(19) Евразийское патентное ведомство

(11) 044006 (13) B1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2023.07.18

(21) Номер заявки
201992662

(22) Дата подачи заявки
2019.12.06

(51) Int. Cl. ***G06F 21/00*** (2013.01)

(54) СПОСОБ ВНЕСЕНИЯ ЦИФРОВЫХ МЕТОК В ЦИФРОВОЕ ИЗОБРАЖЕНИЕ И УСТРОЙСТВО ДЛЯ ОСУЩЕСТВЛЕНИЯ СПОСОБА

(31) **2019137214**
(32) **2019.11.20**
(33) **RU**
(43) **2021.05.31**

(56) US-B2-8942413
US-B2-8712094
US-B1-6807285
US-B1-8806558

(71)(73) Заявитель и патентовладелец:
ПУБЛИЧНОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО "СБЕРБАНК РОССИИ" (ПАО СБЕРБАНК) (RU)

(72) Изобретатель:
Крамаренко Сергей Михайлович (RU)

(74) Представитель:
Герасин Б.В. (RU)

(57) Данное изобретение в общем относится к области кодирования и декодирования данных, а в частности к способу и устройству для внесения цифровых меток в цифровое изображение. Техническим результатом, достигаемым при решении вышеуказанной технической задачи, является обеспечение возможности автоматизированного формирования и внедрения в цифровое изображение цифровых меток. Указанный технический результат достигается благодаря осуществлению способа внесения цифровых меток в цифровое изображение, содержащего этапы, на которых получают кортеж данных, подлежащих внесению в виде цифровых меток в цифровое изображение, выводимое на экран устройства пользователя; определяют форму и максимально допустимую размерность символа цифровой метки; определяют форму и размерность внутренней матрицы пикселей базовой яркости символа цифровой метки; осуществляют формирование последовательности символов цифровых меток; формируют шаблон-матрицу, определяющую построчное расположение последовательности сформированных символов цифровых меток для вывода на экран; накладывают сформированную шаблон-матрицу на цифровое изображение; выводят цифровое изображение с наложенной упомянутой выше шаблон-матрицей на экран устройства пользователя.

044006 B1

044006 B1

Область техники

Данное техническое решение в общем относится к области кодирования и декодирования данных, а в частности к способу и устройству для внесения цифровых меток в цифровое изображение.

Уровень техники

Проблема защиты конфиденциальной информации (далее - КИ) от ее несанкционированного разглашения и распространения является не только важной и актуальной в коммерческих и государственных организациях в силу ценности информации как цифрового актива, но и прямым требованием действующего законодательства РФ о защите персональных данных, банковской, коммерческой и иных видов тайн.

Несанкционированное/неправомерное разглашение конфиденциальной информации может приводить для организаций как к репутационному ущербу (судебные иски, претензии, негативный опыт и отток клиентов, разрыв отношений с подрядчиками и партнерами), так и к прямым финансовым убыткам (штрафы регуляторов, компенсации клиентам и контрагентам, потеря доли рынка, недополучение прибыли в следствии приостановления/прекращения деятельности из-за отзыва лицензий и т.п.). Несмотря на развитие современных цифровых технологий и усовершенствование методов/средств защиты информации от несанкционированного доступа и разглашения, существование видового канала утечки информации было и остается наиболее рисковым, действующим и трудно предотвратимым каналом компрометации конфиденциальных сведений. Одновременно с этим, чрезвычайно трудоемким и ресурсозатратным является создание надежных процедур контроля утечек через видовой канал, которые бы позволили однозначно идентифицировать злоумышленника в произвольный момент времени, производившего несанкционированные действия при проведении фото, видео съемки экрана монитора при обработке КИ.

В современных условиях ведения бизнеса постоянно растет значимость информации, как одного из наиболее ценных активов организации, что диктует необходимость защищать как ИТ-системы, так и непосредственно сами конфиденциальные данные, обрабатываемые в таких системах, причем не только от внешних, но и от внутренних злоумышленников [1]. В частности, внутренние злоумышленники могут скомпрометировать конфиденциальные сведения, просто открыв электронный документ, файл с презентацией или таблицей, базу данных, сайт или приложение и сделав снимки экрана компьютера с помощью цифровой камеры или мобильного телефона. Такой способ копирования конфиденциальной информации позволит злоумышленнику избежать регистрации его действий штатными или дополнительными средствами защиты информации, используемыми в системах обработки КИ, в отличии от, например, отправки документа по электронной почте. Осуществление таких действий значительно затрудняет выявление и идентификацию злоумышленника. Даже наличие принятой в организации политики безопасности, запрещающей фото-видео копирование конфиденциальных сведений с экрана персонального компьютера (далее - ПК) не может полностью устранить угрозу неправомерного копирования и последующего несанкционированного раскрытия КИ. В целях минимизации описанного риска предлагается новый способ формирования и внедрения невидимых человеческому глазу цифровых меток (digital watermarking), внедряемых в изображение, выводимое на экран компьютера. Закодированная в цифровых метках информация содержит сведения о дате, времени, названии компьютера и логине пользователя, который осуществлял обработку информации, и может быть извлечена из копий изображений, полученных в результате неправомерного фотографирования таких сведений с экрана компьютера.

Эволюция технологий вотермаркирования развивалась от встраивания видимых меток в электронные документы, подготавливаемых как непосредственно на ПК, так и печатаемых на бумажных копиях документов средствами, встроенными в многофункциональные печатающие устройства, до встраивания невидимых человеческому глазу аффинных преобразований в произвольный цифровой контент, преобразованный из базовых, общеупотребимых форматов электронных документов (Microsoft Office, Adobe PDF и т.п.) в один из графических форматов (JPEG, PNG, TIFF и т.п.). Более ранние подходы к скрытому маркированию изображений, в основном [2, 11, 13], использовали способы размещения данных о водяных знаках путем их внедрения в младшие биты, отвечающие за цвет отдельных пикселей изображения. Получающиеся при этом небольшие изменения цвета изображения незаметны для человеческого глаза, но описываемые подходы скрытного вотермаркирования не предполагают случаев преобразования изображений, например, из цветного в черно-белое, что будет вполне приемлемо для злоумышленника, похищающего КИ, содержащуюся в тексте документа выводимого на экран ПК. В более перспективных подходах [9], когда защите подлежат непосредственно электронные документы, осуществляется их преобразование из общеупотребимых форматов в графические и одновременно с этим вносятся невидимые искажения непосредственно в изображение (аффинные преобразования), конверсия фотокопии такого защищенного документа в другой формат или преобразование цветного изображения в черно-белое - будет лишено смысла, так как фотокопия защищенного таким способом графического документа унаследует все внедренные аффинные преобразования. Однако, осуществляемая конверсия из одного формата в другой требует не только временных и ресурсных затрат мощностей ПК, хранения исходно маркируемых электронных документов в связке с артефактами вносимых аффинных преобразований в привязке к конкретному получателю уникальной копии, существования механизма индексирования содержимого для осуществления поиска по образцу скомпрометированного контента, но и трудоемкого инструментария

