DOI: 10.18372/2410-7840.19.12207
УДК 004.056.5:003.26:347.77

СТЕГАНОГРАФИЧЕСКИЙ МЕТОД ЗАЩИТЫ ОБЪЕКТОВ АВТОРСКОГО ПРАВА И ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

Андрей Сагун, Леонид Щербак, Владислав Хайдуров, Валентина Кунченко-Харченко, Станислав Костянец, Михаил Тетьора

Защита информации, которая относиться к объектам интеллектуальной собственности или авторского права, является достаточно специфической задачей, потому что часто сложно определить существует ли обязательной необходимость в защите такой информации, либо же, такая защита является опционной. Частично, такую задачу можно решать при помощи сценария «демонстрации авторского права», частично, при помощи скриптового сценария «предотвращение копирования». В большинстве случаев такой метод защиты известен как сокрытие информации. В результате была разработана модификация криптографического встраивания по типу алгоритма LSB с использованием ключей. Была улучшена стойкость метода по сравнению с классическими LSB–стеганоалгоритмами. Основной сутью предложенного стеганографического метода является встраивание полноцветных изображений в динамические полноцветные информационные объекты. Таким образом, если уровень интенсивности пикселя изображения изменяется от 0 до 255, то это означает, что данное изображение может быть представлено в 8-битных плоскостях. Соответственно, само встраивание базируется на методологии информационного сокрытия LSB. Статья оперирует методологией развития систем защиты и преобразования графики, текстовой информации в динамических графических объектах. Моделирование было произведено в прикладной среде моделирования MATLAB, в результате чего были получены результаты в виде временных зависимостей. На основе разработанной модификации LSB-метода можно улучшить защиту прав интеллектуальной собственности в анимированных и видеографических объектах путем внедрения различных полноцветных цифровых водяных знаков. Также, предложенный метод обладает свойствами универсальной применимости.

Ключевые слова: *система защиты информации, интеллектуальная собственность, авторское право, стеганографический метод, разложение на битовые плоскости, динамические графические объекты, среда моделирования MATLAB.*

Введение. В связи с тем, что в информационных системах используется информация, которая может быть отнесена к объектам интеллектуальной собственности или авторского права, то существует необходимость определения таких объектов, четкой их дифференциации и применения к ним законодательных норм защиты в соответствии с Законодательством Украины. Разработка системы защиты подобных объектов часто является нетривиальной задачей и может быть решена при помощи стеганографии [1]. Актуальность ее решения очевидна в связи с тем, что на предприятиях различной формы собственности создаются тысячи образцов ноу-хау, которые часто не имеют аналогов в своей сфере, как в Украине, так и в мире. Отчасти, задача может быть решена сценарием «Демонстрации законного права собственности», отчасти – использованием сценария «Сдерживание копирования» [2].

Целью разработки является создание такого стеганографического метода, который бы обеспечивал поддержку сценария «Демонстрация законного права собственности» для объектов авторского права и интеллектуальной собственности с одной стороны и имел бы потенциал решать подобную задачу для цифровых объектов разных компьютерных форматов, в том числе – полноцветных динамических.

Методы и алгоритмы решения рассматриваемой задачи сильно зависят от того, какого рода информация подлежит защите. Так, например, в Гражданском кодексе Украины существует норма статьи 505 [3]. Руководствуясь этой статьей можно четко определить, имеем ли мы дело с коммерческой тайной. В данном случае речь может идти о встраивании цифровых меток в различные информационные объекты с целью контроля их использования [2, 4, 5].

Системы встраивания информации можно рассматривать как системы, которые способны защищать объекты интеллектуальной собственности и авторского права от копирования без ведома автора. Такие системы позволяют скрывать сам факт передачи информации от одного объекта к другому в файлах, к примеру, того же авторского права и другое. Достаточно часто при построении системы защиты информации за основу берется тот факт, что сама система содержит две подсистемы: подсистема для записи информации, подсистема для извлечения информации [4-8].

