8 / 1	5 / 6	3 / 2	12 / 10
		12 / 10	6 / 1,7	4 / 5	2,3 / 1,5	9 / 8
	256	42 / 37	39 / 18	27 / 33	25 / 32	81 / 79
		16 / 14	15 / 7	10 / 12	10 / 12	31 / 30

ТАБЛИЦА 2. Результаты эксперимента по подбору длины ШПС для цветных изображений

Декодер	Вложение, бит	Длина ШПС						
		100	200	300	500	700	900	1100
		Количество ошибочных бит (красным – в %)						
Информированный / Слепой	64	6 / 20	4 /10	3 / 7	0 / 4	0 / 0	0 / 0	2 / 2
		9 / 31	6 / 15	5 / 11	0 / 6	0 / 0	0 / 0	3 / 3
	128	14 /32	4 / 16	3 / 7	0 / 4	2 / 1	14 / 12	33 / 29
		10 / 5	3 / 12	2 / 5	0 / 3	1,5 / 0,7	11 / 9	25 / 22
	256	31 / 45	4 / 17	13 / 8	12 / 9	47 / 45	86 / 81	90 / 93
		12 / 17	1,5 / 6	5 / 3	5 / 4	18 / 18	34 / 31	35 / 36

ТАБЛИЦА 3. Результаты эксперимента по подбору глубины ШПС для цветных изображений

Декодер	Вложение, бит	Глубина ШПС					
		4	5	6	7	8	9
		Количество ошибочных бит (красным – в %)					
Информированный / Слепой	64	3 / 9	1 / 4	0 / 1	0 / 0	1 / 0	0 / 0
		9 / 14	1,5 / 6	0 / 1,5	0 / 0	1,5 / 0	0 / 0
	128	4 / 11	2 / 4	3 / 2	2 / 0	1 / 0	0 / 0
		3 / 8,6	1,5 / 3	2,3 / 1,5	1,5 / 0	0,7 / 0	0 / 0
	256	43 / 40	21 / 19	34 / 38	1 / 15	2 / 0	2 / 2
		17 / 16	8 / 7	13 / 14	0,4 / 6	0,7 / 0	0,7 / 0,7

ТАБЛИЦА 4. Результаты экспериментов

Размер сообщения, бит	Информированный декодер / Слепой декодер		
	Номер изображения		
	1	2	32
	Количество ошибочных бит (красным – в %)		
64	0 / 7	0 / 1	0 / 0
	0 / 11	0 / 1,6	0 / 0
128	0 / 7	0 / 1	0 / 0
	0 / 5,5	0 / 0,8	0 / 0
256	0 / 7	0 / 1	1 / 0
	0 / 2,7	0 / 0,4	1,4 / 0
512	18 / 13	25 / 23	4 / 15
	3,5 / 2,5	4,9 / 4,5	2,7 / 2,9

Для каждого эксперимента представлены результаты извлечения как с использованием оригинального изображения (информированный декодер ШПС), так и без него (слепой декодер ШПС, известен только размер изображения). Вероятность ошибки при использовании «слепого» декодера выше, хотя встречаются и отдельные исключения из этого правила.

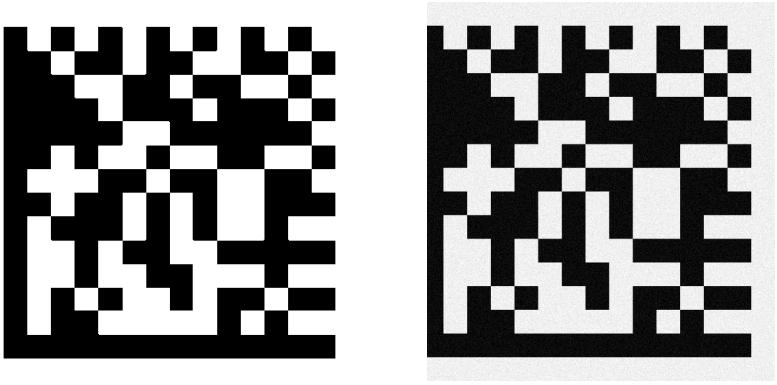
Стоит заметить, что в большинстве проведенных экспериментов видно, что количество ошибочных бит не равно 0, однако если их количество не превышает 2–3 %, то результат можно считать успешным, так как такие ошибки легко устраняются с помощью кодов с исправлением ошибок.

