ЗАЩИТА ИНФОРМАЦИОННОГО СОДЕРЖАНИЯ ИЗОБРАЖЕНИЙ В УСЛОВИЯХ НАЛИЧИЯ ДЕСТРУКТИВНОГО ВОЗДЕЙСТВИЯ

Абасова А.М.[1], Бабенко Л.К.[2]

Цель статьи: *повышение эффективности защиты такого объекта интеллектуальной собственности, как цифровое изображение за счет внедрения в него модифицированного цифрового водяного знака авторской разработки.*

Методы: *использованы методы математической морфологии, которые позволяют реализовать нелинейное встраивание бит данных в значимые области цифрового изображения. Использованы методы модулярной арифметики (метод ортогональных базисов и другие), которые позволяют повысить целостность цифрового водяного знака при наличии деструктивных воздействий.*

Результаты: *В работе представлен алгоритм преобразования, внедрения, извлечения и коррекции цифрового водяного знака для обеспечения противодействия угрозам хищения изображения. Описаны особенности реализации алгоритма на практике. В основе алгоритма лежит определение ключевых и значимых для восприятия изображения областей, в которые будет производиться внедрение информации об авторе изображения, встраиваемые данные будут модифицированы в избыточный модулярный код, позволяющий повысить их целостность в случае возникновения деструктивных воздействий. Проведены вычислительные эксперименты с использованием разработанной программы реализации алгоритма, получены сравнительные характеристики по отношению к существующим программным продуктам в данном сегменте интересов (для обеспечения защиты авторских прав).*

Ключевые слова: *стеганография, цифровой водяной знак, авторское право, интеллектуальная собственность, морфологическая обработка изображений, модулярная арифметика, избыточный модулярный код, структурный элемент.*

DOI: *10.21681/2311-3456-2019-2-50-57*

Введение

В связи с активным развитием и повсеместным внедрением информационных технологий в различные области деятельности граждан наблюдается рост нарушений, характерных для каждой из информационных систем. Так, например, по причине большого количества средств массовой информации, представленной в сети Интернет, растет спрос на контент для их наполнения (в данном случае рассматриваются такие объекты как изображения), однако в следствии возможности легкого копирования и незаконного использования данных объектов мы наблюдаем нарушение авторских прав, что влечет за собой материальные потери для автора или правообладателя [1].

На данный момент для защиты авторских прав на изображения отдается предпочтение внедрению цифровых водяных знаков (ЦВЗ) в данные объекты по причине невысокой стоимости, в отличии от других известных технических и организационных методов, а также возможности использования при регистрации цифровых изображений, что недоступно для многих организационных методов [2].

Проведенный анализ деструктивных воздействий на системы ЦВЗ показал, что при нарушении авторских прав злоумышленниками с большей вероятностью использовались атаки, так или иначе направленные на удаление или изменение ЦВЗ (например, в следствии сжатия изображения или изменения его яркости или контрастности) или блокирующие корректную работу стегодетектора, влияющую на возможность корректного приема, а именно обнаружения факта наличия ЦВЗ (например, усечение изображения или перестановка его пикселей).

Для эффективной защиты цифрового изображения от угроз хищения объектов интеллектуальной собственности необходимо обеспечить высокую устойчивость ЦВЗ к атакам, характерным при нарушении авторских прав, в совокупности с выполнением слепого извлечения самого ЦВЗ, когда у декодера нет информации об исходном изображении-контейнере, и его незаметности, то есть отсутствия визуального отличия заполненного изображения от исходного.

С учетом общих требований к ЦВЗ и системам ЦВЗ, таких как, например, сохранение ЦВЗ при максимальных искажениях контейнера, сохранение приемлемой вычислительной сложности [3] и результатам упомянутого ранее анализа о типичных атаках при нарушении авторских прав был сделан вывод о целесообразности поиска актуальной области для внедрения ЦВЗ, которая наименее вероятно будет изменена.

1 Абасова Анастасия Михайловна, аспирант, Южный Федеральный Университет «ЮФУ», Институт компьютерных технологий и информационной безопасности, г. Таганрог, Россия. E mail: moonriel@yandex.ru

2 Бабенко Людмила Климентьевна, доктор технических наук, профессор, Южный Федеральный Университет «ЮФУ», Институт компьютерных технологий и информационной безопасности, г. Таганрог, Россия. E mail: lkbabenko@sfedu.ru