В работе предлагается метод встраивания полноцветных изображений в динамические полноцветные графические объекты.

Встраивание информации разного происхождения в наименее значимые биты контейнера – это один из самых распространенных методов, к которому можно производить достаточно много модификаций [4, 8]. Такого рода подход может применяться как для стеганографии, так и для защиты сигналов при помощи цифровых водяных знаков [6-8]. Реализация простейшего метода встраивания информации достаточно проста и не требует выделения дополнительной памяти на обработку того или иного изображения [8]. Время работы такого алгоритма занимает $O(mn)$, где *m* и *n* указывают на количество пикселей вдоль оси абсцисс и оси ординат соответственно. Следует отметить, что применение данного подхода дает возможность скрыть достаточно большой объем информации без искажений, которые может определить человек визуально. Введем терминологию для дальнейших выкладок. Пустым контейнером будем называть изображение, в которое нужно вставить некоторый водяной знак. Заполненным контейнером будем называть с уже встроенным в него водяным знаком.

Несмотря на то, что методы, подобные данному имеют низкую устойчивость при повреждении заполненного контейнера, они имеют весьма универсальную применимость [4,6-13]. Тем не менее, НЗБ-внедрение можно использовать при кодировании последовательности битов, которые получаются в результате двоичного представление кодируемой строки в некоторое изображение.

Постановка задачи. В результате анализа производственно-технологических процессов на предприятии N, которое специализируется на производстве мебели и изделий из дерева, было установлено, что, в соответствии с ч. 2 статьей 433 ЦК [14] и статьей 11 Закона Украины «Про авторське право і суміжні права» [15] присутствуют следующие объекты авторского права и интеллектуальной собственности:

– дизайн-проекты мебели;

– 3D-визуализации отдельных элементов мягкой мебели;

– элементы фирменного стиля;

– дизайн-проекты интерьеров.

Перечисленные выше объекты по факту являются объектами авторского права [14, 15]. Авторское право на них возникает по факту их создания.

Целью работы есть реализация программного комплекса, который содержит главный функциональный модуль для встраивания полноцветного изображения в анимированные графические объекты с использованием алгоритмов встраивания информации на основании наименьшего значимого бита.

Решение задачи. Для простоты понимания самого процесса встраивания полноцветного водяного знака, мы будем рассматривать процесс встраивания информации в конкретную *p*-ю битовую плоскость. Если значение интенсивности пикселя некоторого изображения меняется от 0 до 255, это означает, что само изображение может быть представлено в виде восьми битовых плоскостей, т. к. $\log_2 256 = 8$. Заполненный встроенной информацией контейнер является носителем информации. Тогда его можно обозначить в виде:

$$C^W(n_1,n_2) = C_1^W(n_1,n_2) + \ldots C_K^W(n_1,n_2)\cdot 2^{K-1}, \quad (1)$$

для всех пикселей вида (n_1,n_2) входного контейнера, причем $C_s^W(n_1,n_2) \in \{0;1\}$, s – номер плоскости, *K=8, где* $C_s^W(n_1,n_2)$ – разложение s-ой битовой плоскости пикселя (n_1,n_2), $s = \overline{1,K}$, C – пустой контейнер, а C_s^W – заполненный контейнер (контейнер с вшитой информацией).

На сегодняшний день существует достаточно большое количество систем на основе изменения наименьшего значимого бита (НЗБ), которые отличаются способом обработки конкретной битовой плоскости [8].

Пусть в НЗБ контейнера необходимо встроить изображение, которое есть цифровым водяным знаком того же размера, причем известно, что оно содержит бинарные значения (0 – черный цвет, а 1 – белый). Тогда могут использоваться следующие варианты модификации.

Подмена битовой плоскости контейнера битами скрываемой информации. В данном случае это имеет следующий вид:

$$C^W(n_1,n_2) \to W(n_1,n_2), \quad (2)$$

где $W(n_1,n_2)$ – значение (ноль или один) интенсивности цвета пикселя с координатами (n_1,n_2) некоторого водяного знака, который встраивается во входной контейнер. Извлечение информации производится в обратном порядке. Для того, чтобы получить встраиваемую информацию из заполненного контейнера, достаточно взять значение битов разложения из соответствующей битовой плоскости заполненного контейнера.