DOI:10.31854/1813-324X-2019-5-3-75-85

3. ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ ВЛОЖЕНИЯ ЦВЗ В DATAMATRIX-КОДЫ

Пример изображения с вложением ЦВЗ в DataMatrix-код при выбранных параметрах α = 15 и N = = 700 приведен на рисунке 8. Алгоритм вложения ЦВЗ остался таким же, каким он был для черно/белых с градациями серого и цветных фотографий. На первый взгляд, различие между рисунками 8а и 8б оказывается не заметно, однако при использовании увеличительного стекла можно заметить присутствие небольшой модуляции яркостью на черных и белых блоках DataMatrix-кода. Такое свойство может служить для скрытия дополнительно вложенной информации от технически невооруженного нарушителя.

Для данного случая так же возникает проблема устранения перспективных искажений, особенно при считывании вложения ЦВЗ при помощи мобильных средств (фотоаппаратов, смартфонов и планшетов). Решение этой проблемы упрощается для данного вида изображений ввиду того, что DataMatrix изначально разработан для подобных условий. В каждом DataMatrix-коде присутствует шаблон поиска (рисунок 9), необходимый для его обнаружения и успешного декодирования.



а) б)

Рис 8. Изображение DataMatrix-кода до (а) и после (б) вложения ЦВЗ

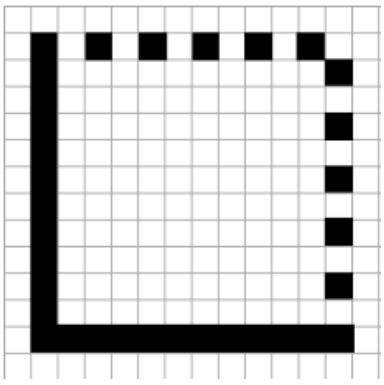


Рис 9. Шаблон поиска DataMatrix-кода

Однако широкодоступные алгоритмы позиционирования оказались недостаточно точны, так как для декодирования DataMatrix достаточно его позиционирования с точностью до модуля, поэтому пришлось дорабатывать существующие алгоритмы для получения приемлемой точности.

В таблице 5 представлены результаты эксперимента с расчетом вероятности ошибки при вложении в два DataMatrix-кода, взятых с бумажных копий размером 2×2, 3×3, 4×4, 5×5, 6×6 и 9×9 см при выборе параметров вложения α = 15, N = 700. Все изображения были напечатаны на лазерном принтере и отсканированы с разрешением 600 dpi. Результаты эксперимента показали, что, используя сканер, можно успешно извлекать до 128 бит данных из изображений размером 3×3 см. При увеличении физического размера изображения количество доступных для вложения бит увеличивается. Например, для изображения размером 4×4 см, это уже 256 бит, а для изображения 5×5 см – 320 бит.

В таблице 6 представлены результаты эксперимента для тех же изображений, однако вместо сканера была камера мобильного телефона.