проведения расследований фактов компрометации документов, содержащих конфиденциальные сведения преимущественно в ручном или полуавтоматизированном режиме, что делает использование такого рода технологий ограниченными в масштабах больших предприятий, с числом работников, исчисляемых тысячами, и где электронный документооборот подразумевает обмен значительным числом конфиденциальных документов с большим числом получателей уникальных экземпляров электронных документов, защищенных с помощью внедренных в контент невидимых аффинных меток. При этом, процессы подготовки защищенных копий электронных документов, хранения артефактов сформированных преобразований, проведения расследований по фактам утечек, ставших известными службам безопасности организаций, без относительно затрат на выявление самих фактов утечки, могут быть крайне трудо/время затратными. Используемые при этом технологии внедрения невидимых аффинных преобразований имеют к тому же ограничения по числу подготавливаемых для каждого получателя уникальных, различимых между собой копий исходного конфиденциального документа.

Работы, например, Caronni [5], в которых осуществляется встраивание цифровой метки путем изменения яркости нескольких смежных пикселей, требует для извлечения данных из метки исходного изображения, в то время как в предложенном решении этого не требуется. Используемые в современной мультимедийной индустрии методы защиты цифрового контента путем внедрения цифровых меток в частотный спектр изображения [7, 18, 19] обеспечивают приемлемую скрытность для цветных изображений, но обычно проявляют себя демаскирующим образом в текстовых документах [12, 14]. Таким образом, вышеописанные способы внедрения цифровых меток не подходят для скрытного маркирования разнородного контента. Используемые синтаксические и семантические подходы к изменениям самого текста в электронных документах, путем, например, разделения текста на блоки слов или букв с последующим их перемещением или заменой, также являются непригодными для целей защиты КИ поскольку нельзя охватить все многообразие программ обработки текста для различных операционных систем, требуют больших вычислительных затрат, что ставит под сомнение их пригодность для обработки информации в режиме реального времени, и в любом случае, не охватывают случаи скрытого маркирования КИ, обрабатываемой в нетекстовых редакторах (например, в веб-формах сайтов или в БД).

Предложенное решение позволяет внести модификации в яркость видеоизображения воспроизводимого на экране ПК незаметно для пользователя. Изменение яркости видеоизображения осуществляется с учетом предопределенной пиксельной схемы - символа цифровой метки, изменение яркости некоторых пикселей которой по отношению к яркости базового видеоизображения зависит от того, какие данные подлежат кодированию (далее описанный процесс будем называть "цифровым маркированием"). Набор данных, используемых для однозначной идентификации электронной учетной записи пользователя, осуществлявшего обработку КИ на ПК, с точностью до даты и времени далее будем называть "цифровой меткой". Изобретение предназначено для защиты любой конфиденциальной информации, обрабатываемой пользователем ПК, независимо от формы ее представления (текст, графика, видео) и приложений, в которых осуществляется обработка, от несанкционированного копирования с экрана ПК с целью последующего неправомерного распространения или раскрытия таких сведений, компрометации иными любыми способами. Цифровое маркирование видеоизображения осуществляется скрытно, средствами специализированного программного обеспечения (далее - ПО), визуально невидимо для глаз пользователя ПК. Скрытность закодированных цифровых меток, внедренных в выводимое на экран ПК видеоизображение, достигается за счет того, что человеческий глаз, особенно в областях светлых тонов [3, 6], менее чувствителен к небольшим изменениям яркости, чем цифровые камеры фотоаппаратов или мобильных телефонов.

Обратный процесс, связанный с анализом дифференциалов яркости пикселей копии видеоизображения, полученного с экрана ПК, в результате которого определяется размер символа цифровой метки и последовательное (посимвольное) определение встроенных в видеоизображение данных, будем называть извлечением данных.

Принципиальным технологическим результатом изобретения является повышение защиты конфиденциальных сведений от несанкционированного копирования с экрана монитора ПК и их неправомерного распространения за счет обеспечения возможности установления точной даты, названия ПК и идентификации пользователя, допустившего утечку защищаемой информации, путем извлечения таких сведений из скрытых в изображении цифровых меток. В настоящей заявке раскрывается способ модификации видеоизображения, внесения невидимых человеческому глазу цифровых меток, а также способы обработки цифровых изображений, сделанных путем фотографирования и/или копирования экрана (screen shot), содержащих защищаемые сведения, извлечения встроенных данных, восстановления цифровых меток с целью установления источника и идентификации виновника утечки конфиденциальных сведений.

Предлагаемое изобретение не требует создания отдельной базы данных для хранения информации об уникальных характеристиках (артефактах), внедренных в видеоизображение цифровых меток, поскольку предполагается, что в ходе программной реализации все необходимые данные об названии ПК, логине пользователя, осуществившего успешный вход на ПК, а также дате и времени будут непосредственно получены на ПК и встроены в виде невидимых цифровых меток в выводимое на экран ПК видео-

изображение. В случаях проведения расследований по фактам утечки КИ, сотруднику службы безопасности достаточно будет получить копию (screenshot) или фото экрана ПК, сделанные злоумышленником, чтобы после обработки изображения программным способом восстановить вышеуказанные данные, внедренные в виде скрытых меток и тем самым однозначно идентифицировать как пользователя, так и ПК, на которым была осуществлена компрометация КИ, в конкретный момент времени.