Еще один способ бинарной вставки контейнера есть побитовое сложение некоторой битовой плоскости разложения входного контейнера с битами той информации, которую нужно скрыть информации. Этот процесс может придать вид:

$$C_p^W(n_1,n_2)=C_p(n_1,n_2)\oplus W(n_1,n_2). \quad (3)$$

Очевидно, что извлечение скрытой информации будет произведено путём побитового сложения $C_p^W(n_1,n_2)$ и $C_p(n_1,n_2)$, что можно представить в виде следующего выражения:

$$W(n_1,n_2)=C_p(n_1,n_2)\oplus C_p^W(n_1,n_2). \quad (4)$$

Следует отметить, что при простой подмене некоторой плоскости пустого контейнера соответствующими битами водяного знака, мы получили систему выражений, которая не требует изначальной информации о пустом контейнере. В методе (3)-(4) мы получаем извлеченную информацию на основании двух контейнеров, а именно: пустого и заполненного.

Обоснование метода. Используя основные теоретические положения о встраивание битовой информации [8], можно получить несколько разных методов и их модификаций для битового встраивание текстовой информации в: а) изображение; б) видео и аудиоданные [8]. В рассматриваемом случае при побитовом встраивании информации в пустой контейнер, передаётся бинарный вектор некоторой фиксированной длины L. Очевиден тот факт, что длина данного вектора значительно меньше количества пикселей входного изображения. Здесь, все так же, встраивание битов происходит путём замены битов входного контейнера.

Для противодействия простейшим методам стеганографического анализа используют следующие подходы [8,12,13]:

1) выполняют процесс заполнений небольшой часть части контейнера. Это означает, что величина заполненности контейнера есть существенно меньше единицы;

2) входной контейнер заполняют битами по некоторому криптографическому закону или на основании случайных чисел. Можно предположить, что для полного извлечения встроенной в контейнер информации нужно иметь ключ (адреса и последовательность извлечения встроенных битов).

Проведем анализ следующего факта. При встраивании информации в некоторую конкретную p-ю битовую плоскость яркость конкретного взятого пикселя либо не меняется, либо меняется ровно на число, которое есть степенью числа 2, причём заведомо известно, что в большую сторону. Для определённости решим задачу встраивания в пиксель с яркостью 21 значение 1. Представление числа 21 в двоичной записи имеет вид 00010101. Исходя с представления двоичной записи видно, что во втором с конца битом стоит число 0. Таким образом при встраивании битовой единицы, прибавляется единица к значению яркости данного пикселя. В итоге получаем 23.

На основании необходимых теоретических методов по встраиванию битовой информации в обычные изображения, можно перейти к встраиванию полноцветных водяных знаков в динамические графические объекты. Так для рассматриваемого случая – это gif-файл.

Предположим, что имеется некоторый контейнер, который являет собой полноцветный графический динамический файл. Обозначим его в виде трех компонент $\left\{C_R^S;C_G^S;C_B^S\right\}$, где s – это количество полноцветных кадров, которое имеет входной контейнер. После разложения на битовые плоскости каждой компоненты этого пустого контейнера будем иметь общее бинарное представление пустого входного контейнера

$$\left\{C_{Rp}^S(n_1,n_2);C_{Gp}^S(n_1,n_2);C_{Bp}^S(n_1,n_2)\right\}. \quad (5)$$

Пусть водяной знак, который нужно вставить во входной контейнер имеет вид $\left\{W_R;W_G;W_B\right\}$. Тогда его представление по битовым плоскостям имеет следующий вид

$$\left\{W_{Rp}(n_1,n_2);W_{Gp}(n_1,n_2);W_{Bp}(n_1,n_2)\right\}. \quad (6)$$

Очевидно, что при решении данной задачи считается, что значение $s\ge 8\ge p, p=\overline{1;8}$.