ТАБЛИЦА 5. Результаты эксперимента при считывании сканером с разрешением 600 dpi

Размер сообщения, бит	Изображение 1 / Изображение 2					
	2×2	3×3	4×4	5×5	6×6	9×9
	Количество ошибочных бит (красным – в %)					
64	9 / 19	3 / 5	2 / 2	2 / 2	2 / 2	2 / 2
	14 / 29,6	4,7 / 7,8	3,13 / 3,13	3,13 / 3,13	3,13 / 3,13	3,13 / 3,13
128	40 / 52	6 / 22	3 / 2	2 / 2	2 / 2	2 / 2
	31,2 / 40,63	4,7 / 17,2	2,34 / 1,56	1,56 / 1,56	1,56 / 1,56	1,56 / 1,56
256	94 / 101	52 / 76	24 / 17	2 / 3	2 / 2	2 / 2
	36,7 / 39,5	20,3 / 29,7	9,38 / 6,64	0,78 / 1,17	0,78 / 0,78	0,78 / 0,78
320	114 / 130	75 / 95	43 / 34	5 / 9	2 / 2	2 / 2
	35,6 / 40,6	23,4 / 13,4	13,4 / 10,6	1,56 / 2,81	0,63 / 0,63	0,63 /0,63

ТАБЛИЦА 6. Результаты эксперимента при считывании телефоном (YotaPhone 2, камера 8 мегапикселей)

Размер сообщения, бит	Изображение 1 / Изображение 2			
	4×4	5×5	6×6	9×9
	Количество ошибочных бит (красным – в %)			
64	5 / 9	11 / 8	6 / 9	3 / 3
	23,4 / 10,1	17,2 / 12,5	9,38 / 14	4,69 / 4,69
128	34 / 35	30 / 35	9 / 24	3 / 4
	26,6 / 27,3	23,4 / 27,3	7,03 / 18,7	2,34 / 3,13
256	77 / 90	73 / 82	41 / 57	4 / 11
	30,1 / 35,1	28,5 / 32	16 / 22,3	1,56 / 4,3
320	98 / 108	92 / 103	69 / 79	6 / 15
	30,6 / 33,7	28,8 / 32,1	21,6 / 24,7	1,88 / 4,69

Результаты эксперимента показали, что, используя камеру телефона, успешно извлекать 128 бит данных можно только из изображений размером 6×6 см и больше, что в два раз больше, чем при использовании сканера.

ЗАКЛЮЧЕНИЕ

В работе для предложенного метода были экспериментально подобраны оптимальные параметры длины и глубины ШПС. Исходя из результатов экспериментов, можно сделать вывод о том, что наличие или отсутствие оригинального изображения при использовании данного метода в меньшей степени влияет на вероятность ошибочного извлечения сообщения, чем процесс печати и последующего сканирования изображения с ЦВЗ, приводящий к серьезным искажениям геометрии и цветового пространства изображения. Оригинальное изображение в основном нужно для его точного автоматического позиционирования. Однако если эту задачу решить альтернативным способом (например, в «ручном режиме» или методом обнаружения обводящей рамки), то можно обойтись и без оригинального изображения, а при извлечении необходимо будет знать только размер изображения, который может быть оговорен заранее.

Исследование возможности вложения ЦВЗ в баркоды, напечатанные на бумаге, показало, что успешное извлечение с использованием смартфона возможно только для их достаточно большого физического размера – не менее чем 6х6 см. В противном случае физический размер при том же объеме вложения может быть уменьшен до 3×3 см.

Следует добавить, что в настоящей статье не рассматривалась возможность использования данного метода для защиты от копирования печатных изображений. Эта проблема требует дальнейших исследований.

Список используемых источников

1. Коржик В.И., Небаева К.А., Герлинг Е.Ю., Догиль П.С., Федянин И.А. Цифровая стеганография и цифровые водяные знаки. Часть 1. Цифровая Стеганография. СПб.: СПбГУТ, 2016. 226.с.

2. Анфиногенов С.О. Разработка и исследование методов построения нульбитовой системы цифровых «водяных» знаков устойчивой к случайным и преднамеренным преобразованиям: дис. … канд. тех. наук. СПб.: СПбГУТ, 2014.

3. Tkachenko I. Generation and analysis of graphical codes using textured patterns for printed document authentication. D.Sc Thesis. Montpellier: Université de Montpellier, 2015.