Существующие исследования по данному направлению, как правило, направлены на встраивание ЦВЗ в частотные области изображения. Так, например, в работе [4] предлагается разделять изображение на блоки размером 64 на 64 пикселя и осуществлять встраивание ЦВЗ по частям в определенные области этих блоков, в работе [7] предлагается встраивать ЦВЗ в центральную область изображения. Достоинством методов, осуществляющих встраивание ЦВЗ в частотную область изображения, является устойчивость к модификации изображения в пространственной области, однако необходимо отметить, что ЦВЗ легко удалить с помощью фильтрации при известной полосе частот, в которой содержится ЦВЗ. Также общим недостатком приведенных выше и подобных им методов можно назвать необходимость декомпозирования изображения для последующего встраивания ЦВЗ в определенные спектральные области изображения-контейнера [5, 6], что существенно увеличивает их вычислительную сложность. Для спектрального преобразования изображения контейнера используют такие операции как дискретное косинусное преобразование, дискретное вейвлет-преобразование, дискретное преобразование Фурье и преобразование Карунена-Лоева. Дополнительно отметим, что если рассматривать профессиональную художественную сьемку, то авторы в своих работах применяют правила золотого сечения (золотой пропорции/гармонического деления) [8], при которых ключевой объект не располагается в центре изображения, что не учитывается в работе [7].

1. Предлагаемое направление для защиты авторских прав на изображение. По результатам анализа специфики методов обхода наличия ЦВЗ злоумышленником для использования изображения в противоправных целях было выявлено, что ключевые объекты, располагаемые на переднем плане изображения остаются нетронутыми, так как они представляют ценность изображения, особенно это выражено при использовании корреспондентских фотографий или рекламных работ. Можно сделать вывод о целесообразности применения для внедрения ЦВЗ блоков переднего плана. Объектами переднего плана принято считать множество ключевых объектов, распределенных по изображению (каждый – в конкретной выделенной части изображения), причем к переднему плану относят объекты, которые находятся на наименьшем расстоянии от камеры по сравнению с объектами локального фона, их окружающих [9].

При определении объектов, расположенных на переднем плане изображения, используют методы сегментации [10], однако их общим недостатком является достаточно высокая ресурсоемкость при выполнении операций алгоритмов; в некоторых случаях требуется вносить дополнительную уточняющую информацию, необходимую для работы алгоритмов (например, ручное указание примерных границ искомых объектов) и, что является существенным недостатком при решении поставленной цели, обнаружение четких контуров объектов (однако следует отметить, что в результате работы разных алгоритмов выходные данные могут несколько отличаться). Предлагается для определения блоков переднего плана выполнять сравнительно простую операцию маркирования, а именно выявления и выделения связанных между собой компонентов на изображении с помощью методов математической морфологии. Для реализации маркирования будем применять морфологическую эрозию и дилатацию (последовательно) или иными словами размыкание изображения [11] – выполнение данных процедур дополнительно позволяет исключить мелкие, малозначимые детали изображения; в некоторых случаях (при наличии множества темных объектов на изображении) будет использоваться замыкание (первым этапом выполняется дилатация, а вторым эрозия).

Операции размыкания и замыкания применяются к полутоновому изображению, поэтому исходное цветное изображение-контейнер I(x,y) необходимо преобразовать в I’ (x,y) – полутоновое. Для вычисления указываются данные структурного элемента S= b(x,y) (размера g×h, причем будем считать, что $g=2a_{1+1}$ и $h=2a_{2+1}$, где a_1, a_2 – неотрицательные целые числа). Структурный элемент представляет собой бинарное изображение в разы меньше чем I’ (x,y). I’ и b соотносят значение яркости каждой группе координат. Полутоновая эрозия I^’ по примитиву b, отмечается $I' \ominus b$, определяется как:

$$(I' \ominus b)(s,t)=\min\{I'(s+x,t+y)-b(x,y) \mid (s+x,t+y)\in D_{I'};(x,y)\in D_b\}, \quad (1)$$

где $D_{I'}$, D_b – области определения I’, b соответственно, s – сдвиг по координате x равный a_1, t - сдвиг по координате y равный a_2.

Полутоновая дилатация I^’ по структурному элементу b отмечается как $I' \oplus b$ и определяется как:

$$(I' \oplus b)(s,t)=\max\{I'(s-x,t-y)+b(x,y) \mid (s-x,t-y)\in D_{I'};(x,y)\in D_b\}. \quad (2)$$

На практике операция размыкания дополнительно позволит удалить из рассмотрения небольшие несущественные детали на изображении, при этом в итоге сохранив общую яркость и крупные объекты. Стоит отметить преимущество морфологических методов по сравнению со стандартными линейными фильтрами: морфологические методы обработки не искажают основные геометрические формы изображения в отличие от фильтров. Недостатком морфологических методов можно указать отсутствие маркирования некоторых скрытых объектов на изображении, то есть в результате выполнения операций, упомянутых выше, отдельные изолированные пиксели не будут обработаны, однако данный недостаток не повлияет на решение поставленной цели вследствие того, что данные неявные объекты будут изъяты из рассмотрения как не ключевые.