Используя сформулированную стратегию и методику встраивание битов в конкретную битовую плоскость, на основании простейшего описанного выше метода подмены битовой плоскости получим следующую формулу для встраивания полноцветного водяного знака:

$$\begin{cases} C^W{}_R{}_p^S(n_1,n_2)=W_{Rp}(n_1,n_2) \\ C^W{}_G{}_p^S(n_1,n_2)=W_{Gp}(n_1,n_2) \\ C^W{}_B{}_p^S(n_1,n_2)=W_{Bp}(n_1,n_2) \end{cases}. \quad (7)$$

Извлечение информации из заполненного контейнера производится очевидным обратным способом.

Аналогичным образом, для получения системы встраивания полноцветного водяного знака

в анимированный графический объект с использованием системы (3)-(4). Процесс встраивания изображения водяного знака в пустой входной контейнер можно производить на основании следующей формулы:

$$\left\{\begin{array}{l} C^W{}_{Rp}^S\left(n_1,n_2\right)=C_{Rp}^S\left(n_1,n_2\right)\oplus W_{Rp}\left(n_1,n_2\right) \\ C^W{}_{Gp}^S\left(n_1,n_2\right)=C_{Gp}^S\left(n_1,n_2\right)\oplus W_{Gp}\left(n_1,n_2\right) \\ C^W{}_{Bp}^S\left(n_1,n_2\right)=C_{Bp}^S\left(n_1,n_2\right)\oplus W_{Bp}\left(n_1,n_2\right) \end{array}\right\}. \quad (8)$$

Процесс извлечение полноцветного водяного знака выполняется обратным образом по принципу, аналогичному к (4), то есть

$$\left\{\begin{array}{l} W_{Rp}\left(n_1,n_2\right)=C^W{}_{Rp}^S\left(n_1,n_2\right)\oplus C_{Rp}^S\left(n_1,n_2\right) \\ W_{Gp}\left(n_1,n_2\right)=C^W{}_{Gp}^S\left(n_1,n_2\right)\oplus C_{Gp}^S\left(n_1,n_2\right) \\ W_{Bp}\left(n_1,n_2\right)=C^W{}_{Bp}^S\left(n_1,n_2\right)\oplus C_{Bp}^S\left(n_1,n_2\right) \end{array}\right\}. \quad (9)$$

Иными словами, для того, чтобы вставить полноцветный водяной знак в некоторый пустой контейнер, который представлен в виде анимированного графического файла, нужно битовые плоскости каждой цветовой компоненты вставлять поочередно в битовые плоскости кадров анимированного изображения. К примеру, если входной анимированный файл имеет 16 кадров, это означает, что в него можно два раза записать полноцветный водяной знак. Если же входной анимированный графический объект имеет 80 кадров, тогда в него можно записать 10 водяных знаков.

После того, как основной принцип битовой вставки в динамические (анимированные) графические объекты получен, можно рассмотреть несколько существенных модификаций.

1. В анимированные графические объекты можно выполнять вставку нескольких водяных знаков, что повысит степень защиты самого файла.

2. Производить вставку водяных знаков меняя битовые плоскости по некоторому ключу. Данная модификация существенной усложнит извлечение водяного знака, который может представлять собой важную графическую информацию. Поэтому, очевидно, что для извлечения информации также нужен ключ.

3. Выполнение вставки битовых плоскостей разных водяных знаков по некоторому ключу. Эта модификация также усложнит поиск как одного полноцветного водяного знака, так и всех, которые были встроены в контейнер.

4. Перед непосредственной вставкой водяного знака, можно выполнить сжатие битов, к примеру, с использованием метода Хаффмана или RLE-сжатия данных [12]. Эта модификация имеет две положительные черты: меньше данных вставляем – меньше вероятность несанкционированного корректного извлечения нужной информации из заполненного контейнера; данные кодируются на основании дерева (если был использован метод Хаффмана). Можно предположить, что для извлечения информации понадобится ключ, по которому можно извлечь последовательность нужных битов (и алфавита, который присутствует в таких методах сжатия, как, к примеру, тот же метод Хаффмана).