4. Ho A.T.S., Shu F. A print-and-scan resilient digital watermark for card authentication // Proceedings of the 4th International Conference on Information, Communications and Signal. Formal Methods and Security (ICICS-PCM, Singapore, Singapore,15–18 December 2003). Piscataway, NJ: IEEE, 2003. DOI:10.1109/ICICS.2003.1292640

5. Monga V., Evans B.L. Perceptual Image Hashing Via Feature Points: Performance Evaluation and Tradeoffs // IEEE Transactions on Image Processing. 2006. Vol. 15. Iss. 11. PP. 3452–3465. DOI:10.1109/TIP.2006.881948

6. Кочкарев А.И. Решение проблемы извлечения информации для каскадной системы ЦВЗ при атаке вырезанием фрагментов изображения // Телекоммуникации. 2016. № 10. С. 27–38.

7. Dong P., Brankov J.G., Galatsanos N.P., Yang Y., Davoine F. Digital Watermarking Robust to Geometric Distortions // IEEE Transactions on Image Processing. 2006. Vol. 14. Iss. 12. PP. 2140–2150. DOI:10.1109/TIP.2005.857263

8. Bruckstein A.M., Richardson T.J. A Holographic Transform Domain Image Watermarking Method // Circuits, Systems, and Signal Processing. 1998. Vol. 17. Iss. 3. PP. 361–389. DOI:10.1007/BF01202298

9. Коржик В.И., Яковлев В.И. Основы криптографии: учебное пособие. СПб.: ИЦ «Интермедиа», 2016. 312 с.

10. Bay H., Tuytelaars T., Van Gool L. SURF: Speeded Up Robust Features // Proceedings of the 9th European Conference on Computer Vision (ECCV, Graz, Austria, 7–13 May 2006). Lecture Notes in Computer Science. Part 1. 2006. Vol. 3951. PP. 404–417. DOI:10.1007/11744023_32

11. Harris C., Stephens M. A Combined Corner and Edge Detector // Proceedings of the 4th Alvey Vision Conference (AVC, Manchester, UK, 31st Augusyt – 2nd September 1988). Manchester: University of Manchester Publ., 1988. PP. 23.1–23.6. DOI:10.5244/C.2.23

12. Muja M., Lowe D.G. Fast Approximate Nearest Neighbors with Automatic Algorithm Configuration // Proceedings of the International Conference on Computer Vision Theory and Applications (VISAPP, Lisboa, Portugal, 5–8 February 2009). Setubal: INSTICC Press, 2009. Vol. 1. PP. 331–340. DOI:10.5220/0001787803310340

13. Fischler M.A., Bolles R.C. Random sample consensus: a paradigm for model fitting with applications to image analysis and automated cartography // Communications of the ACM. 1981. Vol. 24. Iss. 6. PP. 381–395. DOI:10.1145/358669.358692

* * *

DIGITAL WATERMARK SYSTEM WITH AN ABILITY OF ITS EXTRACTION FROM HARD COPIES OF DATA

V. Korzhik[1], **D. Flaksman**[1]

[1]The Bonch-Bruevich Saint-Petersburg State University of Telecommunications,
St. Petersburg, 193232, Russian Federation

Article info
The article was received 12 April 2019

For citation: Korzhik V., Flaksman D. Digital Watermark System with an Ability of its Extraction from Hard Copies of Data. *Proceedings of Telecommunication Universities*. 2019;5(3):75–85. (in Russ.) Available from: https://doi.org/10.31854/1813-324X-2019-5-3-75-85

Abstract: *In this paper it is presented Digital Watermark System for color images. The main feature of this system is an ability to extract digital watermarks even after printing and following scanning of watermarked images. There is a description of algorithms for embedding and extracting of additional information. These methods are based on the usage of spread-spectrum signals in the frequency domain. Furthermore, there is described algorithms of distortion correction after printing out and following scanning the paper copies of digital data. The results of the experimental research on evaluation of a possible embedding volume and the reliability after extraction of the embedded data are also presented.*

Keywords: *digital watermarking, spread spectrum signals, perspective distortion correction.*

