СПОСОБ ФОРМИРОВАНИЯ ЦИФРОВОГО ВОДЯНОГО ЗНАКА ДЛЯ ФИЗИЧЕСКИХ И ЭЛЕКТРОННЫХ ДОКУМЕНТОВ

Сагайдак Д.А., Файзуллин Р.Т.
Омский государственный технический университет

Аннотация

В статье предложен универсальный способ формирования водяного знака как для физических, так и для электронных документов. Подобный водяной знак может применяться как для проверки подлинности документов, так и для скрытой передачи информации. Описан порядок обмена информацией между сторонами для обоих случаев. Проведён анализ сложности обнаружения наличия водяного знака и извлечения встроенной информации третьей стороной, показавший работоспособность предложенного метода.

Ключевые слова: подлинность физического документа, подлинность электронного документа, стеганография, стегоконтейнер, цифровой водяной знак (ЦВЗ), клише, пиксельное представление изображения.

Введение

Вопрос об определении подлинности документов, будь то физические документы (деньги, ценные и конфиденциальные документы) или электронные документы (сканированные копии, фотографии, электронный печатный текст) в настоящее время поднимается всё чаще. Это вызвано увеличением объёма документооборота между организациями, а также развитием технологий обмена документами. В связи с этим появляется множество различных методов защиты документов от подделки.

Например, для защиты физических документов могут использоваться следующие методы:

- технологический – использование водяных знаков, защитной нити/волокна, определённого состава красящих веществ, kipp-эффекта и т.п.;
- графический – использование псевдоводяного знака, гильоширных рамок/розеток, микротекста, защитной сетки, нерегулярного растра, ассюре, корро, различных по форме и сочетанию шрифтов и т.п.;
- химический – появление цветовой реакции при взаимодействии документа с другим веществом, например, водой;
- физический – использование элементов с голограммами, люминесценции веществ с различным квантовым выходом, веществ с различными магнитными свойствами и т.п.;
- комбинированный – всевозможные комбинации методов, описанных выше.

Для защиты электронных документов возможно применение:

- криптографического метода – использования электронной цифровой подписи (ЭЦП), стойкость которой основывается на сложности вычисления дискретного логарифма в группе точек эллиптической кривой, а также на стойкости хэш-функции по ГОСТ Р 34.10-2001 [1];
- стеганографических методов [2, 3] – встраивания текста в электронный документ (изображение) или встраивания цифрового водяного знака [далее – ЦВЗ], а также внесения специального шума.

Как правило, применение методов защиты от подделки физических документов является затратной процедурой, так как для этого требуется наличие специализированной техники и определённого навыка по внедрению этих методов защиты.

Для определения подлинности электронного документа, подписанного ЭЦП, приходится прибегать к услугам третьей стороны (услугам удостоверяющих центров), что, в свою очередь, может быть накладно и затратно по времени, кроме того, пользователь может не доверять третьей стороне.

В настоящее время большинство электронных документов распространяется в таких форматах, как pdf, bmp, jpg и tif, т.е. в виде изображения, но с использованием каких-либо алгоритмов сжатия.

Ввиду вышесказанного можно предложить универсальный способ определения подлинности как физических, так и электронных документов посредством внедрения в них водяных знаков (для электронных документов — ЦВЗ). Причём внедряемые водяные знаки можно использовать как для доказательства подлинности документа, так и для встраивания в них определённой информации, например, для денежной купюры можно встроить серию и номер.

В настоящее время предложено множество методов встраивания информации в изображение. Например, разработаны такие пространственные методы, как:

- метод LSB (Last Significant Bit) [4];
- метод случайного интервала [5];
- метод псевдослучайной перестановки (выбора) [6];
- метод блочного скрытия [7].

Приведённые выше методы являются наиболее близкими к предлагаемому способу.

Суть метода LSB заключается в замене младших значащих битов в байтах изображения (контейнере), отвечающих за кодирование цвета, на биты скрываемого сообщения. Основными достоинствами данного метода являются: 1) тот факт, что человеческий глаз в большинстве случаев не способен заметить изменения в младших битах; 2) простота самого метода; 3) возможность скрывать в относительно небольших изображениях достаточно большие объёмы информации. Основным недостатком метода LSB является его высокая чувствительность к искажениям контейнера. Для ослабления этой чувствительности зачастую

применяют помехоустойчивое кодирование [8]. Кроме того, метод LSB имеет низкую стеганографическую стойкость к атакам пассивного и активного нарушителей [9].

В отличие от метода LSB, в котором каждый бит скрываемого сообщения записывается в последовательно идущие младшие биты, метод случайного интервала позволяет осуществлять случайное распределение битов этого сообщения по контейнеру, в результате чего расстояние между двумя встроенными битами скрываемого сообщения определяется случайным образом. Но есть и недостаток данного метода — биты скрываемого сообщения в контейнере размещаются в той же последовательности, что и в самом скрываемом сообщении. Поэтому, во избежание этого недостатка, прибегают к методу псевдослучайной перестановки (выбора), суть которого заключается в том, что при помощи генератора псевдослучайных чисел образуется последовательность индексов j_1, j_2,…, j_k и выполняется сохранение k-*го* бита сообщения в пикселе с индексом j_k.

Суть метода блочного скрытия заключается в следующем: изображение-оригинал разбивается на l_m непересекающихся блоков Δi $(1 \le i \le l_m)$ произвольной конфигурации, для каждого из которых вычисляется бит чётности $b(\Delta i) = \sum_{j \in \Delta_i}^{\mathrm{mod}\,2} LSB(C_j)$. В каждом блоке выполняется скрытие одного секретного бита M_i. Если бит чётности $b(\Delta i) \neq M_i$, то происходит инвертирование одного из наименьших значащих битов блока Δi, в результате чего $b(\Delta i) = M_i$. Выбор блока может происходить псевдослучайно с использованием стеганоключа.

По сути данный метод обладает такой же устойчивостью к искажениям, что и методы, описанные выше, но по сравнению с ними он обладает рядом преимуществ: во-первых, существует возможность модифицировать значение такого пикселя в блоке, изменение которого приведёт к минимальному изменению статистики контейнера; во-вторых, влияние последствий встраивания секретных данных в контейнер можно уменьшить за счёт увеличения размера блока [10].

Следует заметить, что методы случайного интервала, псевдослучайной перестановки (выбора) и блочного скрытия являются своего рода усложнением метода LSB.

Наиболее идейно близкими к предлагаемому авторами способу являются, например, метод PatchWork [11] и его модификация PatchTrack [12].

Суть метода PatchWork заключается в следующем: вначале псевдослучайным образом в соответствии с ключом выбираются два пикселя изображения. Затем значение яркости одного из них увеличивается на некоторую величину (от 1 до 5), другого – уменьшается на ту же величину. Эта операция повторяется многократно (около 10000 раз), далее находится сумма значений всех разностей:

$$S_n = \sum_{i=1}^{n}((a_i + c) - (b_i - c)) = 2cn + \sum_{i=1}^{n}(a_i - b_i),$$

где a_i и b_i – значения яркости двух выбранных пикселей на шаге i, c – величина приращения, на которую изменятся яркость на каждом шаге алгоритма.