В процессе выполнения данной работы был реализован программный комплекс в математическом прикладном пакете MatLab 2017a с графическим интерфейсом пользователя.

Как известно, MatLab – это один из немногих программных пакетов, который адаптирован для решения прикладных и научно-технических задач общего вычислительного назначения. Выбор MatLab обусловлен необходимостью упростить работу с цифровой обработкой изображений, в частности их числовом представлении.

В таблицах 1-2 представлены зависимости времени, которое необходимо затратить на обработку одного кадра контейнера, внедрения и извлечения соответствующей битовой плоскости водяного знака (трех его компонент) системой (7)…(9) от размерности кадра в пикселях. Таблица 3 содержит основные характеристики процессора, на котором производилось тестирование предложенных методов.

Таблица 1

Время обработки одного кадра контейнера. Вставка битовой плоскости водяного знака (RGB)

Размер изображения	Количество обрабатываемых точек	Время работы программы, в сек.
800 x 600	480000	0,08512
1021 x 768	784128	0,16150
1366 x 768	1049088	0,24841
1920 x 1080	2073600	0,71154

Таблица 2

Время обработки одного кадра контейнера. Извлечение битовой плоскости водяного знака (RGB)

Размер изображения	Количество обрабатываемых точек	Время работы программы, в сек.
800 x 600	480000	0,02471
1021 x 768	784128	0,11871
1366 x 768	1049088	0,19564
1920 x 1080	2073600	0,567232

Таблица 3

Основные характеристики процессора

Марка процессора	AMD Phenom X4
Количество ядер	4
Количество потоков	4
Тактовая частота работы	3,4 ГГц

Программная реализация с использованием GUIDE среды MatLab описанного выше метода защиты информации содержит ряд компонент, которые представлены на рисунке 1.

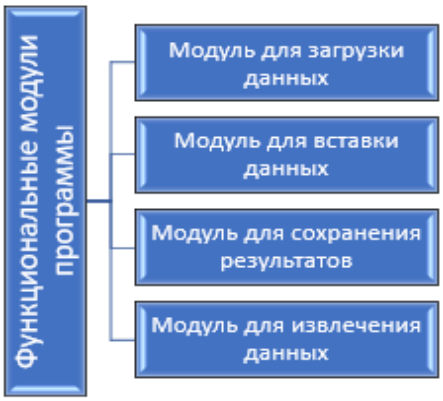

Рис. 1. Основные компоненты модели программной реализации метода защиты информации в среде MatLab

Тестирование программного комплекса проведено на разных входных данных. На основании разработанных модификаций метода НЗБ можно производить различные технологии по защите анимированных графических объектов интеллектуальной собственности и авторского права произвольными полноцветными водяными знаками.

Выводы. При выполнении работы по защите анимированных графических объектов, были получены основные результаты применения встраивания битовой информации в наименьше значимые биты. Также была смоделирована работа полученного алгоритма в среде MatLab 2017a, с помощью которого были получены цифровые данные графических объектов для дальнейшей работы с ними и разработан удобный интерфейс пользователя, с помощью которых можно выполнять защиту анимированных графических файлов с использование полноцветных водяных знаков.

В работе предложено ряд модификаций данного алгоритма встраивания информации в наименее значащие биты. К ним относятся криптографические алгоритмы встраивания информации с использованием ключей. Данные алгоритмы дают большую устойчивость классических алгоритмов, поскольку известно, что большинство современных криптосистем используют комплексный подход, а именно: применение стеганографии и криптографии как единое целое [1-3].

Также предложен вариант применения метода Хаффмана или RLE-сжатия данных для того, чтобы результат вставки битов был более устойчив к стеганоанализу заполненных контейнеров.

Полученные результаты можно использовать на практике не только для сокрытия данных в графических файлах. Такой же подход можно применять к защите и других видов информации, например, аудиоданных и видеоданных, которые также представляют собой объекты интеллектуальной собственности или авторского права.