References

1. Korzhik V.I., Nebaeva K.A., Gerling E.I., Dogil P.S., Fedianin I.A. *Tsifrovaia steganografiia i tsifrovye vodianye znaki. Chast 1. Tsifrovaia Steganografiia* [Digital Steganography and Digital Watermarks. Part 1. Digital Steganography.] St. Petersburg: The Bonch-Bruevich Saint-Petersburg State University of Telecommunications Publ.; 2016. 226 p. (in Russ.)
2. Anfinogenov S.O. *Razrabotka i issledovanie metodov postroeniia nulbitovoi sistemy tsifrovykh "vodianykh" znakov ustoichivoi k sluchainym i prednamerennym preobrazovaniiam* [Development and Research of Methods for Constructing a Nulbit Digital Watermark System Resistant to Random and Intentional Transformations]. PhD Thesis. St. Petersburg: The Bonch-Bruevich Saint-Petersburg State University of Telecommunications Publ.; 2014. (in Russ.)
3. Tkachenko I. *Generation and analysis of graphical codes using textured patterns for printed document authentication*. D.Sc Thesis. Montpellier: Université de Montpellier; 2015.
4. Ho A.T.S., Shu F. A print-and-scan resilient digital watermark for card authentication. *Proceedings of the 4th International Conference on Information, Communications and Signal. Formal Methods and Security, ICICS-PCM, 15–18 December 2003, Singapore, Singapore*. Piscataway, NJ: IEEE; 2003. Available from: https://doi.org/10.1109/ICICS.2003.1292640
5. Monga V., Evans B.L. Perceptual Image Hashing Via Feature Points: Performance Evaluation and Tradeoffs. *IEEE Transactions on Image Processing*. 2006;15(11):3452–3465. Available from: https://doi.org/10.1109/TIP.2006.881948
6. Kochkarev A.I. Solution of information extraction problem for concatenated digital watermarking system in case of attack by image patch cutting-out. *Telekommunikatsii*. 2016;10:27–38. (in Russ.)
7. Dong P., Brankov J.G., Galatsanos N.P., Yang Y., Davoine F. Digital Watermarking Robust to Geometric Distortions. *IEEE Transactions on Image Processing*. 2006;14(12):2140–2150. Available from: https://doi.org/10.1109/TIP.2005.857263
8. Bruckstein A.M., Richardson T.J. A Holographic Transform Domain Image Watermarking Method. *Circuits, Systems, and Signal Processing*. 1998;17(3):361–389. Available from: https://doi.org/10.1007/BF01202298
9. Korzhik V.I., Iakovlev V.I. Osnovy kriptografii: uchebnoe posobie [Cryptography Basics: Tutorial]. St. Petersburg: Intermedia Publ.; 2016. 312 p. (in Russ.)
10. Bay H., Tuytelaars T., Van Gool L. SURF: Speeded Up Robust Features. *Proceedings of the 9th European Conference on Computer Vision, ECCV, 7–13 May 2006, Graz, Austria. Lecture Notes in Computer Science. Part 1.* 2006. vol.3951. p.404–417. Available from: https://doi.org/10.1007/11744023_32
11. Harris C., Stephens M. A Combined Corner and Edge Detector. *Proceedings of the 4th Alvey Vision Conference, AVC, 31st Augusyt – 2nd September 1988, Manchester, UK*. Manchester: University of Manchester Publ.; 1988. p.23.1–23.6. Available from: https://doi.org/10.5244/C.2.23
12. Muja M., Lowe D.G. Fast Approximate Nearest Neighbors with Automatic Algorithm Configuration. *Proceedings of the International Conference on Computer Vision Theory and Applications, VISAPP, 5–8 February 2009, Lisboa, Portugal*. Setubal: INSTICC Press; 2009. vol.1. p.331–340. Available from: https://doi.org/10.5220/0001787803310340
13. Fischler M.A., Bolles R.C. Random sample consensus: a paradigm for model fitting with applications to image analysis and automated cartography. *Communications of the ACM*. 1981;24(6):381–395. Available from: https://doi.org/10.1145/358669.358692