Сущность изобретения

Технической проблемой или задачей, поставленной в данном техническом решении, является создание простого, незаметного для пользователей и надежного способа и устройства для внесения цифровых меток в цифровое изображение, содержащих информацию о дате, времени и обстоятельствах обработки КИ (например, наименование устройства и логин авторизованного на нем пользователя).

Техническим результатом, достигаемым при решении вышеуказанной технической задачи, является обеспечение возможности автоматизированного формирования и внедрения в цифровое изображение цифровых меток, сгруппированных из пикселей переменной яркости в последовательность символов, содержащих закодированную информацию, например, необходимую для проведения расследования и установления обстоятельств в случае утечки КИ путем несанкционированного копирования, в т.ч. через видовой канал (например, путем фотографирования экрана).

Указанный технический результат достигается благодаря осуществлению способа внесения цифровых меток в цифровое изображение, выполняемого по меньшей мере одним вычислительным устройством, содержащего этапы, на которых

получают кортеж данных, подлежащих внесению в виде цифровых меток в цифровое изображение, выводимое на экран устройства пользователя;

определяют форму (в виде попиксельного представления) и максимально допустимую размерность символа цифровой метки исходя из используемого пользователем разрешения экрана устройства;

на основе информации о форме и размерности символа цифровой метки определяют форму и размерность внутренней матрицы пикселей базовой яркости символа цифровой метки;

на основе данных, содержащихся в кортеже, представлении о форме и максимально допустимой размерности символа цифровой метки и форме и размерности внутренней матрицы пикселей базовой яркости символа цифровой метки осуществляют формирование последовательности символов цифровых меток;

исходя из используемого пользователем разрешения экрана устройства формируют шаблон-матрицу, определяющую построчное расположение последовательности сформированных символов цифровых меток для вывода на экран;

накладывают сформированную шаблон-матрицу на цифровое изображение, предназначенное для вывода на экран;

выводят цифровое изображение с наложенной упомянутой выше шаблон-матрицей, содержащей последовательность сформированных символов цифровых меток на экран устройства пользователя.

В одном из частных примеров осуществления способа дополнительно осуществляют помехоустойчивое кодирование полученного кортежа данных. В другом частном примере осуществления способа дополнительно выполняют этапы, на которых: для кортежа данных вычисляют контрольную сумму для проверки целостности данных; добавляют полученную контрольную сумму к кортежу данных.

В другом частном примере осуществления способа дополнительно определяют текущие параметры экрана, причем максимально допустимая размерность символа цифровой метки определяется с учетом текущих параметров экрана и размера кортежа данных.

В другом частном примере осуществления способа дополнительно собирают данные об устройстве пользователя, включающие: дату, установленную на устройстве пользователя; время, установленное на устройстве пользователя; идентификатор устройства пользователя; имя пользователя (LOGIN), осуществившего авторизацию на устройстве 10 пользователя; причем кортеж данных формируется из данных об устройстве пользователя.

В другом предпочтительном варианте осуществления заявленного решения представлено устройство внесения цифровых меток в цифровое изображение, содержащее по меньшей мере одного вычислительное устройство и по меньшей мере одно устройство памяти, содержащее машиночитаемые инструкции, которые при их исполнении по меньшей мере одним вычислительным устройством выполняют указанный выше способ.

Краткое описание чертежей

Признаки и преимущества настоящего изобретения станут очевидными из приводимого ниже подробного описания изобретения и прилагаемых чертежей.

На фиг. 1 представлены возможные сценарии компрометации конфиденциальных сведений.

На фиг. 2 представлен пример системы отображения данных.

На фиг. 3 представлены примеры символов цифровых меток.

На фиг. 4 представлены примеры исходного изображения экрана с и без накладываемых символов цифровых меток (яркость символов увеличена).

На фиг. 5 представлен пример общего вида вычислительного устройства.

Подробное описание изобретения

Ниже будут описаны понятия и термины, необходимые для понимания данного технического решения.

В данном техническом решении под системой подразумевается, в том числе компьютерная система, ЭВМ (электронно-вычислительная машина), ЧПУ (числовое программное управление), ПЛК (программируемый логический контроллер), компьютеризированные системы управления и любые другие устройства, способные выполнять заданную, четко определенную последовательность операций (действий, инструкций).

Под устройством обработки команд подразумевается электронный блок либо интегральная схема (микропроцессор), исполняющая машинные инструкции (программы).

Устройство обработки команд считывает и выполняет машинные инструкции (программы) с одного или более устройств хранения данных. В роли устройства хранения данных могут выступать, но не ограничиваясь, жесткие диски (HDD), флеш-память, ПЗУ (постоянное запоминающее устройство), твердотельные накопители (SSD), оптические приводы.

Программа - последовательность инструкций, предназначенных для исполнения устройством управления вычислительной машины или устройством обработки команд.

Кортеж данных - упорядоченный набор данных фиксированной длины. В подавляющем большинстве случаев внедренные в современных организациях административные, организационные и технические меры защиты КИ, как правило, не могут помешать злоумышленникам-инсайдерам [1] скопировать конфиденциальные сведения путем фотографирования с экрана ПК. Такие несанкционированные действия не оставляют никаких цифровых следов в журналах ПК, что не позволяет идентифицировать злоумышленника, как и установить сам факт фотографирования КИ.

Предлагаемый в изобретении подход предполагает покрытие двух следующих сценариев, изображенных на фиг. 1.