Как отмечалось выше, при выполнении морфологических операций используется некий структурный элемент, который представляет собой бинарное изображение небольшого размера, где совокупность нулей определяет его форму. При решении простых задач с использование математической морфологии данный структурный элемент представляется простой формой, такой как круг, квадрат, ромб. В разработанном алгоритме структурный элемент выполняет роль

0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0
0	0	1	1	1	1	1	0	0	1	0	0	1	0	0	0	0
0	1	1	1	1	1	1	1	1	1	0	1	1	1	0	1	0
0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0
0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0
0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	0
0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	0
0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	0
0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	0
0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	0	0
0	0	0	0	0	1	1	1	1	1	1	0	1	1	0	0	0
0	0	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0
0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Рис 1. Пример структурного элемента сложной формы.

ключа и представляет собой элемент сложной формы [12]. Пример одного из структурных элементов, используемых в алгоритме, представлен на Рис.1.

Кроме того предлагается использовать дополнительную ключевую информацию в виде критериев выбора объектов переднего плана для внедрения [13] в связи с тем, что на практике количество подходящих для внедрения информации блоков переднего плана будет превышать необходимое количество. Такими критериями могут быть: размер блоков переднего плана, расстояние от границ всех найденных блоков до границы изображения, расстояние между найденными блоками.

Рассмотрим каждый из критериев с учетом того, что условие по достаточному размеру каждого из блоков переднего плана для внедрения уже выполнено. В случае использования дополнительного критерия – выбор блоков переднего плана, наиболее удаленных друг от друга, наблюдаем существенное превышение вычислительной и временной сложности алгоритма, по причине определения взаимного расстояния между каждым из найденных блоков. Неявным недостатком данного критерия является тот факт, что на некоторых изображениях имеются группы взаимосвязанных между собой блоков (по сценарию), таким образом, при удалении блока, отдаленного от остальных, может возникнуть проблема с восстановлением той части ЦВЗ, которая была в нем заключена.

Другим критерием является выбор наиболее удаленных от края изображения блоков. В данном случае условие будет отлично работать с небольшой группой типов изображений таких, как рекламные постеры, в которых в центральную часть вынесен объект интересов. Также необходимо будет учитывать информацию о расположении изображения (горизонтальное/вертикальное) и расстояние до всех границ.

С точки зрения сохранения относительной простоты алгоритма оптимальным является критерий выбора самых больших по размеру блоков для внедрения, по факту будет анализироваться информация, уже ранее вычисленная на предыдущих этапах работы алгоритма.

Перспективным и масштабным направлением будущих исследований является формирование критерия, который включает комплекс из указанных выше критериев, возможно с применением нейронных сетей.

Следующим этапом работы алгоритма является выбор способа заполнения каждого блока ЦВЗ. В связи с известной распространенной проблемой заполнения бит изображения последовательно/на основе линейных функций, влияющей на быстроту и легкость стегоанализа злоумышленником, предложено использовать конкретную точку отсчета при встраивании ЦВЗ, которая будет зависеть от конкретного блока переднего плана. Данной точкой будет являться геометрический центр блока переднего плана или, иными словами, его центроид – центр масс фигуры аналогичной формы и размера как у рассматриваемого блока переднего плана [14]. Центроид вычисляется с использованием формул [15]:

$$\bar{x} \iint b(x,y)dx\,dy = \iint xb(x,y)dx\,dy \quad (3)$$

относительно оси x, а относительно оси y:

$$\bar{y} \iint b(x,y)\,dx\,dy = \iint yb(x,y)\,dx\,dy \quad (4)$$

где ($\bar{x}$, $\bar{y}$) – координаты геометрического центра, b(x,y) – плотность яркости изображения. Интеграл в левой части указанных выше соотношений является площадью блока переднего плана.

Координаты пикселей для встраивания ЦВЗ также будут зависеть от самого метода встраивания, так как существуют методы, в которых недопустимо использование пикселей, близко расположенных друг к другу, например в методе Куттера-Джордана-Боссена [16].

Как указывалось ранее, для внедрения будет использоваться модифицированный ЦВЗ. Сам ЦВЗ в ис-

ходном виде может представлять собой совокупность чисел [17], символов и/или текста [18], который содержит знак охраны авторских прав, либо являться бинарным изображением с логотипом (наиболее актуально в случае когда автор – юридическое лицо) [19], в некоторых случаях ЦВЗ является QR – кодом со ссылкой на сайт автора или с информацией об авторе. Несмотря на широкий выбор видов ЦВЗ он может быть представлен в виде корректирующего кода. Для модификации был выбран избыточный модулярный код как перспективный, но не изученный на данный момент при представлении ЦВЗ в области направления защиты авторских прав и позволяющий разделить полученный ЦВЗ на независящие друг от друга части одного размера. Использование избыточного модулярного кода дает возможность обнаружения и коррекции ошибки в случае возникновения деструктивного воздействия на ЦВЗ или систему ЦВЗ.