ЛИТЕРАТУРА

[1]. M. Khosrow-Pour, "Encyclopedia of E-Commerce, E-Government and Mobile Commerce", *Resources Management Association. Idea Group Reference,* pp. 480-487, 2006.

[2]. M. Barni, F. Bartolini, *Watermarking Systems Engineering*, NewYork: Marcel Dekker, inc., 2004, 485 p.

[3]. Цивільний кодекс України. Стаття 505. Поняття комерційної таємниці: [Електронний ресурс]. Режим доступу: http:// radnuk. info / komentar / chky / chky-knuga4/140-kn4-glava46/2214--505-.html.

[4]. F. Shih, *Watermarking, Steganography, and Forensics*, New York: CRC Press, 2012, 424 p.

[5]. К. Защелкин, А. Ищенко, Е. Иванова, "Решение проблемы классификации блоков контейнера при JPEG-атаке на стеганографический метод Бенгана-Мемона-Эо-Юнг", *Радіоелектронні і комп'ютерні системи*, №6(70), С. 164-168, 2014.

[6]. J. Fridrich, *Steganography in Digital Media*, New York: Cambridge University. Press, 2010, 448 p.

[7]. I. Cox, M. Miller, J. Bloom, J. Fridrich, *Digital Watermarking and Steganography*, Burlington: Morgan Kaufmann Publishers, 2008, 592 p.

[8]. В. Федосеев, *Цифровые водяные знаки и стеганография*, Самара. Издательство СГАУ, 2015, 128 с.

[9]. F. Hartung, B. Girod, "Watermarking of Uncompressed and Compressed Video", *Signal Processing*, vol. 66, no. 3, pp. 283–301, 1998.

[10]. T. Kalker, A.J.E.M. Janssen, "Analysis of Watermark Detection using SPOMF", *Proceedings of ICIP*, vol. 1, pp. 316-319, 1999.

[11]. H.J. Wang, P.C. Su, C.C.J. Kuo, "Wavelet-based digital image watermarking", *Optics Express*, vol. 3, no. 12, pp. 491–496, 1998.

[12]. R. Wang, *Introduction to Orthogonal Transforms: with Applications in Data Processing and Analysis*, Cambridge University Press, 2011.

[13]. Н. Глумов, В. Митекин, "Алгоритм встраивания полухрупких цифровых водяных знаков для задач аутентификации изображений и скрытой передачи информации", *Компьютерная оптика*, Т. 35, С. 262–267, 2011.

[14]. Цивільний кодекс України. ч. 2 ст. 433. [Електронний ресурс]. Режим доступу: http://zakon5.rada.gov.ua/ laws/show/435-15/page8

[15]. Закон України "Про авторське право і суміжні права". Ст. 11. [Електронний ресурс]. Режим доступу: http://zakon2.rada.gov.ua/laws/show/3792-12/page.

REFERENCES

[1]. M. Khosrow-Pour, "Encyclopedia of E-Commerce, E-Government and Mobile Commerce", *Resources Management Association. Idea Group Reference,* pp. 480-487, 2006.

[2]. M. Barni, F. Bartolini, *Watermarking Systems Engineering*, NewYork: Marcel Dekker, inc., 2004, 485 p.

[3]. Civil Code of Ukraine. Art. 505. Tsyvil'nyy kodeks Ukrayiny. Stattya 505. Ponyattya komertsiynoyi tayemnytsi. [Electronic resource]. Available at: http://radnuk.info/komentar/chky/chky-knuga4/140-kn4-glava46/2214--505-.html

[4]. F. Shih, *Watermarking, Steganography, and Forensics*, New York: CRC Press, 2012, 424 p.

[5]. K. Zashhelkin, A. Ishhenko, E. Ivanova, "Classification problem solution of container units at jpeg–attack on steganographic method of Benham–Memon–Yeo–Yeung", *Radioelectronic and Computer Systems*, Kharkiv, no. 6(70). pp. 164-168, 2014.