Сценарий 1: инсайдер-злоумышленник 1 делает фотоснимок конфиденциальной информации, отображаемой, например, на экране ПК 2, с помощью камеры мобильного телефона или фотоаппарата, затем пересылает и публикует файл в сети Интернет 3. Сценарий 2: инсайдер-злоумышленник 1 делает фотокопию, например, с экрана ПК 2 (например, через стандартную функцию print screen), затем пересылает и публикует файл в сети Интернет 3. В обоих случаях злоумышленник может скомпрометировать КИ, передав файл как в исходном, так и в преобразованном виде, путем применения специальных фотоэффектов (blur, noise, sharpen и т.п.) [4] или сжатия изображения через конверсию в изображение другого формата (например, из BMP в PNG или из RAW в JPEG), и тем самым цифровая копия изображения экрана приобретёт артефакты (ореол или пятна характерные для формата JPEG). Ситуация со сценарием 1 может быть усложнена тем, что фотографирование экрана может быть выполнено при плохом освещении, под углом (не перпендикулярно экрану ПК 2), с заранее предопределенным плохим качеством съемки. Кроме того, фотокопия может быть зашумлена вследствие особенностей работы аппаратно-программной реализации самой фотокамеры и получить как цветовой шум, так и шум светимости (зернистость). Наиболее простой для проведения расследований фактов утечки КИ вариант предполагает получение доступа к файлу с копией экрана по сценарию 2, т.е. к исходному неизмененному изображению или, в ряде случаев, к файлам, сохраненным на мобильном устройстве, например, изъятом у злоумышленника в ходе задержания правоохранительными органами. Но такие случае не могут считаться частыми, типовыми. В виду вышеизложенного, необходимо решить задачу по идентификации злоумышленника 1, допустившего компрометацию КИ, места (например, название ПК 2, на котором велась обработка) и времени только на основании анализа того изображения, которое было получено непосредственно из источника неправомерного размещения. Для решения вышеописанной задачи предлагается подход по внедрению скрытых (невидимых человеческому глазу) цифровых меток (знаков) в изображение, выводимое на экран ПК. Цифровая метка может содержать, например, такую закодированную информацию как: дата, время, имя ПК (название рабочей станции, с экрана которой была сделана копия КИ), а также имя пользователя (LOGIN), осуществившего авторизацию на данном ПК. В случае получения доступа к (измененной) фотокопии экрана, специалисты по компьютерным расследованиям или сотрудники безопасности организации смогут декодировать перечисленные выше сведения из цифровых меток и идентифицировать злоумышленника и рабочее место, на котором велась обработка КИ с точностью до даты и времени. Предлагаемый подход является перманентным по своей реализации, поскольку злоумышленник способен сделать снимок экрана в любое время, не на всех ПК могут стоять или функционировать средства защиты КИ, отсутствовать организационные или административные контрольные процедуры, поэтому цифровая метка должна присутствовать при обработке любой КИ в любой форме представления независимо от используемых приложений. Внедряемый в выводимое на экран монитора изображение цифровая метка должна быть незаметной для глаза пользователя как на текстовых документах, так и не добавлять видимых артефактов в графику, которые бы могли бы стать демаскирующими элементами самого изображения. Описываемый подход предполагает внедрение робастных к искажениям копии изображения цифровых меток, позволяющих, при этом, слепое извлечение закодированной в них информации, то есть извлечение данных о дате, времени, имени ПК и пользователе без оригинала

изображения. В соответствии со схемой, приведенной на фиг. 2, система отображения данных включает: устройство 10 пользователя и устройство 100 внесения цифровых меток в цифровое изображение. Устройство 10 пользователя может выполнено на базе вычислительного устройства, оснащенного средствами вывода цифровых изображений, и может представлять, например, портативный или стационарный компьютер, планшет, мобильный телефон, смартфон или прочее устройство.

Устройство 100 внесения цифровых меток в цифровое изображение может быть реализовано на базе программно-аппаратных средств устройства 10 пользователя, либо представлять самостоятельное устройство, подключаемое к упомянутому устройству 10 по проводной и/или беспроводной связи и содержащее по меньшей мере одно вычислительное устройство. Устройство 100 внесения цифровых меток может содержать: модуль 101 сбора данных, модуль 102 обработки данных, модуль 103 кодирования данных и модуль 104 вывода данных. Указанные модули могут быть реализованы на базе программно-аппаратных средств устройства 100, сконфигурированные таким образом, чтобы выполнять приписанные этим модулям в настоящей заявке функции. Согласно заложенному разработчиком в модуль 101 сбора данных программному алгоритму, модуль 101 обращается к устройству 10 пользователя для сбора сведений о текущих параметрах экрана, например, о разрешении экрана, и данных об устройстве 10 пользователя, которые могут включать

дату, установленную на устройстве 10 пользователя;

время, установленное на устройстве 10 пользователя;

идентификатор устройства 10 пользователя, например, имя упомянутого устройства;

имя пользователя (LOGIN), осуществившего авторизацию на устройстве 10 пользователя.

Собранные данные об устройстве 10 пользователя объединяются модулем 101 сбора данных в кортеж данных, подлежащих внесению в виде цифровых меток в цифровое изображение, выводимое на экран устройства пользователя, например, вида:

||ггмсддччмнFQDN|UserLogin,

где:

- "|" - специальный символ, указывающий на начало кортежа данных и выступающий в качестве разделителя полей FQDN и UserLogin, 0x7C (код символа "|" в шестнадцатеричном виде). Предполагается, что указанный спецсимвол не может быть использован в полях FQDN и UserLogin;

- ггмсддччмн - 10 байт данных фиксированной длины о текущем годе, месяце, дне, часе и минутах, полученные из операционной системы устройства 10 пользователя, на котором осуществляется обработка КИ, где в свою очередь:

гг - последние 2 цифры текущего года, например, для 2019 года будет записано значение "19";

мс - месяц;

дд-день;

чч - час;

мн - минуты;

FQDN - Fully Qualified Domain Name или полное имя устройства 10 пользователя [8], имеет ограничение в 255 байт, например: WS-CA111.company.com;

UserLogin - имя пользователя устройства 10, который осуществил успешную аутентификацию на рабочей станции, данное поле имеет ограничение в 20 байт в случае использования атрибута "sAMAccountName" в домене Microsoft Active Directory [10]. В случае использования атрибута "userPrincipalName" и отведения в домене под имя пользователя устройства 10 64 байт, предлагается обрезать имя пользователя до 20 байт, так как основным идентифицирующим факт обработки КИ признаком будет FQDN.