Математическое ожидание суммы разностей значений яркости пикселей в незаполненном контейнере $\sum_{i=1}^{n}(a_i - b_i)$ близка к нулю при достаточно большом значении n. Таким образом, при наличии ЦВЗ величина S_n значительно больше нуля [11].

Основное достоинство метода PatchWork — достаточная стойкость к операциям сжатия, усечения и изменения контрастности изображения. К недостаткам метода относится его неустойчивость к афинным преобразованиям (повороту, сдвигу, масштабированию), а также его малая пропускная способность (для передачи 1 бита скрываемого сообщения требуется 20000 пикселей). Основной отличительной чертой PatchTrack от PatchWork является принцип формирования псевдослучайной последовательности, в соответствии с которой выбираются пиксели изображения. Псевдослучайная последовательность формируется таким образом, что полученные значения могут быть восстановлены после ряда геометрических атак [12].

Также предлагаемый способ идейно сравним с технологией проставления меток (жёлтых точек) цветными лазерными принтерами на каждой печатаемой ими странице. Как правило, принтер осуществляет встраивание кода, содержащего информацию о его серийном номере, а также дате и времени печати документа. В 2005 году специалистами из Electronic Frontier Foundation был расшифрован код, проставляемый принтерами семейства Xerox DocuColor [13]. А позже было подтверждено использование данного метода в принтерах, выпускаемых под торговыми марками Brother, Canon, Dell, Epson, Hewlett-Packard, IBM, Konica, Kyocera, Lanier, Lexmark, NRG, Panasonic, Ricoh, Savin, Toshiba, Xerox [14].

Принцип встраивания водяного знака

Как правило, внедрение ЦВЗ осуществляется в область исходного изображения без использования громоздких вычислений и за счёт определённых преобразований яркости изображения и цветовых составляющих изображения (*r*,*g*,*b*). Следует отметить, что одним из важных этапов построения стегосистемы является определение оптимального размера ЦВЗ, который может быть встроен в исходный документ (стегоконтейнер) без снижения надёжности системы [10]. В случаях, если не удаётся определить оптимальный размер встраиваемого ЦВЗ и есть подозрения, что будет снижена надёжность стегосистемы, предполагается возможным прибегнуть к введению в

документ «побочного шума», например, дополнительных точек.

1) Рассмотрим некоторую прямоугольную область в декартовой системе координат (X, Y), разбитую на MN квадратов (рис.1). Далее данную прямоугольную область будем называть документом (стегоконтейнером).

2) Произвольным образом осуществим выбор K квадратов, далее будем называть эти квадраты «закрашенными». Выбранные квадраты должны быть единственными в столбце.

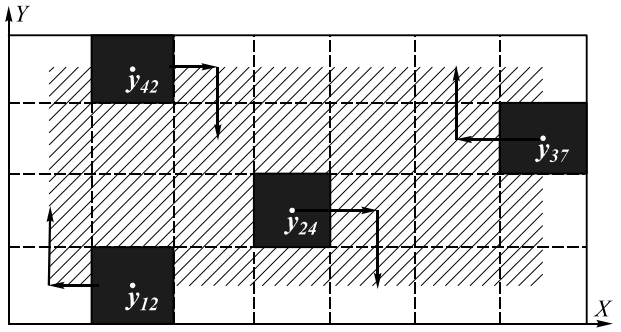

Рис. 1. Прямоугольная область, разбитая на MN квадратов

3) Вычислим сумму расстояний R от центров этих квадратов до какой-либо из осей координат, например, до оси X: $\sum_{i,\,j\in\Xi} y_{ij} = R$, где Ξ – это множество, индексирующее выбранные квадраты, пара (ij) – естественные индексы квадратов в общей нумерации, y_{ij} – координаты центров квадратов по оси Y. Например, для «закрашенных» (отмечены чёрным цветом) квадратов на рис. 1 сумма расстояний $R = \sum_{i,\,j\in\Xi} y_{ij} = y_{12} + y_{42} + y_{24} + y_{36}$.

4) Осуществим внесение «некоторого шума» при помощи создания дополнительных смещённых «закрашенных» квадратов.

При смещении квадратов следует учесть то условие, что исходные и полученные смещённые квадраты должны быть единственными в столбце.

С помощью датчиков псевдослучайных величин сформируем два множества целых чисел.

Множество $\mathrm{I} = (r_k, k = 1,.., mes(\Xi))$ формируется таким образом, что $\sum_k r_k = 0$ и r_k выбираются без каких-либо ограничений по величине, но с соблюдением следующих условий:

если $(x_{ij} + r_k) > N$, то $x_{ij}' = (x_{ij} + r_k) - N \cdot \left[\dfrac{x_{ij} + r_k}{N} \right]$;

если $(x_{ij} + r_k) < 0$, то $x_{ij}' = (x_{ij} + r_k) - N \cdot \left[\dfrac{|x_{ij} + r_k|}{N} \right] + N$;

если $0 \le (x_{ij} + r_k) \le N$, то $x_{ij}' = (x_{ij} + r_k)$,

где x_{ij} – координаты центров «закрашенных» квадратов по оси X, x_{ij}' – координаты смещённых по оси X центров «закрашенных». Причём r_k формируются таким образом, что в последующем полученные по приведённым выше условиям координаты центров смещённых «закрашенных» квадратов x_{ij}' по оси X должны соответствовать следующему условию: $x_{11} \le x_{ij}' \le x_{1N}$, где x_{11}, x_{1N} – координаты первого и последнего центров квадратов первой строки, полученных при разбиении прямоугольной области на MN квадратов.

Множество $J = (s_k, k = 1,.., mes(\Xi))$ формируется таким образом, что $\sum_k s_k = 0$. Затем осуществляется смещение центров «закрашенных» квадратов по оси Y на s_k: $y_{ij}' = y_{ij} + s_k$, где y_{ij}' – координаты центров смещённых «закрашенных» квадратов по оси Y.

Причём s_k во множестве $J = (s_k, k = 1,.., mes(\Xi))$ формируются таким образом, что в последующем полученные координаты центров смещённых «закрашенных» квадратов y_{ij}' по оси Y должны соответствовать следующему условию:

$$\min y_{ij} \le y_{ij}' \le \min(M - y_{ij}).$$

Таким образом, центры смещённых «закрашенных» квадратов остаются в рамках некой ограниченной области (заштрихованная область на рис. 1).

Очевидно, что для вновь полученного множества квадратов также будет выполняться условие:

$$\sum_{i,\,j\in\Xi} y_{ij}' = R.$$

Предположим, что документ маркирован независимым номером W, и будем интерпретировать этот номер как такт работы некоторого генератора, задающего множество индексов Ξ и R. Установление соответствия номера W и множеств «закрашенных» квадратов может служить критерием подлинности документа, иначе говоря, выступать в качестве процедуры проверки водяного знака. Следует отметить, что при осуществлении процедуры проверки подлинности проверяющему заранее известны координаты «закрашенных» квадратов.

Полученные множества можно подвергнуть тестам на случайность, итеративно подобрать I, J так, чтобы тесты проходили успешно. Но что будет, если квадрат, полученный при перемещении, совпадёт с каким-то первоначально «закрашенным» квадратом? В этом случае в качестве критерия для смещённых квадратов следует выбрать близость к величине $R / mes(\Xi)$.