[6]. J. Fridrich, *Steganography in Digital Media*, New York: Cambridge University. Press, 2010, 448 p.

[7]. I. Cox, M. Miller, J. Bloom, J. Fridrich, *Digital Watermarking and Steganography*, Burlington: Morgan Kaufmann Publishers, 2008, 592 p.

[8]. V. Fedoseev, *Digital Watermarks and Stegonography*, Iz. SGAU, Samara, 2015, 128 p.

[9]. F. Hartung, B. Girod, "Watermarking of Uncompressed and Compressed Video", *Signal Processing*, vol. 66, no. 3, pp. 283–301, 1998.

[10]. T. Kalker, A.J.E.M. Janssen, "Analysis of Watermark Detection using SPOMF", *Proceedings of ICIP*, vol. 1, pp. 316-319, 1999.

[11]. H.J. Wang, P.C. Su, C.C.J. Kuo, "Wavelet-based digital image watermarking", *Optics Express*, vol. 3, no. 12, pp. 491–496, 1998.

[12]. R. Wang, *Introduction to Orthogonal Transforms: with Applications in Data Processing and Analysis*, Cambridge University Press, 2011.

[13]. N. Glumov, V. Mitekin, "Popular digital watermarks embedding algorithm for images authentications' tasks and hided information transmission", *Computer optic*, vol. 35, pp. 262-267, 2011.

[14]. Civil code of Ukraine. Ch. 2, art. 433. [Electronic resource]. Available at: http://zakon5.rada.gov.ua/ laws/show/435-15/page8

[15]. The Law of Ukraine, art. 11. [Electronic resource]. Available at: http:// zakon2. rada. gov. ua / laws/ show/3792-12/page

СТЕГАНОГРАФІЧНИЙ МЕТОД ЗАХИСТУ ОБ'ЄКТІВ АВТОРСЬКОГО ПРАВА ТА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

Захист інформації, яка належить до об'єктів інтелектуальної власності або авторського права, є досить специфічною задачею, тому що часто складно визначити чи існує обов'язкова необхідність в захисті такої інформації, або ж, такий захист є опційним. Частково, таку задачу можна вирішувати за допомогою сценарію «демонстрації авторського права», частково, за допомогою скриптового сценарію «запобігання копіювання». У більшості випадків такий метод захисту відомий, як приховування інформації. В результаті була розроблена модифікація криптографічного вбудовування по типу алгоритму LSB з використанням ключів. В результаті чого, була поліпшена стійкість методу в порівнянні класичними LSB-стеганоалгоритмами. Основною суттю запропонованого стеганографічного методу є вбудовування повнокольорових зображень в динамічні повнокольорові інформаційні об'єкти. Тобто, якщо рівень інтенсивності пікселя зображення змінюється від 0 до 255, то це означає, що дане зображення може бути представлене в 8-бітних площинах. Відповідно, саме вбудовування базується на методології інформаційного приховування LSB. Стаття оперує методології розвитку систем захисту і перетворення графіки, текстової інформації в динамічних графічних об'єктах. Моделювання було проведено в прикладному середовищі моделювання MATLAB, в результаті чого були отримані результати у вигляді часових залежностей. На основі розроблених модифікацій LSB-методу можна покращити захист прав інтелектуальної власності в анімованих і відеографічних об'єктах шляхом вбудовування різноманітних повнокольорових цифрових водяних знаків. Також, запропонований метод має властивості універсальної застосовності.

Ключові слова: система захисту інформації, інтелектуальна власність, авторське право, стеганографіний метод, розкладання на бітові площини, динамічні графічні об'єкти, середовище моделювання MATLAB.