Таким образом, общая длина кортежа данных, подлежащих кодированию (payload), в приведенном выше примере, в пределе не будет превышать 288 байт. Далее сведения о текущих параметрах экрана и кортеж данных модуль 101 сбора данных передает в модуль 102 обработки данных, который по сформированному кортежу данных вычисляет контрольную сумма для проверки целостности данных - циклический избыточный код (англ. Cyclic redundancy check, CRC), например, по алгоритму CRC32 [17]. Полученную контрольную сумму упомянутый модуль 102 добавляет к кортежу данных, после чего получившийся кортеж данных в 292 байта передается в модуль 103 кодирования данных, который осуществляет помехоустойчивое кодирование полученного кортежа данных с использованием, например, адаптированного сверточного кодера и передает кортеж кодированных данных в модуль 104 вывода данных. Параметры, необходимые для работы модуля 103, в частности, используемый алгоритм помехоустойчивого кодирования и соответствующие ему настройки, могут быть заранее заданы разработчиком устройства 100 внесения цифровых меток исходя из соотношения мощности кодера по исправлению ошибок, которые могут возникнуть в процессе извлечения данных из копии изображения, к сложности и трудозатратности программной реализации выбранного помехоустойчивого кодека (кодера-декодера), а также доступности к реализации соответствующих алгоритмов с учетом соблюдения их патентной защиты.

Дополнительно, модуль 102 обработки данных выполнен с возможностью определения формы (в виде попиксельного представления) и максимально допустимой размерности символа цифровой метки (примеры которых приведены на фиг. 3) - т.е. расчета количества пикселей по вертикали и горизонтали,

образующих символ, например, на основе сведений о текущих параметрах экрана и размере кортежа данных, полученных из модуля 101. Для этого упомянутый модуль 102 на основе сведений о текущих параметрах экрана, в частности исходя из используемого пользователем разрешения экрана устройства 10, определяет общее количество пикселей, которое вместит экран, после чего определяет количество бит данных исходя из размера кортежа данных, подлежащих кодированию в виде символов цифровых меток. Далее модуль 102 определяет форму и максимально возможную размерность символа цифровой метки, при использовании которой все подлежащие кодированию данные (в виде последовательности бит кортежа данных) полностью могут быть размещены на экране в виде последовательно выводимых символов цифровых меток с построчным переносом по достижении предела горизонтального разрешения экрана, исходя из соотношения: один бит данных кодируется одним символом цифровой метки.

Примеры символов цифровой метки приведены на фиг. 3, в частности для размерностей 3×3 и 6×6 пикселей. Серым цветом на фиг. 3 показаны пиксели символа цифровой метки с базовой яркостью исходного изображения, черным цветом - пиксели с измененной (отличительной) яркостью. Информация о разрешениях экрана устройства 10 пользователя, соответствующих им формах цифровых меток и формах внутренней матрицы пикселей базовой яркости символа цифровой метки могут быть заранее заданы разработчиком устройства 100 внесения цифровых меток.

Согласно фиг. 3, на основе формы и рассчитанной максимально возможной размерности символа цифровой метки, упомянутый модуль 102 определяет форму и размерность внутренней матрицы пикселей базовой яркости символа цифровой метки, характеризующую количество пикселей с базовой яркостью, которое будет содержаться в символе цифровой метки. Информация о размерности символа цифровой метки и о размерности внутренней матрицы пикселей базовой яркости, соответствующей упомянутой размерности символа цифровой метки, может быть заранее задана в модуле 102 обработки данных разработчиком устройства 100 внесения цифровых меток. Так, например, для разрешения 2560×1440 точек экран вместит 3686400 пикселей. Для кортежа данных, длиной, к примеру, 289 байт = 2312 бит (без помехоустойчивого кодирования, но с CRC32), каждый бит, кодируемый посимвольно в выводимое на экран устройства 10 пользователя изображение, может быть отображен матрицей максимальной размерностью в: $\sqrt{3686400 \text{ пикселей} \div 2312 \text{ бит}} \approx 39 \text{ пикселей}$. Основываясь на полученной максимально допустимой размерности символа цифровой метки в модуле 102 принимается решение и о размерности внутренней матрицы пикселей базовой яркости, яркость которых будет отличаться от периметровых пикселей того же символа, исходя из следующих расчетов и ограничений. Согласно определенной на фиг. 3 квадратной форме символа цифровой метки (пиксельной матрицы), размер внутренней матрицы пикселей базовой яркости должен быть в три раза меньше максимально допустимой размерности символа. Так, для приведенного выше примера, исходя из рассчитанной максимальной размерности символа в 39 пикселей, размер внутренней матрицы пикселей базовой яркости будет равен 39/3=13 пикселей. В случаях, когда рассчитанная максимальная размерность символа не будет кратна трем, при проведении вычисления размера внутренней матрицы пикселей базовой яркости необходимо осуществлять округление до ближайшего целого значения в сторону уменьшения.

В целях внесения в изображение информационной избыточности, для последующего восстановления данных из цифровых меток, предлагаемый подход предполагает адаптивное уменьшение пиксельной размерности символа от максимально возможного в сторону уменьшения, что повышает скрытность цифрового маркирования, потенциально позволяет восстанавливать данные по фрагменту копии изображения экрана, но уменьшает робастность цифровой метки к трансформационным преобразованиям изображения. Соответственно, информация о форме и рассчитанной размерности символа цифровой метки и о форме и размерности внутренней матрицы пикселей базовой яркости модулем 102 обработки данных передается в модуль 104 вывода данных.

Модуль 104 вывода данных, получив из модуля 103 кортеж кодированных данных, защищенных адаптивным помехоустойчивым кодером, и параметры символа цифровой метки, характеризующие форму и размерность символа цифровой метки и форму и размерность внутренней матрицы пикселей базовой яркости, осуществляет формирование последовательности символов цифровых меток, подлежащих встраиванию (яркостному наложению) в видеоизображение, выводимое на экран устройство 10 пользователя, в соответствии со следующими принципами.