Встраивание водяного знака в физические документы. В качестве документа можно рассмотреть лист бумаги, на котором при помощи принтера и предложенного выше способа при распечатке каких-либо документов предварительно осуществляется расстановка так называемого «специального шума». Таким образом, с минимальными затратами можно

нанести водяной знак. Аналогично, в целях реализации предложенного способа, можно использовать некое устройство, приведённое на рис. 2 и представляющее собой платформу со вставленными в неё стержнями с резьбой и квадратным основанием. Данное устройство предполагается использовать в виде клише. Осуществляя ввинчивание стержней предложенного устройства или используя, например, эгутёр, можно выполнить тиснение по бумаге водяного знака [15], [16].

Встраивание ЦВЗ в электронные документы. В качестве простейшего стегоконтейнера можно рассматривать электронный документ, например, изображение в формате bmp, где каждому пикселю может соответствовать вектор размерностью 24 бита (т.е. 24-разрядный bmp документ). Выбирая подмножество пикселей мощности $H = mes(\Xi)$, можно присвоить младшим битам векторов значение 0. Понятно, что при изменении последнего бита в 24-битовом векторе преобразованное изображение не будет иметь существенных отличий от исходного изображения, заметных человеческому глазу [4]. Или же вовсе можно прибегнуть к полной цветовой модификации пикселя, например, полной заменой цвета пикселя на жёлтый цвет [11].

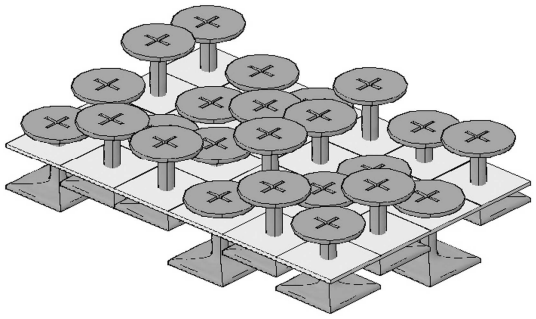

Рис. 2. Предлагаемое устройство для формирования водяного знака на физических документах

Далее вместо квадратов (в соответствии со способом, описанным выше) следует понимать пиксели изображения. На рис. 3 приведён пример смещения пикселей A_1 и A_2 (внесение «некоторого шума») в соответствии с приведённым выше способом, где для последующей наглядности для исходных пикселей (в данном случае A_1, A_2) используются чёрные квадраты (■), а для смещённых A_1', A_2' – белые квадраты (□).

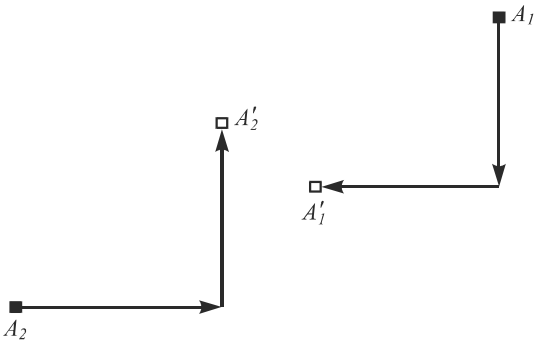

Рис. 3. Смещение пикселей (внесение «некоторого шума»)

На рис. 4 приведена общая в увеличенном виде картина при смещении $H = 40$ пикселей.

Обратим внимание на то, что в качестве базы для вычисления расстояний можно рассматривать некую точку – центр окружности, расположенную вне выбранной прямоугольной области, а смещения $\mathrm{I} = (r_k, k = 1,..,mes(\Xi))$, $J = (s_k, k = 1,..,mes(\Xi))$ осуществлять по окружностям, проходящим через «закрашенные» квадраты (в случае с ЦВЗ – пиксели) и по радиусам, проведённым через «закрашенные» квадраты (пиксели) и центр окружности.

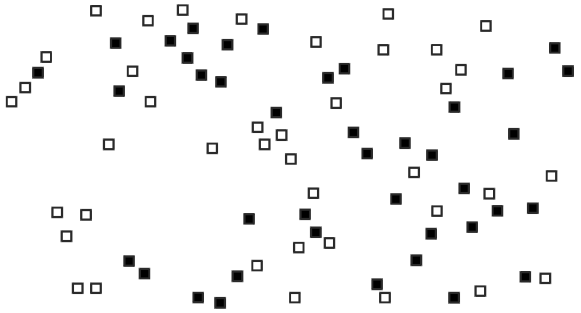

Рис. 4. Исходные и смещённые пиксели

Из описанного выше следует заметить, что в зависимости от разновидностей стегоконтейнера и от характеристик канала передачи этого стегоконтейнера (наличие помех и пр.) предлагаемый авторами способ встраивания ЦВЗ может отражаться в разных реализациях: в виде использования LSB-метода (изменение самого или не самого младшего бита), в виде полной цветовой модификации пикселя (например, в виде печати жёлтой точки), в виде тиснения на бумаге и пр.

Совместно с предложенным способом также возможно применение схемы разделения секрета [17] для потока видеоданных, когда, например, на сервере центра обработки данных (далее – ЦОД) осуществляется хранение не видеоинформации как таковой, а некоторых преобразованных данных [18]. Ввиду того, что в настоящее время технические возможности ЦОД позволяют хранить большие объёмы данных, то критичной по размеру является часть секрета, хранимая у клиента для восстановления и последующего воспроизведения потока видеоданных с сервера ЦОД. Казалось бы, эту малую часть секрета можно рассматривать как ключ, хранящийся у клиента, но принципиальное отличие от схем шифрования заключается в том, что, по всей видимости, здесь можно добиться строгих результатов о невозможности восстановления информации только по большей части данных. Следует учесть, что декомпозиция и композиция информации осуществляется на клиентской стороне схемы, поэтому требуется применение максимально простых и эффективных алгоритмов, работающих «на лету» [19].

Встраивание информации в цифровой водяной знак

Оптимальным стегоконтейнером может являться любой документ, имеющий внешние идентификаци-

онные признаки. Например промаркированная неким номером T38N1 (т.е. это том 38 (T38) номер 1 (N1)) страница электронного журнала в формате *.bmp (далее – страница), содержащая какой-либо текст. Бинарное представление этого номера 1010100 110011 111000 1001110 110001, размерностью в 32 бита. В качестве примера осуществим встраивание ЦВЗ, содержащего этот уникальный номер, в указанную страницу.

Вначале, в соответствии с описанным выше способом, осуществляется внесение ЦВЗ в исходный стегоконтейнер. Затем из пикселей с координатами x_{ij} или x'_{ij} произвольным образом выбираются 32 пикселя, но выбор осуществляется с условиями:

1) если в ЦВЗ необходимо записать «1», то произвольно выбираемым координатам x_{ij} или x'_{ij} должны соответствовать координаты $y_{ij} > \frac{L}{2}$ или $y_{ij}' > \frac{L}{2}$ соответственно, $\frac{L}{2}$ – середина стегоконтейнера (документа);

2) если в ЦВЗ необходимо записать «0», то произвольно выбираемым координатам x_{ij} или x'_{ij} должны соответствовать координаты $y_{ij} < \frac{L}{2}$ или $y_{ij}' < \frac{L}{2}$ соответственно.

Для последующего восстановления информации пользователю необходимо хранить не только координаты пикселей, несущих эту информацию, но и их последовательность.