Предположим, заданы модули – это положительные числа, а также взаимно простые основания системы: $p_1,p_2,...,p_i,...,p_k$, НОД$(p_1,p_k)=1$ для $i\neq k$.

Информационный диапазон заданной числовой системы определяет значение $P=\prod_{i=1}^{k} p_i$. ЦВЗ для данных, представленных в виде текста, – это набор чисел, соответствующий каждой цифре/букве/символу в выбранной кодировке. Для бинарного изображения или QR-кода – это будет матрица чисел, которая образуется после преобразования матрицы, состоящей из нулей и единиц в форму, пригодную для обработки.

Любой произвольный ЦВЗ может быть представлен матрицей положительных целых чисел, каждый столбец в которой будет содержать остатки по определенному модулю всех позиционных значений ЦВЗ, в то время как строками являются представления позиционных значений в модулярном коде. Каждое неотрицательное целое число A можно задать в виде модулярного кода $A=\{\alpha_1,\alpha_2,...,\alpha_i,...,\alpha_k\}$, который будет содержать натуральные числа, удовлетворяющие критерию $0\leq\alpha_i<p_i$, где $i=1,2,...,k$.

Предположим, что основаниями заданной системы будут являться попарно взаимно простые модули $\{p_1,p_2,...,p_i,...,p_k\}$, а число $A\in Z(P)$, в таком случае, его модулярное представление $\{\alpha_1,\alpha_2,...,\alpha_i,...,\alpha_k\}$ возможно задать выражением $\alpha_i=|A|_{p_i}$, где $i=1,2,...,k$. Отличительной особенностью кода, который обладает свойствами обнаружения и исправления ошибок, в данном случае, является присутствие двух групп цифр – информационного диапазона $J_A=\{\alpha_1,\alpha_2,...,\alpha_i\}$ и контрольного диапазона $K_A=\{\alpha_{k+1},...,\alpha_{k+n}\}$. В информационном диапазоне присутствуют цифры, которые несут в себе числовое значение закодированной величины, в то время, как в контрольном диапазоне – цифры, которые позволяют обеспечивать возможность обнаружения и коррекции ошибок. При этом контрольная группа цифр будет являться избыточной.

Согласно правилам и положениям модулярной арифметики, числа должны содержаться в диапазоне [0,P'). Признаком присутствия искажения будет является выполнение неравенства $A\geq P$ [20]. При этом, ошибкой будем считать искажение значения, которое соответствует любому из модулей в модулярном представлении числа.

В разработанном алгоритме матрица с элементами ЦВЗ, представленными ИМК, разделяется на n матриц одинакового размера для того, чтобы остатки по каждому основанию системы записывались в свой отдельный блок переднего плана изображения (соответствующий определенному основанию системы). При такой организации внесения информации данные по каждому из оснований будут относительно изолированы друг от друга, и даже в случае удаления части изображения, которая включает полностью один или более блоков переднего плана, ЦВЗ возможно будет восстановить.

Зависимость между способностью восстановить ЦВЗ и количеством удаленных маркированных объектов переднего плана вычисляется на основании количества избыточных (контрольных) оснований (модулей):

$$\frac{M^T-M}{M}*100\%, \quad (5)$$

где M^T- полный диапазон системы, M – рабочий диапазон системы.

Для извлечения ЦВЗ выполняются преобразования, аналогичные преобразованиям, выполняемым для встраивания ЦВЗ. С использованием стего – ключа (структурного элемента и дополнительного критерия) производится вычисление маркированных объектов переднего плана. После выполнения данной операции производится вычисление геометрических центров (центроидов) маркированных объектов переднего плана и, в соответствии с принятой схемой встраивания (в зависимости от метода встраивания), определяются пиксели, в которые было встроено ЦВЗ.

Процесс обнаружения и коррекции ошибок будет производиться на основе известных методов ИМК. На первом этапе осуществляется проверка данных на наличие ошибок. Для этого предлагается перевести ИМК в полиадический код.