В случае необходимости кодирования нулевого бита данных, пиксели, показанные на фиг. 3 черным, делаются по яркости менее интенсивными, чем яркость пикселей базового изображения. Для кодирования единичного бита, пиксели, показанные на фиг. 3 черным, делаются по яркости более интенсивными, чем яркость пикселей базового изображения. В работе M.Ramasubramanian [15] была описана модель восприятия изображения человеком, учитывающая разную чувствительность глаза к перепадам яркости в зависимости от яркости фона и от однородности. Расчет величины, на которую яркость периметровых пикселей символа цифровой метки должна отличаться от фона, чтобы человек не заметил отличия, может рассчитываться, например, на основе предложенной Ramasubramanian модели. После того, как в модуле 104 была сформирована последовательность символов цифровых меток, упомянутый модуль 104 на основе сведений о текущих параметрах экрана устройства 10 пользователя, в частности ис-

ходя из используемого пользователем разрешения экрана устройства, формирует шаблон-матрицу, определяющую построчное расположение последовательности подготовленных символов цифровых меток для вывода на экран устройства 10 пользователя. Таким образом, сформированная в модуле 104 шаблон-матрица состоит из пикселей переменной яркости размерностью, соответствующей текущим параметрам экрана устройства 10 пользователя. Далее модуль 104 вывода данных, используя упомянутый шаблон-матрицу, содержащий последовательность сформированных символов цифровых меток, осуществляет ее наложение с исходным цифровым изображением, после чего итоговое (с измененной яркостью определенных пикселей согласно упомянутому шаблону-матрицы) сформированное цифровое изображение направляется в устройство 10 пользователя, которое выполняет известными из уровня техники методами вывод изображения на экран устройства 10. Таким образом, обеспечивается достижение указанного технического результата, заключающегося в обеспечении возможности автоматизированного формирования и внедрения в цифровое изображение цифровых меток.

На фиг. 4 представлены примеры увеличенных копий исходного изображения фрагмента экрана с наложенной цифровой меткой и без цифровой метки (яркость символов увеличена). Соответственно на фиг. 4 представлены:

А. фрагмент копии изображения с наложенными символами цифровых меток увеличенной яркости;

Б. фрагмент копии исходного изображения без наложения символов цифровых меток.

За счет предварительного формирования кортежа кодируемых данных с частотой один раз в минуту (время кодируется с точностью до минуты) достигается экономия ресурсов устройства 100 внесения цифровых меток. При этом, модуль 101 сбора данных из операционной системы устройства 10 пользователя должен отслеживать ряд системных событий, связанных с входом/выходом пользователя из системы. В случае настройки модуля 101 на отслеживание событий блокировки/разблокировки экрана, перехода устройства 10 пользователя в спящий режим или режим гибернации, также станет возможным экономия ресурсов устройства 10 пользователя, поскольку наложение упомянутого выше шаблона-матрицы (оверлейной маски) будет лишено смысла по причине блокировки экрана ПК и невозможности для злоумышленника сделать фотокопию изображения. Таким образом, критичным с точки зрения реализации и ресурсоемким будет только процесс модификации выводимого на экран видеоизображения в соответствии с предсформированным яркостным попиксельным шаблоном.

Извлечение данных из цифровых меток осуществляется следующим образом. В ходе обратного преобразования символов цифровых меток в бинарную последовательность данных происходит попиксельный анализ дифференциалов яркости полученного в ходе расследования изображения экрана устройства 10 пользователя, например, экрана ПК. При этом, происходит определение размерности символа цифровой метки, например, путем проведения анализа яркости пикселей на полях копии электронного документа, не содержащих текста. Такой подход основан на том простом факте, что белый цвет и яркость фона явно доминируют в типичных текстовых документах, что позволяет использовать фон для определения локальных эталонных значений яркости для последующего декодирования символов цифровых меток. Установив размер символа цифровой метки происходит сравнение яркости центральных пикселей символа с их окружением. В случае, если яркость периметровых пикселей менее интенсивная, чем яркость центральных пикселей символа цифровой метки - регистрируется нулевой бит, в противоположном случае - единичный бит. Восстановленная по изображению бинарная последовательность данных подвергается помехоустойчивому декодированию, например, с использованием алгоритма Витерби [16], позволяющему находить и исправлять ошибки в восстановленном массиве данных, которые могут возникать как в ходе преобразования символов цифровых меток в бинарную последовательность, так и в следствии ухудшения качества копии изображения экрана ПК, применения специальных фотоэффектов или конверсии в изображение другого формата. Мощность помехоустойчивого декодирования по исправлению одиночных и блочных ошибок напрямую зависит от эффективности использованного алгоритма, избыточности, вносимой в защищаемый от искажения исходный бинарный массив данных. По итогам помехоустойчивого декодирования должен получиться кортеж данных размером до 292 байт, из которых последние 4 байта представляют собой контрольную сумму, вычисляемую по алгоритму CRC32. В случае совпадения рассчитанной контрольной суммы по начальным 288 байтам с 4 последними проверочными байтами принимается решение о полном и точном восстановлении данных о дате, времени, пользователе и названии ПК, на котором велась обработка КИ.

Таким образом, техническая задача, на решение которой направлено заявляемое изобретение, состоит в обеспечении дополнительной защиты любой обрабатываемой на ПК конфиденциальной информации, выводимой на экран ПК, независимо от формы представления и используемого при этом программного обеспечения, от несанкционированного раскрытия и распространения путем внедрения в изображение незаметных человеческому глазу цифровых меток, позволяющих однозначно идентифицировать как пользователя, так и ПК, на которым была осуществлена компрометация КИ, в конкретный момент времени. Решение поставленной технической задачи достигается тем, что программным образом реализуется робастный к преобразованиям фотокопий экрана ПК способ модификации яркости передаваемого на экран ПК видеоизображения, без видимого искажения для пользователя, во внедренных цифровых метках которого содержится закодированная с использованием эффективных помехоустойчивых

алгоритмов информация о дате, времени, названии ПК и логине пользователя, осуществившего вход в операционную систему ПК, на котором велась обработка КИ. Защита конфиденциальных сведений, обрабатываемых на ПК, с использованием вышеописанного подхода позволит реализовать точку контроля неправомерного фотокопирования информации с экрана ПК, обеспечив возможность установления места (названия ПК) и персоны, которая вела обработку КИ, с точностью до даты и времени, в ходе проведения расследования инцидентов, связанных с утечкой КИ. Технический эффект от предлагаемого изобретения представляет собой возможность получения сведений о фактах и канале утечки конфиденциальных сведений, обрабатываемых на ПК, непосредственно путем извлечения данных из копии скомпрометированного изображения, полученного путем фотографирования экрана ПК. В общем виде (см. фиг. 5) устройство 10 обработки данных процесса содержит объединенные общей шиной информационного обмена один или несколько процессоров (201), средства памяти, такие как ОЗУ (202) и ПЗУ (203), интерфейсы ввода/вывода (204), устройства ввода/вывода (205), и устройство для сетевого взаимодействия (206).