На рис. 5 приведён стегоконтейнер со встроенным в него ЦВЗ, который, в свою очередь, несёт информацию об идентификационном номере T38N1. Для наглядности на рис. 5 пиксели со встроенной информацией обведены в круг.

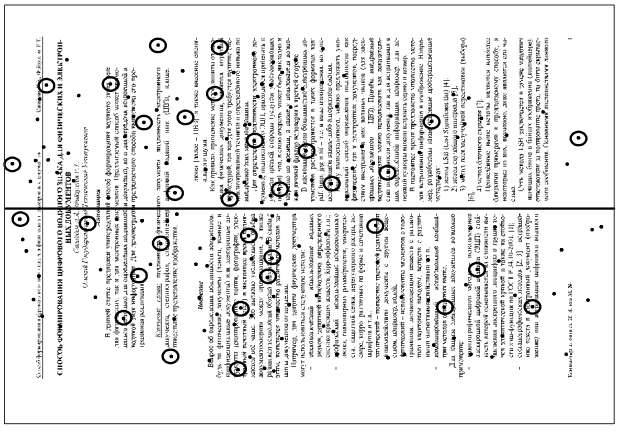

Рис. 5. ЦВЗ, содержащий информацию

Следует заметить, что пиксели, используемые для передачи информации, ничем не отличаются от пикселей ЦВЗ, так как выбор «закрашенных» пикселей, необходимых для передачи информации, осуществляется среди всего множества «закрашенных» пикселей ЦВЗ. Главный критерий – это расположение выбранного «закрашенного» пикселя относительно середины изображения. Для выбранных пикселей запоминаются только координаты по оси X.

Также для встраивания дополнительной информации в стегоконтейнер можно воспользоваться третьей координатой Z, если расположить стегоконтейнер, например, следующим образом (рис. 6).

В качестве параметров для координаты Z могут выступать, например, яркости пикселей ЦВЗ со встроенной в них информацией, вычисляемые по формуле $I = 0,299 \cdot R + 0,587 \cdot G + 0,114 \cdot B$, где: I – значение яркости пикселя; R, G, B – красный, зелёный и синий каналы этого пикселя соответственно (стандарт МСЭ-R BT.601) [20].

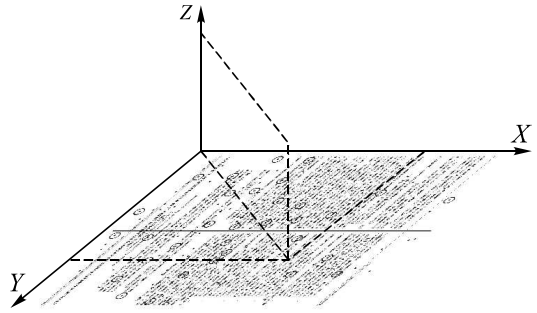

Рис. 6. Встраивание дополнительной информации при помощи дополнительной координаты Z

Описание системы встраивания ЦВЗ в предлагаемом способе. Оценка возможности детектирования ЦВЗ

Зачастую на практике не стоит задача внедрения абсолютно стойких ЦВЗ. Иногда достаточно разработать такую систему встраивания ЦВЗ, при которой злоумышленник не сможет полностью разрушить или подменить цифровые метки. Основной целью встраивания ЦВЗ в предлагаемом авторами способе является защита документа от подделки, а также передача встроенной в него информации, например, для последующей идентификации этого документа.

Как правило, выделяют следующие типы систем встраивания ЦВЗ: бесключевые системы, системы с открытым ключом, системы с закрытым ключом и смешанные.

В предлагаемом авторами способе предусмотрена система встраивания ЦВЗ с *закрытым ключом*. Согласно принципу Керкгоффса [21], применительно к системам встраивания ЦВЗ их стойкость основывается на некоторой секретной информации, без знаний которой нельзя извлечь из контейнера встроенную в него информацию. Т.е. при оценке надёжности системы встраивания ЦВЗ следует полагать, что злоумышленник обладает полной информацией о структуре и алгоритмах данной системы. В качестве ЦВЗ в предлагаемом авторами способе выступают произвольно выбранные «закрашенные» и соответствующие им смещённые «закрашенные» пиксели.

В качестве ключевой информации выступают:

– координаты по оси X «закрашенных» пикселей (координаты пикселей для определения наличия

ЦВЗ), причём следует учесть, что при данных координатах X «закрашенный» пиксель является единственным в столбце;
- датчик случайных чисел, при помощи которого осуществляется смещение «закрашенных» пикселей;
- сумма расстояний R от «закрашенных» пикселей до оси координат X;
- координаты по оси X «закрашенных» пикселей, по которым определяется встроенная информация.

На этапе извлечения информации из стегоконтейнера основной задачей является определение наличия (детектирование) ЦВЗ. После того как установлено, что стегоконтейнер содержит ЦВЗ, осуществляется декодирование информации, встроенной в ЦВЗ. Задачей противника является обнаружить факт внедрения ЦВЗ в стегоконтейнер и в дальнейшем определить, какая информация была встроена в данный ЦВЗ.

Ввиду того, что основной задачей предлагаемого авторами способа является определение подлинности документа, должна исключаться возможность совершения каких-либо кардинальных действий с данным документом (сильное искажение / изменение / обрезка). При определении наличия ЦВЗ в стегоконтейнере анализируется близость значения R', равного сумме расстояний от «закрашенных» пикселей до какой-либо из осей координат при детектировании наличия ЦВЗ, к исходному значению R, рассчитываемому аналогичным образом на этапе внедрения ЦВЗ в стегоконтейнер. Поэтому внедряемый ЦВЗ можно отнести к полухрупким. Как правило, полухрупкие ЦВЗ обладают избирательной стойкостью, т.е. данные ЦВЗ устойчивы по отношению к одним воздействиям и неустойчивы к другим. Например, ЦВЗ встраиваемый по предлагаемому авторами способу, может быть устойчив к переворотам изображения, но не устойчив к вырезке некоторых фрагментов изображения.

Так как в первую очередь анализируется близость значений R' и R, то для точного определения, был ли встроен ЦВЗ в стегоконтейнер, можно прибегнуть к схеме Бернулли (распределению Бернулли) [22]. Пусть существует случайная величина U, которая имеет распределение Бернулли, и она может принимать всего лишь два значения – «закрашен» или «не закрашен» пиксель, с вероятностями p и q соответственно. Тогда среднеквадратическое отклонение (стандартное отклонение/стандартный разброс) случайной величины U: $\sigma = \sqrt{H \cdot p \cdot q}$, где H – количество пикселей, а p и q – вероятности того, «закрашен» или «не закрашен» пиксель соответственно. Среднее значение расстояний от пикселей до какой-либо из осей координат (например, до оси X) $Sr = \sum_{i=1}^{2 \cdot H} x_i / (2 \cdot H)$. Тогда, в соответствии с «правилом трёх сигм» [23]: если $R - 3 \cdot Sr \cdot \sigma \le R' \le R + 3 \cdot Sr \cdot \sigma$, то можно с достаточной уверенностью утверждать, что в изображение встроен ЦВЗ, и в дальнейшем, в зависимости от близости R' к R, можно судить о целостности встроенного ЦВЗ и осуществить его обнаружение и извлечение встроенной в него информации.