Значения разрядов полиадического кода $\{z_1,z_2,...,z_{n+k}\}$ по основаниям-модулям $p_1.p_2,...,p_i,...,p_{k+1},...,p_{k+n}$ возможно получить из ИМК $\{\alpha_1,\alpha_2,...,\alpha_i,...,\alpha_{k+n}\}$ с помощью системы:

$$\begin{cases} z_1=\alpha_1, \\ z_2=\left|p_1^{-1}\right|_{p_2}(\alpha_2-z_1)\Big|_{p_2}, \\ z_3=\left|\left|p_2^{-1}\right|_{p_3}(\left|p_1^{-1}\right|_{p_3}(\alpha_3-z_1)-z_2)\right|_{p_3} \\ \dots \\ z_n=\left|\left|p_{n-1}^{-1}\right|_{p_n}\left(\left|p_{n-2}^{-1}\right|_{p_n}\left(\dots\left|p_2^{-1}\right|_{p_n}(\left|p_1^{-1}\right|_{p_n}(\alpha_n-z_1)-z_2)\dots\right)-z_{n-1}\right|_{p_n}\right. \end{cases}. \quad (6)$$

Допустим, $A=\{z_1,z_2,...,z_{n+k}\}$ – полученный результат вычислений. В таком случае, число A находится в диапазоне разрешенных значений, тогда и только тогда, когда цифры по избыточным разрядам полиадического кода равны нулю, т.е. $z_{n+r}=0$ для $r=1,2,...,k$.. В случае, если число A – правильное, то его исходное значение в двоичной форме может быть восстановлено из полученных ранее коэффициентов обобщенной полиадической системы на основании данной формулы:

$$A=z_{n+k}p_{n+k-1}p_{n+k-2}...p_1+z_3\,p_2\,p_1+z_2\,p_1+z_1. \quad (7)$$

Если обнаружено искажение, то его исправление может быть осуществлено на основе метода проек-

ций, который имеет следующий алгоритм исправления ошибок:

На первом этапе осуществляется вычисление проекции числа $\tilde{A}$ по всем основаниям системы

$$\widetilde{A_1}, \widetilde{A_2}, \dots, \widetilde{A_i}, \dots, \widetilde{A_k}, \dots, \widetilde{A_{k+2}}. \quad (8)$$

На втором этапе происходит выявление искаженного (ошибочного) основания. Среди проекций есть хотя бы одна $\widetilde{A_i} < \frac{P}{p_{n+1}, p_{n+2}}$. В таком случае ошибочной является цифра $\tilde{\alpha}_i$.

На третьем этапе происходит исправление искаженного основания. После того как ошибочная цифра найдена, ее исправление производится по следующей формуле:

$$\alpha_i = \tilde{\alpha}_i + \left[\frac{p_i(1+np_{k+1})}{p_{k+1}m_i} - \frac{\bar{A}}{B_i}\right]. \quad (9)$$

На основе разработанного алгоритма были разработаны программы с помощью которых выполняется внедрение, извлечение ЦВЗ в/из изображения-контейнера и при необходимости его коррекция. Данные программы выполнены со схемами встраивания на основе методов LSB (программа № 1 – название ALStego) и метода Куттера-Джордана-Боссена (программа № 2 – название AStego). Обе программы реализованы на языке Matlab в связи с широкими возможностями по обработке и анализу изображений. В рамках оценки способности корректного извлечения ЦВЗ при различных деструктивных воздействиях были проведены эксперименты над различными изображениями в количестве ста штук. Изображения были выбраны разнообразного характера и назначения (рекламные постеры, корреспондентские фотографии, натюрморты, художественные фотографии; монотонные, многоцветные, текстурные и другие) по причине необходимости оценки не только вероятности правильного извлечения ЦВЗ но и подтверждения способности обнаружения необходимого количества блоков переднего плана для внедрения ЦВЗ.

Для корректной оценки эффективности ΔQ необходимо было вычислить показатели эффективности существующих программ по защите авторских прав и сравнить

Таблица 1

Результаты экспериментальных исследований

Программа / Деструктивное воздействие		Suresign		Drop WaterMark		ALStego		Изменение контрастности	
		Частн.	Групп.	Ч.	Гр.	Ч.	Гр.	Ч.	Гр.
Изменение контрастности	+10%	1	1	1	1	0	0	1	1
	+50%	1		1		0		1	
	-10%	1		1		0		1	
	-50%	1		1		0		1	
Изменение яркости	+10%	1	1	1	1	0	0	1	0,99
	+50%	1		1		0		0,97	
	-10%	1		1		0		1	
	-20%	1		1		0		1	
Смена формата изображения на JPEG	качество 8	1	1	1	1	0	0	1	1
	качество 10	1		1		0		1	
	качество 12	1		1		0		1	
	качество 14	1		1		0		1	
Смена формата изображения	BMP	1	0,84	1	0,86	1	0,83	1	0,85
	TIFF	1		1		1		1	
	PNG	1		1		1		1	
	GIF	0,37		0,42		0,3		0,4	
Вычеркивание	5 строк шириной 5 пикс	0	0	0	0	0,62	0,84	1	1
	10 строк шириной 1 пикс	0		0		1		1	
	5 столбцов шириной 5 пикс	0		0		0,73		1	
	10 столбцов шириной 1 пикс	0		0		1		1	