Процессор (201) (или несколько процессоров, многоядерный процессор и т.п.) может выбираться из ассортимента устройств, широко применяемых в настоящее время, например, таких производителей, как: Intel™, AMD™, Apple™, Samsung Exynos™, MediaTEK™, Qualcomm Snapdragon™ и т.п. Под процессором или одним из используемых процессоров в устройстве (200) также необходимо учитывать графический процессор, например, GPU NVIDIA или Graphcore, тип которых также является пригодным для полного или частичного выполнения способа, а также может применяться для обучения и применения моделей машинного обучения в различных информационных системах. ОЗУ (202) представляет собой оперативную память и предназначено для хранения исполняемых процессором (201) машиночитаемых инструкций для выполнение необходимых операций по логической обработке данных. ОЗУ (202), как правило, содержит исполняемые инструкции операционной системы и соответствующих программных компонент (приложения, программные модули и т.п.). При этом, в качестве ОЗУ (202) может выступать доступный объем памяти графической карты или графического процессора.

ПЗУ (203) представляет собой одно или более устройств постоянного хранения данных, например, жесткий диск (HDD), твердотельный накопитель данных (SSD), флэш-память (EEPROM, NAND и т.п.), оптические носители информации (CD-R/RW, DVD-R/RW, BlueRay Disc, MD) и др. Для организации работы компонентов устройства (200) и организации работы внешних подключаемых устройств применяются различные виды интерфейсов В/В (204). Выбор соответствующих интерфейсов зависит от конкретного исполнения вычислительного устройства, которые могут представлять собой, не ограничиваясь: PCI, AGP, PS/2, IrDa, FireWire, LPT, COM, SATA, IDE, Lightning, USB (2.0, 3.0, 3.1, micro, mini, type C), TRS/Audio jack (2.5, 3.5, 6.35), HDMI, DVI, VGA, Display Port, RJ45, RS232 и т.п. Для обеспечения взаимодействия пользователя с устройством (200) применяются различные средства (205) В/В информации, например, клавиатура, дисплей (монитор), сенсорный дисплей, тач-пад, джойстик, манипулятор мышь, световое перо, стилус, сенсорная панель, трекбол, динамики, микрофон, средства дополненной реальности, оптические сенсоры, планшет, световые индикаторы, проектор, камера, средства биометрической идентификации (сканер сетчатки глаза, сканер отпечатков пальцев, модуль распознавания голоса) и т.п.

Средство сетевого взаимодействия (206) обеспечивает передачу данных посредством внутренней или внешней вычислительной сети, например, Интранет, Интернет, ЛВС и т.п. В качестве одного или более средств (206) может использоваться, но не ограничиваться: Ethernet карта, GSM модем, GPRS модем, LTE модем, 5G модем, модуль спутниковой связи, NFC модуль, Bluetooth и/или BLE модуль, Wi-Fi модуль и др.

Дополнительно могут применяться также средства спутниковой навигации в составе системы (200), например, GPS, ГЛОНАСС, BeiDou, Galileo. Конкретный выбор элементов устройства (200) для реализации различных программно-аппаратных архитектурных решений может варьироваться с сохранением обеспечиваемого требуемого функционала.

Модификации и улучшения вышеописанных вариантов осуществления настоящего технического решения будут ясны специалистам в данной области техники. Предшествующее описание представлено только в качестве примера и не несет никаких ограничений. Таким образом, объем настоящего технического решения ограничен только объемом прилагаемой формулы изобретения.

Ссылки на литературу.

[1] https://encyclopedia.kaspersky.com/knowledge/recognizing-different-types-of-insiders/

[2] W. Bender, D. Gruhl, N. Morimoto, and A. Lu. Techniques for data hiding. IBM Syst. J., 35(3-4):313–336, Sept. 1996.

[3] Tom N. Cornsweet. Visual Perception. Academic Press, 1970.

[4] https://helpx.adobe.com/ru/photoshop/using/filter-effects-reference.html

[5] G. Caronni. Assuring ownership rights for digital images. In Verlaessliche ITSysteme, DUD-Fachbeitraege, pages 251–263. Vieweg+Teubner Verlag, 1995.

[6] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker. Digital Watermarking and Steganography. Morgan Kaufmann, 2007.

[7] I. J. Cox, J. Kilian, F. Leighton, and T. Shamoon. Secure spread spectrum watermarking for multimedia. IEEE Trans. on Image Processing, 6(12):1673–1687, Dec 1997.

[8] RFC #1035 "DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION", November 1987, https://tools.ietf.org/html/rfc1035

[9] http://www1.fips.ru/registers-doc-view/fips_servlet?DB=RUPAT&DocNumber=2646341&TypeFile=html

[10] https://docs.microsoft.com/en-us/dotnet/api/system.web.security.activedirectorymembershipprovider.createuser?redirectedfrom=MSDN&view=netframework-4.8#System_Web_Security_ActiveDirectoryMembershipProvider_CreateUser_System_String_System_String_System_String_System_String_System_String_System_Boolean_System_Object_System_Web_Security_MembershipCreateStatus_

[11] R. Van Schyndel, A. Tirkel, and C. Osborne. A digital watermark. In IEEE Int. Conf. on Image Processing (ICIP), volume 2, pages 86–90 vol.2, Nov 1994.

[12] Y. Liu, J. Mant, E. Wong, and S. H. Low. Marking and detection of text documents using transformdomain techniques. Proceedings of SPIE - Volume 3657, Electronic Imaging Conference on Security and Watermarking of Multimedia Contents, pages 317-328, 1999.

[13] N. Nikolaidis and I. Pitas. Robust image watermarking in the spatial domain. Signal Processing, 66(3):385 – 403, 1998.

[14] A. M. Alattar and O. M. Alattar. Watermarking electronic text documents containing justified paragraphs and irregular line spacing. Proceedings of SPIE - Volume 5306, Security, Steganography, and Watermarking of Multimedia Contents VI, pages 685-695, Jan 2004.