Например, пусть заранее известно число «закрашенных» пикселей при встраивании ЦВЗ. Чем больше количество этих «закрашенных» пикселей, тем больше вероятность того, что их распределение будет осуществляться по нормальному закону распределения. В случае, если при детектировании ЦВЗ обнаружено отсутствие «закрашенного» пикселя по заданной координате, то осуществляется пропуск данного пикселя и переход к следующему. Таким образом, сумма R' считается только для обнаруженных пикселей.

Предположим, что вероятность ошибки равна $q = 0{,}1$ (вероятность того, что пиксель «не закрашен»), тогда вероятность того, что пиксель «закрашен» $p = 1 - q = 0{,}9$. Количество «закрашенных» пикселей, например, равно $H = 30$. Найдём среднеквадратическое отклонение:

$$\sigma = \sqrt{n \cdot p \cdot q} = \sqrt{30 \cdot 0{,}9 \cdot 0{,}1} = 1{,}64.$$

Далее находится среднее значение расстояний $H = 30$ пикселей до оси X. Оно равно $Sr = R / 30$, где R – сумма расстояний до оси X от «закрашенных» пикселей, которая хранится в ключевой последовательности. Тогда:

$$R - 3 \cdot (R/30) \cdot \sigma \le R' \le R + 3 \cdot (R/30) \cdot \sigma;$$
$$R \cdot (1 - 0{,}164) \le R' \le R \cdot (1 + 0{,}164);$$
$$0{,}836 \cdot R \le R' \le 1{,}164 \cdot R.$$

Понятно, что часть некоторых бит, предназначенных для извлечения встроенной информации, может быть утеряна, т.е. при детектировании ЦВЗ получилось так, что пиксель «не закрашен». Тогда, в случае, если в ЦВЗ осуществляется встраивание какого-либо уникального номера, можно попытаться восстановить данный уникальный номер методом подбора подходящего значения не «закрашенного» бита в бинарном представлении этого номера, так как обычно уникальные номера присваиваются в соответствии с каким-либо правилом.

Рассмотрим конкретный пример обмена информацией при помощи предлагаемого метода, по традиции обозначив его участников именами Алиса и Боб. Пусть Алиса осуществила встраивание ЦВЗ с внесённым в него уникальным номером T38N1 (в бинарном представлении 1010100 110011 111000 1001110 110001).

При детектировании ЦВЗ Бобом выяснилось, что есть «не закрашенные» пиксели, которые отвечают за извлечение встроенной информации, в результате получился следующий код:

101010×11001111100×10011101100×1,

где x может принимать только два значения – «0» или «1». Так как встраиваемый номер является уникальным, то можно осуществить некий подбор невосста-

новленных бит: 101010(0 или 1)110011 11100(0 или 1)10011101100(0 или 1)1.

В случае, если:

1010101 110011 111001 1001110 110011

U 3 1 N 3

или если:

1010100 110011 111000 1001110 110001

T 3 8 N 1

Допустим, Боб знает порядок формирования уникального номера и он получил код U31T1, по структуре он понимает, что это, скорее всего, номер тома и журнала. В случае, если этот номер является внешним идентификационным номером (т.е. он изображён на самом контейнере), то Боб сразу сможет его восстановить. Если встраивается просто код и Боб знает порядок формирования уникального номера, тогда вначале он понимает, что вместо U должна быть T, и получит T31N1, или T38N1, или T31N3, или T38N3. Далее он может прибегнуть к анализу самого контейнера и понять, что контейнер относится к T38N1.

Если в случае передачи какого-либо произвольного текста в контейнере и последующего его восстановления из ЦВЗ Боб обнаружил «не закрашенные» пиксели, тогда для полного восстановления этого текста ему придётся прибегнуть к лексико-грамматическому и смысловому анализам, при помощи которых удастся восстановить текст.

Следует заметить, что при помощи одного и того же ключа Алиса может передать Бобу два разных сообщения в двух разных стегоконтейнерах. Это осуществимо следующим образом: Алиса передаёт Бобу некую информационную последовательность, и пусть её бинарный код 01001110. На рис. 7 приведены «закрашенные» пиксели для определения первой встроенной информационной последовательности в первом контейнере.

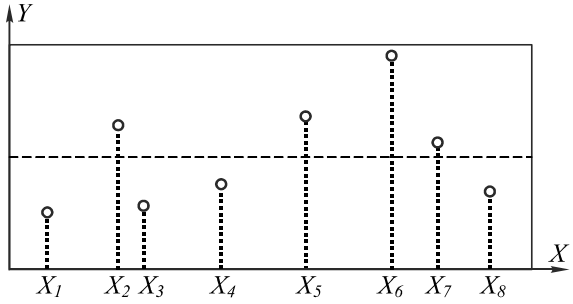

Рис. 7. «Закрашенные» пиксели для определения первой встроенной информационной последовательности в первом контейнере

Предположим, Бобу удалось восстановить первую встроенную информационную последовательность. Заметим, что для восстановления встроенной информационной последовательности Боб хранит координаты «закрашенных» пикселей по оси X. Далее Алиса передаёт Бобу другую информационную последовательность, например, её бинарный код 101010. Следует заметить, что длина бинарного кода второй информационной последовательности не должна превышать длины бинарного кода первой информационной последовательности. В случае, если бинарный код второй информационной последовательности короче, чем бинарный код первой информационной последовательности, то при восстановлении второй информационной последовательности полученная восстановленная часть от первой информационной последовательности игнорируется. Длина второго контейнера не должна быть меньше длины первого. На рис. 8 приведены «закрашенные» точки для определения второй встроенной информационной последовательности во втором контейнере.

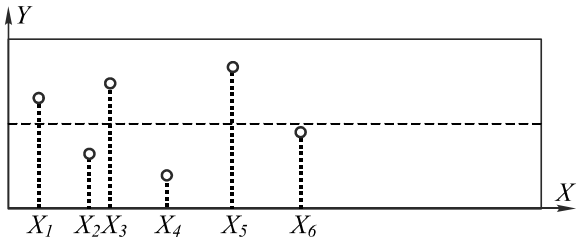

Рис. 8. «Закрашенные» пиксели для определения второй встроенной информационной последовательности во втором контейнере

Понятно, что для передачи второго сообщения с тем же ключом, что и для первого сообщения, во втором контейнере осуществляется формирование нового второго ЦВЗ на основании первого ЦВЗ.

Закрашенные точки с координатами X_1, $X_2,\ldots,X_n$, необходимые для передачи сообщения, смещаются на расстояния по оси Y, сгенерированные с помощью датчика случайных чисел, который также является частью ключевой информации, так, чтобы сохранилось равенство $R_1 = R_2$ (R_1, R_2 – суммы расстояний от «закрашенных» точек до оси X при встраивании первого ЦВЗ в первый контейнер и встраивании второго ЦВЗ во второй контейнер соответственно).