Поворот изображения	на 1°	1	0,67	1	0,67	1	0,67	1	0,67
	на 50°	1		1		1		1	
	на 50,5°	0		0		0		0	
Сдвиг на 10%	по горизонтали	0	0	0	0	0,8	0,78	0,96	0,96
	по вертикали	0		0		0,76		0,96	
Перемещение части изображения	5%	0	0	0	0	0,8	0,76	0,98	0,97
	10%	0		0		0,72		0,95	
Замена изображения	10%	0	0	0	0	0,64	0,58	0,95	0,78
	50%	0		0		0,52		0,6	
Удаление	10 крайних пикселей	0	0	0	0	1	0,79	1	0,89
	50 крайних пикселей	0		0		1		1	
	10% изображения	0		0		0,64		0,95	
	50% изображения	0		0		0,52		0,6	

их значения со значениями разработанных программ. Были выбраны Suresign и DropWaterMark как самые распространенные и популярные решения в области защиты авторских прав на изображения. Для анализа были выбраны частные показатели (табл.1) и вычислены итоговые значения по ним:

$$Q = \frac{1}{n}\sum_{i=1}^{n} q_i, \quad (10)$$

где Q – эффективность метода, q_i – частная эффективность противодействия i-ому деструктивному воздействию.

$$Q_{Suresign} = 0{,}53 \quad (11)$$

$$Q_{DropWaterMark} = 0{,}53 \quad (12)$$

$$Q_{ALStego} = 0{,}49 \quad (13)$$

$$Q_{AStego} = 0{,}92 \quad (14)$$

$$Q_{\text{сущ}} = \max(Q_{Suresign}; Q_{DropWaterMark}) = 0{,}53 \quad (15)$$

$$Q_{\text{разраб}} = \max(Q_{ALStego}; Q_{AStego}) = 0{,}92 \quad (16)$$

$$\Delta Q = Q_{\text{разраб}} - Q_{\text{сущ}} = 0{,}39 \quad (17)$$

Исходя из указанных выше данных, эффективность разработанного алгоритма заключалась в росте корректного извлечения ЦВЗ на 39% относительно существующих программных продуктов.

Заключение

В ходе работы был разработан алгоритм преобразования, внедрения, извлечения и коррекции цифрового водяного знака, отличающийся от известных новой структурой ЦВЗ и использованием морфологического анализа изображения, позволяющий определить значимые ключевые области для внедрения на основе стего ключа – структурного элемента особой сложной формы и дополнительного критерия выбора блоков для внедрения. Для реализации представленного алгоритма было разработано программное обеспечения для предотвращения хищения объектов интеллектуальной собственности с целью доказательства авторских прав, которое может быть использовано в различных системах обработки и передачи изображений для большинства графических форматов. В результате анализа эффективности, проведенного с помощью разработанных и уже известных алгоритмов, был получен результат, указывающий на рост корректного извлечения ЦВЗ на 39%. Замена и удаление части изображения являются наиболее частыми деструктивными воздействиями при нарушении авторских прав на изображение и результаты при данных воздействиях достаточно высоки для обеих программ, что также доказывает высокую эффективность разработанного алгоритма.

В качестве рекомендаций для повышения вероятности корректного извлечения ЦВЗ предлагается:

для выбора объектов переднего плана для внедрения ЦВЗ использовать критерий, который включает комплекс из различных общих параметров, упомянутый в работе;

увеличить количество разрядов представления ЦВЗ в избыточном модулярном коде.

Стоит отметить, что данные рекомендации также будут влиять на вычислительную и временную сложность алгоритма.

Перспективным направлением дальнейшей разработки является проведение комплекса исследований, направленного на применение разработанного алгоритма применительно к другим методам встраивания информации.

Рецензент: *Марков Алексей Сергеевич, доктор технических наук, старший научный сотрудник, профессор МГТУ им. Н.Э. Баумана, г. Москва, Россия. E-mail: a.markov@npo-echelon.ru*