STEGANOGRAPHIC METHOD FOR PROTECTION THE OBJECTS OF INTELLECTUAL PROPERTIES AND INTELLECTUAL RIGHTS

The protection of information, marked as intellectual property or copyrights, is a very special technical task, because often it is difficult to define, if this information is

legally protected or the protection of information is not offered as an option. This task can be partly solved by using the "Copyright Demonstration" script, or by script named as "No Copy" script. In the most cases this method of protection is known as information hiding. As a result, the modification of cryptographic embedded type of LSB–algorithm with keys was developed. The strength of algorithm has been improved in comparison with classical stegano – LSB–algorithms. The main point of proposed steganographic method is the embedding of full-colored images into dynamic full-colored information objects. This way, if the image pixel intensity level changes from 0 to 255, it means that this image can be represented in eight bit-planes. Accordingly, this method is based on LSB–methodology of information hiding. The article deals with the methodology of system development for protecting and transferring graphic, text data to dynamic graphic objects. The modeling was made in the MATLAB application environment and thus the time depending results were obtained. On the basis of the developed LSB–method modification one can improve the protection of intellectual property rights in animated and video graphic objects by embedding the various full-colored digital watermarks. Also, the proposed method may have also a versatile usage.
Keywords: information security system, intellectual property, intellectual rights law, decomposition on the bit-plane, dynamic graphic objects, computing environment MATLAB.

Сагун Андрей Викторович, кандидат технических наук, доцент кафедры информатики и информационной безопасности, Черкасский государственный университет, Черкассы, Украина.
E-mail: avd29@ukr.net.
Сагун Андрій Вікторович, кандидат технічних наук, доцент кафедри інформатики та інформаційної безпеки, Черкаський державний технологічний університет, Черкаси, Україна.
Sagun Andrej, candidate of engineering sciences, associate professor at the department of informatics and information security, Cherkasy State Technological University, Cherkassy, Ukraine.

Щербак Леонид Николаевич, доктор технических наук, профессор, заведующий кафедрой компьютерных наук, Киевский международный университет, Киев, Украина.
E-mail: prof_scherbak@ukr.net.
Щербак Леонід Миколайович, доктор технічних наук, професор, завідуючий кафедри комп'ютерних наук, Київський міжнародний університет, Київ, Україна.
Scherbak Leonid, doctor of engineering sciences, professor of the of computer science department, Kyiv International university, Kyiv, Ukraine.

Хайдуров Владислав Владимирович, старший преподаватель кафедры компьютерных наук, Киевский международный университет, Киев, Украина.
E-mail: allif@ukr.net.
Хайдуров Владислав Володимирович, старший викладач кафедри комп'ютерних наук, Київський міжнародний університет, Київ, Україна.
Hajdurov Vladislav, senior lecturer of computer science department, Kyiv International university, Kyiv, Ukraine.

Кунченко-Харченко Валентина Ивановна, доктор технических наук, профессор кафедры информатики и информационной безопасности, Черкасский государственный университет, Черкассы, Украина.
E-mail: kunchenkokharchenko@gmail.com.
Кунченко-Харченко Валентина Іванівна, доктор технічних наук, професор кафедри інформатики та інформаційної безпеки, Черкаський державний технологічний університет, Черкаси, Україна.
Kunchenko-Kharchenko Valentina, doctor of engineering sciences, professor at the department of informatics and information security, Cherkasy State Technological University, Cherkassy, Ukraine.

Костянец Станислав Олегович, магистрант кафедры информатики и информационной безопасности, Черкасский государственный университет, Черкассы, Украина.
E-mail: stas121293@ukr.net.
Костянець Станіслав Олегович, магістрант кафедри інформатики та інформаційної безпеки, Черкаський державний технологічний університет, Черкаси, Україна.
Kostjanec Stanislav, master of informatics and information security department, Cherkasy State Technological University, Cherkassy, Ukraine.

Тетьора Михаил Сергеевич, магистрант кафедры информатики и информационной безопасности, Черкасский государственный университет, Черкассы, Украина, e-mail: mihailtetyora.94@mail.ru.
Тетьора Михайло Сергійович, магістрант кафедри інформатики та інформаційної безпеки, Черкаський державний технологічний університет, Черкаси, Україна.
Tetiora Mihajlo, master of informatics and information security department, Cherkasy State Technological University, Cherkassy, Ukraine.