Идейно близок предлагаемому авторами методу метод PatchWork. Основным отличием является изменение яркостей пикселей при реализации последнего. По сути область этих изменений ограничена, так как, например, в соответствии со стандартом МСЭ-R BT.601) [20] I – значение яркости пикселя определяется по формуле

$I = 0,299 \cdot R + 0,587 \cdot G + 0,114 \cdot B$,

где: R, G, B – красный, зелёный и синий каналы этого пикселя соответственно, тогда I изменяется в пределах $[0,255]$. В предлагаемом авторами способе изменения происходят в рамках области самого изображения (координатной области), причём если смещение выходит за рамки изображения, то осуществляется переход в начало соответствующей смещению оси координат. Помимо этого, в качестве инструмента обнаружения встроенного в изображение ЦВЗ по методу PatchWork можно использовать локальную интерполяцию (т.е. задействовать локальные методы анализа). В предлагаемом же авторами способе, по всей видимости, нет локального метода обнаружения ЦВЗ, что отчасти подтверждается применением метода кластеризации *к-средних* [24].

Анализ сложности распознавания наличия цифрового водяного знака и содержащейся в нём информации

Рассмотрим вопрос: насколько трудна задача распознавания наличия водяного знака или ЦВЗ в идеальных для атакующего случаях?

Пусть заданы $2H$ «закрашенных» пикселей в документе и известно, что суммарное расстояние до оси X от этих пикселей равно $2R$. Необходимо разделить это множество «закрашенных» пикселей на два подмножества так, чтобы суммарные расстояния для пикселей в каждом полученном подмножестве до оси X были равны R. Если атакующему удастся это сделать, то он с некоторой вероятностью может предположить, что на документ нанесён ЦВЗ.

При добавлении значимого числа шумовых закрашенных пикселей задача становится переборной и экспоненциальной по сложности. Так, зная лишь сумму R, для поиска значений координат y_{ij}', сумма которых даёт R, необходимо осуществить перебор. В этом случае множество решений конечно и каждый выбор набора координат y_{ij}' осуществляется на основе решения задачи о ранце (рюкзаке). В свою очередь, задача о ранце относится к классу *NP-задач* и является *NP-полной*, что доказывается путём сведения к задаче о ранце *NP-полной* задачи разбиения (задача о камнях) [25], задачи Джонсона для трёх и более станков [26], канонической задачи однопроцессорного обслуживания потока заявок [27, 28].

Более того, при решении задачи о ранце можно прибегнуть к методу динамического программирования, при использовании которого строится сеть, что позволит свести задачу о ранце к задаче по нахождению максимально длинного пути в сети (графе) [29]. В случае, если в сети (графе) есть гамильтонов цикл, то данная задача будет иметь решения, но не обязательно, что найденные значения y_{ij}' будут выбраны правильно.

В случае, если значения координат y_{ij}' таковы, что сумма их даёт R и известно, что такой набор единственен, то данную задачу можно отнести к классу $co-NP$, т.е. к классу задач, дополнение к которым принадлежит классу NP. Аналогичная сложность получается, если необходимо показать, что заданы только шумовые точки. Мы получаем перифраз известной задачи из класса $co-NP$: показать, что в графе нет гамильтонова цикла.

Другая попытка анализа стойкости возможна на применении кластерного анализа для пикселей, например, расположенных на рис. 4. Так как смещение по оси X осуществляется по принципу, описанному выше, где предполагается так называемый перенос в начало/конец (в зависимости от сформированного произвольным образом числа) координаты x, то в целях оценки степени разброса смещённых пикселей возможно прибегнуть к методу кластеризации *к-средних* (k-means) [24], т.е. выявлению сходимости данного метода. Основной целью осуществляемого кластерного анализа является выделение в исходных данных таких однородных подмножеств (групп), чтобы объекты внутри этих групп были похожи в известном смысле друг на друга, а объекты из разных групп – не похожи. Выделенные с помощью кластерного анализа изолированные группы можно трактовать как качественно различные. Например, в соответствии с рис. 4 имелось H=40 исходных пикселей, далее было выполнено смещение данных пикселей в соответствии со способом, описанным выше, их стало $2H=80$. Таким образом, с помощью метода к-средних определяется возможность выявления 40 качественно различных групп, в каждую из которых не входят исходный и соответствующий ему смещённый пиксель.

На рис. 9 приведён вариант осуществления разбиения на 40 кластеров.

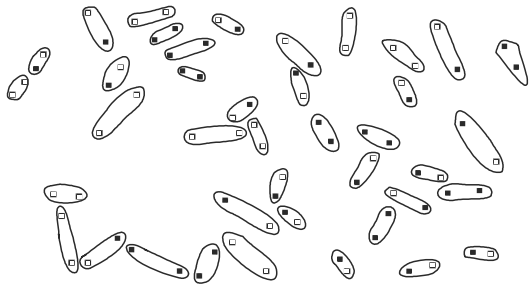

Рис. 9. Кластеризация методом к-средних

С помощью разработанной программы определено 40 кластерных центров, но в полученных кластерах по методу к-средних не содержится исходного и соответствующего ему смещённого пикселя. Можно говорить, что осуществляется достаточно хороший разброс пикселей в пределах исходного документа и с помощью кластерного анализа задача не решается.

Практическое применение предлагаемого способа

Предлагаемый авторами способ может использоваться для идентификации заранее зарегистрированных изделий, включая встраивание в ЦВЗ индивидуальных номеров каждого изготовленного изделия и осуществление последующей маркировки каждого изделия в процессе его изготовления.

Точнее процесс можно описать следующим образом: при изготовлении и упаковке продукции осуществляется присвоение индивидуального номера каждому товару. Затем, в соответствии с описанным выше авторами способом, формируется ЦВЗ со встроенным в него индивидуальным номером. Например, ЦВЗ может внедряться в штрих-код товара. При продаже продавец осуществляет считывание самого штрих-кода и встроенного в него ЦВЗ и данные о проданном товаре передаются в специальную базу.

Покупатель после вскрытия упаковки обнаруживает присвоенный данному товару индивидуальный номер. Затем, например, при помощи камеры мобильного устройства осуществляет считывание ЦВЗ и встроенной в него информации, после этого осуществляет сверку номера на упаковке и номера, получен-

ного после распознавания ЦВЗ. Если они совпадают, то можно с долей уверенности заявить о подлинности продукции.

В случае, если кто-либо захочет осуществить подделку продукции, то он сможет подделать лишь единичные экземпляры, которые легко обнаружатся покупателем при распознавании ЦВЗ (например, находясь у прилавка магазина) и обращении к серверу с запросом о продаже продукта. И вторым эшелоном проверки является вскрытие упаковки продукции и обнаружение там кода, соответствующего полученному при распознавании ЦВЗ мобильным устройством.

Внедрение ЦВЗ-меток можно осуществлять в штрих-код, например, печатая едва заметные жёлтые точки, как в технологии проставления меток (жёлтых точек) цветными лазерными принтерами на каждой печатаемой ими странице [13]. Также возможно располагать сформированные метки просто на белом фоне, как и любой другой код (штрих-код, QR-код).

Заключение

В данной статье был предложен универсальный способ формирования водяного знака как для физических, так и для электронных документов, кроме того, встраиваемый водяной знак способен нести в себе какую-либо информацию, например, определённый номер документа или текст.

Произведён предварительный анализ сложности распознавания цифрового водяного знака и содержащейся в нём встроенной информации.

Для демонстрации предлагаемого способа была разработана программа, реализующая описанные выше действия.