Литература

1. Невская М.А., Тарасова Е.Н., Сухарев Е.Е. Авторское право в издательском бизнесе и СМИ –М: Дашков и К, 2008. -300 с.
2. Абасова А.М., Бабенко Л.К. Разработка алгоритма внедрения цифрового водяного знака на базе морфологической обработки изображения и модулярной арифметики для противодействия угрозам хищения объектов интеллектуальной собственности // Международный журнал прикладных и фундаментальных исследований. – 2018. -№6–С.9-14.
3. Грибунин В.Г., Костюков В.Е., Мартынов А.П., Николаев Д.Б., Фомченко В.Н. Стеганографические системы. Атаки, пропускная способность каналов и оценка стойкости / ред. В.Г. Грибунин. – Саров: ФГУП «РФЯЦ-ВНИИЭФ», 2015. -217 с.
4. Белобокова Ю.А. Метод встраивания цифровых водяных знаков для доказательства подлинности фотоизображений // Известия Тульского государственного университета. Технические науки. – 2013 – № 3 . – С. 106-110.
5. N. Terzija, W. Geisselhardt, “Robust Digital Image Watermarking Based on Complex Wavelet Transform”, In WSEAS Transactions on Communication, Issue 10, Volume 4, pp 1086-1092.
6. Конахович, Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика – К.: МК-Пресс, 2006. -288с.
7. Cox I.J., Miller M., Bloom J., Fridrich J. Digital watermarking and steganography - San Francisco: Morgan Kaufmann Publishing, 2008. - 624 p.
8. Карпин А. Фотография для начинающих – Самиздат, 2012. — 239 с.
9. Gupta S., Girshick R., Arbel´aez P., Malik J. Learning rich features from RGB-D images for object detection and segmentation // European Conference on Computer Vision –Springer. –2014. – Pp. 345–360.
10. Кухаренко Б.Г. Алгоритмы выделения объектов переднего плана из фона и интерактивного редактирования изображений // Приложение к журналу информационные технологии №4. – М.:[б.и.] – 2012. – 32 с.
11. Гонсалес Р., Вудс Р. Цифровая обработка изображений – М.:Техносфера, 2005. – 1072 с.
12. Абасова А.М. Алгоритм повышения устойчивости к деструктивным воздействиям цифровых водяных знаков, встраиваемых в цветное изображение // Известия ЮФУ. Технические науки. Комплексная безопасность сложных систем. – 2014. -№8(157). –С.75-81.
13. Абасова А.М. Защита информационного содержания цифровых изображений путем применения дополнительных критериев выбора объектов для внедрения цифровых водяных знаков // Вестник современных исследований. – 2018. №10-1. –С.249-252.
14. Mills R.L. Novel method and system for pattern recognition and processing using data encoded as Fourier series in Fourier space // Engineering Applications of Artificial Intelligence, Vol. 19, Issue 2, March 2006. pp. 219-234.
15. Хорн Б. К. П. Зрение роботов: Пер. с англ. — М.: Мир, 1989. — 487 с.
16. Kutter M., Jordan F., Bossen F. Digital signature of color images using amplitude modulation // Journal of Electronics Imaging, – 1998. – Vol. 7. – P.326-332.
17. Chu, C.-J. H. Luminance channel modulated watermarking of digital images / C.-J. H. Chu, A. W. Wiltz // Proc. of the SPIE Wavelet Applications Conf. –1999. –P.437-445.
18. Chae, J. Robust Techniques for Data Hiding in Images and Video / J. Chae // PhD thesis, Department for Electrical and Computer Engineering. Univ.of California, Santa Barbara, CA, USA, –1999.
19. Hsu, C.-T. Hidden digital watermarks in images / C.-T. Hsu, J.-L. Wu // IEEE Transactions on Image Processing. –1999. –Vol. 8. № 1. –P. 58-68.
20. Акушский, И.Я. Машинная арифметика в остаточных классах / И. Я. Акушский, Д. И. Юдицкий. –М.: Советское радио, 1968. –440с.

PROTECTION OF INFORMATION CONTENT IMAGES IN THE CONDITIONS OF DESTRUCTIVE EXPOSURE

Abasova A.M.[3], Babenko L.K.[4]

Purpose: *improving the protection of such an object of intellectual property as a digital image due to the introduction of a modified digital watermark authoring.*

Research methods: used methods of mathematical morphology, which allow for the non-linear embedding of data bits into significant areas of the digital image. Also used the methods of modular arithmetic (the method of orthogonal bases and others), which can improve the integrity of the digital watermark in the presence of destructive influences.

Results. *This paper presents an algorithm for the transformation, implementation, extraction and correction of a digital watermark to ensure countering the threat of image theft. The features of the implementation of the algorithm in practice are described. The algorithm is based on the definition of key and meaningful image areas in which information about the image author will be implemented, the embedded data will be modified into the redundant*

3 Anastasiya M. Abasova, Postgraduate at the Southern Federal University «SFedU», Institute of Computer Technologies and Information Security, Taganrog, Russia. E-mail: moonriel@yandex.ru

4 Lyudmila K. Babenko, Dr.Sc., Professor for the Southern Federal University «SFedU», Institute of Computer Technologies and Information Security, Taganrog, Russia. E-mail: lkbabenko@sfedu.ru

modular code which allows to increase their integrity in case of destructive impacts. Computational experiments were carried out using the developed algorithm implementation program, comparative characteristics were obtained with respect to the existing software products in this segment of interests (to ensure copyright protection).