[15] *Mahesh Ramasubramanian, Sumanta Pattanaik, Donald Greenberg* "A Perceptually Based Physical Error Metric for Realistic Image Sythesis", SIGGRAPH-99 Proceedings

[16] A. Viterbi. Error bounds for convolutional codes and an asymptotically optimum decoding algorithm. IEEE Trans. on Information Theory, 13(2):260–269, 1967

[17] Lin, Shu & D. Costello, Error Control Coding, Prentice-Hall, 1983

[18] C.-S. Shieh, H.-C. Huang, F.-H. Wang, and J.-S. Pan. Genetic watermarking based on transform-domain techniques. Pattern Recognition, 37(3):555 – 565, 2004.

[19] T. K. Tsui, X.-P. Zhang, and D. Androutsos. Color image watermarking using multidimensional fourier transforms. IEEE Trans. on Information Forensics and Security, 3(1):16–28, March 2008.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Способ автоматизированного внесения цифровых водяных знаков (ЦВЗ) в цифровое изображение, предназначенное для вывода на экран, выполняемый по меньшей мере одним вычислительным устройством, содержащий этапы, на которых

получают кортеж данных, подлежащих внесению в виде ЦВЗ в цифровое изображение, предназначенное для вывода на экран устройства пользователя;

определяют форму в виде попиксельного представления и максимально допустимую размерность символа ЦВЗ исходя из используемого пользователем разрешения экрана устройства;

на основе информации о форме и размерности символа ЦВЗ определяют форму и размерность внутренней матрицы пикселей базовой яркости символа ЦВЗ, яркость которых будет отличаться от яркости периметровых пикселей того же символа;

на основе данных, содержащихся в кортеже, представлении о форме и максимально допустимой

размерности символа ЦВЗ и форме и размерности внутренней матрицы пикселей базовой яркости символа ЦВЗ осуществляют формирование последовательности символов ЦВЗ;

исходя из используемого пользователем разрешения экрана устройства, формируют шаблон-матрицу, определяющую построчное расположение последовательности сформированных символов ЦВЗ для вывода на экран;

накладывают сформированную шаблон-матрицу на цифровое изображение, предназначенное для вывода на экран;

выводят цифровое изображение с наложенной упомянутой выше шаблон-матрицей, содержащей последовательность сформированных символов ЦВЗ на экран устройства пользователя.

2. Способ по п.1, характеризующийся тем, что дополнительно содержит этап, на котором осуществляют помехоустойчивое кодирование полученного кортежа данных.

3. Способ по п.1, характеризующийся тем, что дополнительно содержит этапы, на которых

для кортежа данных вычисляют контрольную сумму для проверки целостности данных;

добавляют полученную контрольную сумму к кортежу данных.

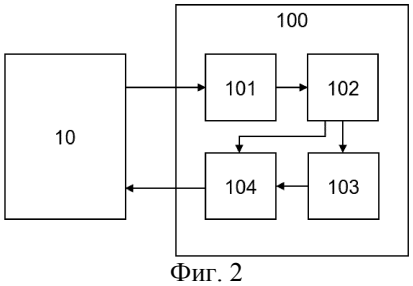
4. Способ по п.1, характеризующийся тем, что дополнительно содержит этап, на котором определяют текущие параметры экрана, причем максимально допустимая размерность символа ЦВЗ определяется с учетом текущих параметров экрана и размера кортежа данных.

5. Способ по п.1, характеризующийся тем, что дополнительно содержит этап, на котором собирают данные об устройстве пользователя, включающие: дату, установленную на устройстве пользователя; время, установленное на устройстве пользователя; идентификатор устройства пользователя; имя пользователя (LOGIN), осуществившего авторизацию на устройстве (10) пользователя;

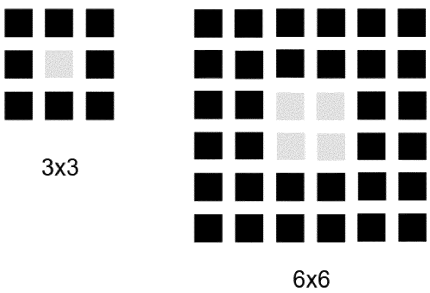
причем кортеж данных формируется из данных об устройстве пользователя.

6. Устройство автоматизированного внесения ЦВЗ в цифровое изображение, предназначенное для вывода на экран, содержащее по меньшей мере одно вычислительное устройство и по меньшей мере одно устройство памяти, содержащее машиночитаемые инструкции, которые при их исполнении по меньшей мере одним вычислительным устройством выполняют способ по любому из пп.1-5.

Фиг. 1

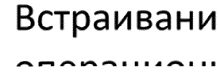


Фиг. 2



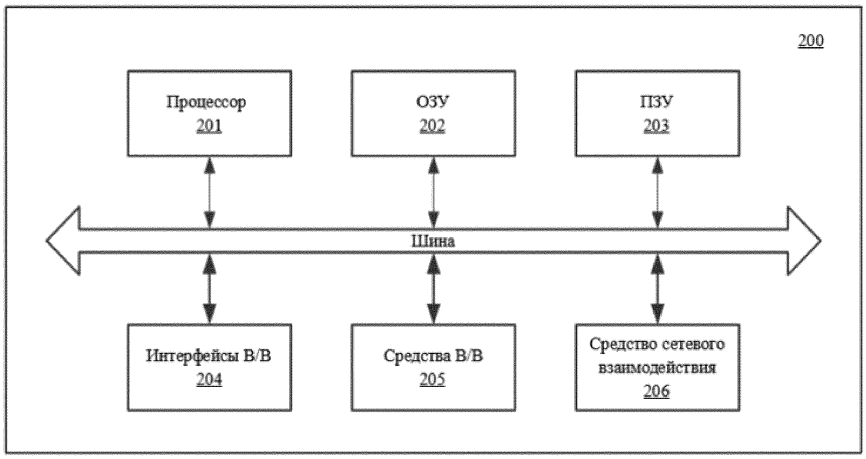
Фиг. 3

А. фрагмент копии изображения с наложенными символами цифровых меток измененной яркости



Б. фрагмент копии исходного изображения без наложения символов цифровых меток

Фиг. 4



Фиг. 5