Литература

1. ГОСТ Р 34.10-2001 Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи [Электронный ресурс]. – Режим доступа: http://www.complexdoc.ru/pdf/ГОСТ%20Р%2034.10-2001/gost_r_34.10-2001.pdf. – Дата обращения: 06.02.2013.
2. **Cox, I.J.** Digital watermarking and steganography / I.J. Cox, M. Miller, J. Bloom, J. Fridrich. – San Francisco: Morgan KaufmannPublishing, 2008. – 624 p.
3. **Fridrich, J.** Methods for Tamper Detection in Digital Images / J. Fridrich // Proceedings of ACM Workshop on Multimedia and Security. –1999. – Vol. 1 – P. 19-23.
4. Википедия – свободная энциклопедия. Least Significant Bit, наименьший значащий бит [Электронный ресурс]. – Режим доступа: http://ru.wikipedia.org/wiki/Стеганография#.D0.9C.D0.B5.D1.82.D0.BE.D0.B4_LSB. – Дата обращения: 07.02.2013.
5. **Moller, S.** Computer Based Steganography: How It Works And Why Therefore Any Restriction On Cryptography Are Nonsense, At Best / S. Moller, A. Pfitzmann, I. Stirand // Information Hiding: First International Workshop «InfoHiding'96», Springer as Lecture Notes in Computing Science. – 1996. – Vol.1174. – P.7-21.
6. **Aura, T.** Practical Invisibility In Digital Communication / T. Aura // Information Hiding: First International Workshop «InfoHiding'96», Springer as Lecture Notes in Computing Sciencею – 1996. – Vol.1174. – P. 265-278.
7. **Хорошко, В.О.** Основы компьютерной стеганографии: уч. пособие для студентов и аспирантов / В.О. Хорошко, О.Д. Азаров, М.Э. Шелест. – Винница: ВДТУ, 2003. – 143 с.
8. Википедия – свободная энциклопедия. Помехоустойчивое кодирование [Электронный ресурс]. – Режим доступа: http://ru.wikibooks.org/wiki/Помехоустойчивое_кодирование. – Дата обращения: 07.02.2013.
9. **Грибунин, В.Г.** Цифровая стеганография / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев. – М.: Солон-пресс: Пандора -1, 2002. – 261 с.
10. **Конахович, Г.Ф.** Компьютерная стеганография. Теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. – Киев: МК-Пресс, 2006. – 288 с.
11. **Bender, W.** Techniques for Data Hiding / W. Bender, D. Gruhl, N. Morimoto, A. Lu // IBM Systems Journal. – 1996. – Vol. 35. – P. 313-336.
12. **Bender, W.** Applications for Data Hiding / W. Bender, W. Butera, D. Gruhl, R. Hwang, F.J. Paiz, S. Pogreb // IBM Systems Journal. – 2000. – Vol. 39, No.3&4. – P. 547-568.
13. Electronic frontier foundation. DocuColor Tracking Dot Decoding Guide [Электронный ресурс]. – Режим доступа: http://w2.eff.org/Privacy/printers/docucolor/. – Дата обращения: 12.03.2013.
14. Electronic frontier foundation. List of Printers Which Do or Do Not Display Tracking Dots [Электронный ресурс]. – Режим доступа: https://www.eff.org/pages/list-printers-which-do-or-do-not-display-tracking-dots. – Дата обращения: 12.03.2013.
15. Википедия – свободная энциклопедия. Водяной знак [Электронный ресурс]. – Режим доступа: http://ru.wikipedia.org/wiki/Водяной_знак. – Дата обращения: 20.03.2013.
16. Большой филателистический словарь / под ред. Н. И. Владинца, В. А. Якобса. – М.: Радио и связь, 1988. – 320 с.
17. **Shamir, A.** How to share a secret / A. Shamir // Communications of the ACM 22. – 1979. – P. 612-613.
18. **Файзуллин, Р.Т.** Алгоритм разделения секрета с использованием принципиально малой части секрета в качестве ключа / Р.Т. Файзуллин, И.Р. Файзуллин, О.Т. Данилова // Вестник Тюменского государственного университета. – 2011. - № 7. – С. 175-179.
19. **Сагайдак, Д.А.** Модели схем разделения секрета в системах передачи видеоинформации / Д.А. Сагайдак, Р.Т. Файзуллин // Компьютерная оптика – 2013. – Т.1, № 1. – С. 105-112.
20. Recommendation ITU-R BT.601-4. Encoding parameters of digital television for studios [Электронный ресурс]. – Режим доступа: http://www-inst.eecs.berkeley.edu/~cs150/Documents/ITU601.PDF. – Дата обращения: 20.03.2013.
21. **Kerckhoffs, A.** La cryptographie militaire / A. Kerckhoffs // Journal des Sciences Militaries. – 1883. – Vol. IX. – P. 5-38, 161-191.
22. **Вентцель, Е.С.** Теория вероятностей: учебное по для вузов / Е.С. Вентцель. – М.: Высшая школа, 1999. – 576 с.
23. **Гурманов, В.Е.** Теория вероятностей и математическая статистика / В.Е. Гурманов – М.: Высшая школа, 2003. – 479 с.
24. **Гэри, М.** Вычислительные машины и труднорешаемые задачи / М. Гэри, Д. Джонсон. – М.: Мир, 1982. – 416 с.

25. **Коган, Д.И.** Динамическое программирование и дискретная многокритериальная оптимизация: учебное пособие / Д.И. Коган. – Н. Новгород: Изд-во Нижегородского университета, 2004. – 150 с.
26. **Klamroth, K.** Dynamic programming approaches to the multiple criteria knapsack problem / K. Klamroth, M. M. Wiecek // Naval Research Logistics 47. – 2000. – P. 57–76.
27. **Липский, В.** Комбинаторика для программистов / В. Липский. – М.: Мир, 1978. – 213 с.
28. **Бурков, В.Н.** Прикладные задачи теории графов / В.Н. Бурков, И.А. Горгидзе, С.Е. Ловецкий. – Тбилиси: Мецниереба, 1974. – 234 с.
29. **Steinhaus, H.** Sur la division des corps matériels en parties / H. Steinhaus // Bull. Acad. Polon. Sci. – 1956. – Vol. IV, C1. III. – P. 801-804.