Keywords: *steganography, digital watermark, copyright, intellectual property, morphological image processing, modular arithmetic, redundant modular code, structural element.*

References

1. Nevskaya M.A., Tarasova E.N., Sukharev E.E. Avtorskoye pravo v izdatelskom biznese i SMI –M: Dashkov i K, 2008. -300 p.
2. Abasova A.M., Babenko L.K. Razrabotka algoritma vnedreniya tsifrovogo vodyanogo znaka na baze morfologicheskoy obrabotki izobrazheniya i modulyarnoy arifmetiki dlya protivodeystviya ugrozam khishcheniya obyektov intellektualnoy sobstvennosti // Mezhdunarodnyy zhurnal prikladnykh i fundamentalnykh issledovaniy. – 2018. -№6–P.9-14.
3. Gribunin V.G., Kostyukov V.E, Martynov A.P., Nikolayev D.B., Fomchenko V.N. Steganograficheskiye sistemy. Ataki, propusknaya sposobnost kanalov i otsenka stoykosti / red. V.G. Gribunin. – Sarov: FGUP «RFYATS-VNIIEF», 2015. -217 p.
4. Belobokova Yu.A. Metod vstraivaniya tsifrovykh vodyanykh znakov dlya dokazatelstva podlinnosti fotoizobrazheniy // Izvestiya Tulskogo gosudarstvennogo universiteta. Tekhnicheskiye nauki. – 2013 – № 3 . – S. 106-110
5. N. Terzija, W. Geisselhardt, “Robust Digital Image Watermarking Based on Complex Wavelet Transform”, In WSEAS Transactions on Communication, Issue 10, Volume 4, pp 1086-1092, October 2005, ISSN 1109-2742.
6. Konakhovich, G.F., Puzyrenko A.Y. Kompyuternaya steganografiya. Teoriya i praktika – K.: MK-Press, 2006. -288p.
7. Cox I.J., Miller M., Bloom J., Fridrich J. Digital watermarking and steganography - San Francisco: Morgan Kaufmann Publishing, 2008. - 624 p.
8. Karpin A. Fotografiya dlya nachinayushchikh – Samizdat, 2012. — 239 p.
9. Gupta S., Girshick R., Arbel´aez P., Malik J. Learning rich features from RGB-D images for object detection and segmentation // European Conference on Computer Vision –Springer. –2014. – P. 345–360.
10. Kukharenko B.G. Algoritmy vydeleniya ob»yektov perednego plana iz fona i interaktivnogo redaktirovaniya izobrazheniy // Prilozheniye k zhurnalu informatsionnyye tekhnologii №4. – M.:[b.i.] – 2012. – 32 p.
11. Gonsales R., Vuds R. Tsifrovaya obrabotka izobrazheniy – M.:Tekhnosfera, 2005. – 1072 p.
12. Abasova A.M. Algoritm povysheniya ustoychivosti k destruktivnym vozdeystviyam tsifrovykh vodyanykh znakov, vstraivayemykh v tsvetnoye izobrazheniye // Izvestiya YUFU. Tekhnicheskiye nauki. Kompleksnaya bezopasnost’ slozhnykh sistem. – 2014. -№8(157). –P.75-81.
13. Abasova A.M. Zashchita informatsionnogo soderzhaniya tsifrovykh izobrazheniy putem primeneniya dopolnitel’nykh kriteriyev vybora ob»yektov dlya vnedreniya tsifrovykh vodyanykh znakov// Vestnik sovremennykh issledovaniy. – 2018. №10-1. –P.249-252.
14. Mills R.L. Novel method and system for pattern recognition and processing using data encoded as Fourier series in Fourier space // Engineering Applications of Artificial Intelligence, Vol. 19, Issue 2, March 2006. P. 219-234.
15. Khorn B. K. P. Zreniye robotov: Per. s angl. — M.: Mir, 1989. — 487 p.
16. Kutter M., Jordan F., Bossen F. Digital signature of color images using amplitude modulation // Journal of Electronics Imaging, – 1998. – Vol. 7. – P.326-332.
17. Chu, C.-J. H. Luminance channel modulated watermarking of digital images / C.-J. H. Chu, A. W. Wiltz // Proc. of the SPIE Wavelet Applications Conf. –1999. –P.437-445.
18. Chae, J. Robust Techniques for Data Hiding in Images and Video / J. Chae // PhD thesis, Department for Electrical and Computer Engineering. Univ.of California, Santa Barbara, CA, USA, –1999.
19. Hsu, C.-T. Hidden digital watermarks in images / C.-T. Hsu, J.-L. Wu // IEEE Transactions on Image Processing. –1999. –Vol. 8. № 1. –P. 58-68.
20. Akushskiy. I.Ya. Mashinnaya arifmetika v ostatochnykh klassakh / I. Ya. Akushskiy. D. I. Yuditskiy. –M.: Sovetskoye radio. 1968. –440s.