References

1. GOST R 34.10-2001 Cryptographic protection of information. The processes of generation and verification of digital signature [Electronic resource]. – Mode of access: http://www.complexdoc.ru/pdf/ГОСТ%20Р%2034.10-2001/gost_r_34.10-2001.pdf. – Access Date: 06.02.2013.
2. **Cox, I.J.** Digital watermarking and steganography / I.J. Cox, M. Miller, J. Bloom, J. Fridrich. – San Francisco: Morgan KaufmannPublishing, 2008. – 624 p.
3. **Fridrich, J.** Methods for Tamper Detection in Digital Images / J. Fridrich // Proceedings of ACM Workshop on Multimedia and Security. –1999. – Vol. 1 – P. 19-23.
4. Wikipedia, the free encyclopedia. Least Significant Bit, LSB [Electronic resource]. – Mode of access: http://ru.wikipedia.org/wiki/%D0%A1%D1%82%D0%B5%D0%B3%D0%B0%D0%BD%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F#.D0.9C.D0.B5.D1.82.D0.BE.D0.B4_LSB. – Access Date: 07.02.2013.
5. **Moller, S.** Computer Based Steganography: How It Works And Why Therefore Any Restriction On Cryptography Are Nonsense, At Best / S. Moller, A. Pfitzmann, I. Stirand // Information Hiding: First International Workshop «InfoHiding'96», Springer as Lecture Notes in Computing Science. – 1996. – Vol.1174. – P.7-21.
6. **Aura, T.** Practical Invisibility In Digital Communication / T. Aura // Information Hiding: First International Workshop «InfoHiding'96», Springer as Lecture Notes in Computing Sciencею – 1996. – Vol.1174. – P. 265-278.
7. **Khoroshko, V.O.** Fundamentals of computer steganography: textbook for undergraduate and postgraduate / V.O. Khoroshko, O.D. Azarov, M.E. Shelest. – Vinnitsa: "VDTU" Publisher, 2003. – 143 p. – (In Russian).
8. Wikipedia, the free encyclopedia. Error Coding [Electronic resource]. – Mode of access: http://ru.wikibooks.org/wiki/%D0%9F%D0%BE%D0%BC%D0%B5%D1%85%D0%BE%D1%83%D1%81%D1%82%D0%BE%D0%B9%D1%87%D0%B8%D0%B2%D0%BE%D0%B5_%D0%BA%D0%BE%D0%B4%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5. – Access Date: 07.02.2013. – (In Russian).
9. **Gribunin, V.G.** Digital steganography / V.G. Gribunin, I.N. Onkov, I.V. Turintsev. – Moscow: "Solon-press" Publisher: Pandora 1, 2002. – 261 p. – (In Russian).
10. **Konahovich, G.F.** Computer steganography. Theory and practice / G.F. Konahovich, A.U. Puzyrenko. – Kiev: "MK Press Publisher", 2006. – 288 p. . – (In Russian).
11. **Bender, W.** Techniques for Data Hiding / W. Bender, D. Gruhl, N. Morimoto, A. Lu // IBM Systems Journal. – 1996. – Vol. 35. – P. 313-336.
12. **Bender, W.** Applications for Data Hiding / W. Bender, W. Butera, D. Gruhl, R. Hwang, F.J. Paiz, S. Pogreb. // IBM Systems Journal. – 2000. – Vol. 39, No.3&4. – P. 547-568.
13. Electronic frontier foundation. DocuColor Tracking Dot Decoding Guide [Electronic resource]. – Mode of access: http://w2.eff.org/Privacy/printers/docucolor/. – Access Date: 12.03.2013.
14. Electronic frontier foundation. List of Printers Which Do or Do Not Display Tracking Dots [Electronic resource]. – Mode of access: https://www.eff.org/pages/list-printers-which-do-or-do-not-display-tracking-dots. – Access Date: 12.03.2013.
15. Wikipedia, the free encyclopedia. Watermark [Electronic resource]. - Mode of access: http://ru.wikipedia.org/wiki/%D0%92%D0%BE%D0%B4%D1%8F%D0%BD%D0%BE%D0%B9_%D0%B7%D0%BD%D0%B0%D0%BA. - Access Date: 20.03.2013. . – (In Russian).
16. Large philatelic dictionary / ed. N.I. Vladintsa, V.A. Jacobs. – Moscow: "Radio and Communications" Publisher, 1988. – 320 p.
17. **Shamir, A.** How to share a secret / A. Shamir // Communications of the ACM 22. – 1979. – P. 612-613.
18. **Faizullin, R.T.** Secret sharing algorithm using essentially small part as a secret key / R.T. Faizullin, I.R. Faizullin, O.T. Danilova // Bulletin of the Tyumen State University. – 2011. – № 7. – P. 175-179. . – (In Russian).
19. **Sagaidak, D.A.** Models of secret sharing schemes in the communications, video / D.A. Sagaidak, R.T. Faizullin // Computer Optics – 2013. – V. 1, № 1. – P. 105-112. – (In Russian).
20. Recommendation ITU-R BT.601-4. Encoding parameters of digital television for studios [Electronic resource]. – Mode of access: http://www-inst.eecs.berkeley.edu/~cs150/Documents/ITU601.PDF. – Access Date: 20.03.2013.
21. **Kerckhoffs, A.** La cryptographie militaire / A. Kerckhoffs // Journal des Sciences Militaries. – 1883. – Vol. IX. – P. 5-38, 161-191.
22. **Wentzel, E.S.** Probability theory: educational software for schools / E.S. Wentzel. – Moscow: "Higher School" Publisher, 1999. - 576 p.
23. **Gurmanov, V.E.** Probability theory and mathematical statistics / V.E. Gurmanov – Moscow: "Higher School" Publisher, 2003. - 479 p. – (In Russian).
24. **Gary, M.** Computers and intractability of the problem / M. Gary, D. Johnson. – Moscow: "Mir" Publisher, 1982. – 416 p.
25. **Kogan, D.I.** Dynamic programming and discrete multi-objective optimization: a training manual / D.I. Kogan. – Nizhny Novgorod: Publishing House of the Nizhny Novgorod University, 2004. – 150 p. – (In Russian).
26. **Klamroth, K.** Dynamic programming approaches to the multiple criteria knapsack problem / K. Klamroth, M. M. Wiecek // Naval Research Logistics 47. – 2000. – P. 57–76.
27. **Lipski, W.** Combinatorics for Programmers / W. Lipsky. – Moscow: "Mir" Publisher, 1978. – 213 p. – (In Russian).
28. **Burkov, V.N.** Applied problems in graph theory / V. N. Burkov, I.A. Gorgidze, S.E. Lovetskiy. – Tbilisi: "Metsniereba" Publisher, 1974. – 234 p. – (In Russian).
29. **Steinhaus, H.** Sur la division des corps matériels en parties / H. Steinhaus // Bull. Acad. Polon. Sci. – 1956. – Vol. IV, C1. III. – P. 801-804.

METHOD OF FORMING A DIGITAL WATERMARK FOR PHYSICAL AND ELECTRONIC DOCUMENTS

D.A. Sagaydak, R.T. Faizullin
Omsk State Technical University

Abstract

In this paper we proposed a universal method for forming the watermark for both physical and electronic documents. Such a watermark can be used for authentication of documents, as well as for secure communication. For both cases we described the procedure for exchange of information between two parties. The analysis of the complexity of detecting the presence of the watermark and extracting the embedded information by a third party was performed, and it showed operability of the proposed method.

Key words: actual physical document, the authenticity of electronic documents, steganography, stegosystem, stegokonteyner, digital watermark (DW), a cliche, the pixel representation of the image.

Сведения об авторах

Сагайдак Дмитрий Анатольевич, аспирант Омского государственного технического университета кафедры комплексной защиты информации. Область научных интересов: криптография, компьютерное моделирование, математические расчёты, программирование.

E-mail: *sagaydak.dmitriy@gmail.com* .

Dmitriy Anatolyevich Sagaydak, a graduate school student of Omsk State Technical University of Complex Protection of Information department. Research interests: cryptography, computer simulations, mathematical calculations, programming.

Файзуллин Рашит Тагирович, доктор технических наук (1999), профессор Омского государственного технического университета кафедры комплексной защиты информации. В списке научных работ Р.Т. Файзуллина более 100 статей, 2 монографии.

E-mail: *frt@omgtu.ru* .

Rashit Tagirovich Faizullin, Doctor of Technical Sciences (1999), professor of Omsk State Technical University of Complex Protection of Information department. He is co-author of more when 100 scientific papers, 2 monographs.

Поступила в редакцию 15 апреля 2013 г.