УДК 004.056

Е.В. Мелешко

Кировоградский национальный технический университет, Кировоград

МЕТОД ВСТРАИВАНИЯ ДВУХУРОВНЕВЫХ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ В МЕДИАФАЙЛЫ ДЛЯ ЗАЩИТЫ АВТОРСКИХ ПРАВ

Предлагается метод встраивания двухуровневых цифровых водяных знаков в медиафайлы, а также протокол распределения стегоключей для защиты авторских прав в компьютерных сетях. Данный метод отличается от существующих наличием публичной и секретной части цифрового водяного знака для обычных пользователей и для арбитра соответственно.

Ключевые слова: *стеганография, цифровые водяные знаки, защита авторских прав, протокол распределения стегоключей.*

Вступление

Одним из перспективных способов защиты авторских прав на мультимедийный контент является внедрение в него невидимых цифровых водяных знаков (ЦВЗ) методами стеганографии. Несмотря на то, что на сегодняшний день существует множество теоретических работ по данной тематике: методы внедрения ЦВЗ в растровые изображения [3 – 8], векторные изображения [2], аудиофайлы [1, 9, 10], видеофайлы [11], общие принципы построения ЦВЗ [12 – 14] – на практике ЦВЗ применяются редко. И хотя общеизвестны такие примеры практического применения, как встраивание изображения обложки аудиодиска в музыкальные файлы, или информации о компьютерной игре в скриншот созданной пользователем, подобные реализации не столько защищают авторские права, сколько играют информационную роль. Такие ЦВЗ легко прочитать, удалить или заменить, так как их стойкость основана только на секретности стегоалгоритма. Также их применение не регламентировано никакими юридическими законами, в отличие от применения, например, электронной цифровой подписи.

Основная часть

При проведении исследования существующих стегоалгоритмов, предназначенных для внедрения ЦВЗ, было выявлено, что в большинстве алгоритмов основное внимание уделяется робастности ЦВЗ и «незаметности» встраиваемой информации для известных методов стегоанализа, но недостаточно внимания уделяется процедурам генерации стегоключей, протоколам их распределения, использованию удостоверяющих центров, фиксированию даты создания файла.

При исследовании работ [1 – 11] было выявлено, что в работах [3, 5, 8, 10, 11] стегоключи отсутствуют вообще, а в работах [1, 2, 4, 6, 7, 9] есть только один секретный стегоключ, протоколов распределения стегоключей не предложено, защита ЦВЗ основана только на «незаметности» стегосообщения для известных алгоритмов стегоанализа, обычные пользователи системы не могут просматривать ЦВЗ, как и кем должна осуществляться проверка авторских прав не предложено. В работе [12] для каждого пользователя системы создается копия одного и того же защищаемого файла с разным уникальным ЦВЗ (идентификатором пользователя), обладающим стойкостью к атаке сговором, информацию об авторе файла такой ЦВЗ не содержит. Данный алгоритм больше подходит для защиты файлов в локальной корпоративной сети с небольшим числом пользователей и позволяет определить злоумышленника при несанкционированном распространении информации за пределы сети, но мало подходит для защиты авторских прав в сети Интернет. В работах [13, 14] предложены протоколы распределения стегоключей. В этих протоколах необходим Арбитр, обычные пользователи читать ЦВЗ не могут, дату и время внедрения ЦВЗ в файл установить нельзя. В [14] ЦВЗ состоит из идентификаторов автора (продавца), пользователя (покупателя) и медиафайла (покупаемого контента), возможность защиты бесплатно распространяемого контента от плагиата в этом протоколе не предусмотрена.

Таким образом поставлена задача разработать метод встраивания ЦВЗ в медиафайлы, реализующий следующие возможности:

1. Однозначно идентифицировать автора (или правообладателя) медиафайла.

2. Определять точную дату создания (регистрации) файла, для разрешения конфликтов, связанных с обвинением в плагиате.

3. Обладать стойкостью к атакам злоумышленников, нацеленным на уничтожение или замену ЦВЗ.

4. Позволять обычным пользователям, покупающим платный или скачивающим свободно распространяемый цифровой мультимедиа-контент, просматривать ЦВЗ, содержащий информацию об авторе, а также быть проинформированными о последствиях нарушения авторских прав.

Третий и четвертый пункты при обычных схемах реализации ЦВЗ явно вступают в противоречие. Ведь если пользователь способен прочитать ЦВЗ, содержа-

щийся в файле, то теоретически он также способен его удалить или заменить. В классических реализациях ЦВЗ защита от его уничтожения или замены основана на секретности алгоритма стегокодера и стегодекодера, встроенного в программу пользователя. Т.е. с помощью закрытого стеганографического ПО пользователь способен просмотреть ЦВЗ, но не знает как он встраивается и извлекается, и в каких участках файла пребывает стегосообщение. Но данные реализации не соблюдают принципа Керкгоффса, рано или поздно любой стегоалгоритм будет рассекречен, поэтому стойкость системы должна основываться на секретности стегоключа. Существуют также стегоалгоритмы позволяющие просматривать ЦВЗ медиафайла только арбитру, в таких случаях пользователь может остаться не проинформированным об авторских правах на файл, если данная информация не размещена на ресурсе, с которого файл был загружен.

Для решения поставленной задачи, автором предлагается:

1. При встраивании ЦВЗ использовать стего ключи и протокол распределения стегоключей.

2. Ввести в протокол распределения стегоключей арбитра, далее называемого Стеганографическим центром защиты авторских прав (СЦЗАП).

3. Использовать двухуровневый ЦВЗ, состоящий из публичной части (ЦВЗ1), доступной для чтения всеми пользователями системы, и секретной части (ЦВЗ2), доступной для чтения только СЦЗАП.

4. Для каждого нового медиафайла создавать уникальные стегоключи, привязанные к дате и времени подачи запроса автора.

Представим двухуровневый ЦВЗ как:

$$W_d = \{W_p, W_s\}, \quad (1)$$

где W_d – двухуровневый ЦВЗ; W_p – публичная часть двухуровневого ЦВЗ, или ЦВЗ1; W_s – секретная часть двухуровневого ЦВЗ, или ЦВЗ2.

Сначала встраивается ЦВЗ1, функция встраивания:

$$F_1(k_p, W_p, C_e, S_1) = C_1, \quad (2)$$

где F_1 – функция встраивания ЦВЗ1 в стегоконтейнер; k_p – публичный стегоключ; C_e – пустой стегоконтейнер; S_1 – стегоалгоритм, используемый для встраивания ЦВЗ1; C_1 – стегоконтейнер, заполненный ЦВЗ1.

Далее встраивается ЦВЗ2, функция встраивания:

$$F_2(k_s, W_s, C_1, S_2) = C_2, \quad (3)$$

где F_2 – функция встраивания ЦВЗ2 в стегоконтейнер; k_s – секретный стегоключ; S_2 – стегоалгоритм, используемый для встраивания ЦВЗ2; C_2 – стегоконтейнер, заполненный ЦВЗ2.

Заполненный двухуровневым ЦВЗ стегоконтейнер представляет собой следующее множество:

$$C_2 = \{B, M_1, M_2\}, \quad (4)$$

где B – множество битов контейнера, которые остались неизменными после внедрения двухуровневого ЦВЗ; M_1 – множество битов контейнера, в которые внедрен ЦВЗ1; M_2 – множество битов контейнера, в которые внедрен ЦВЗ2.

Под стегоключом будем понимать псевдослучайную последовательность чисел, определяющую местонахождение скрытой информации в стегоконтейнере. Для корректной работы алгоритма публичный k_p и секретный k_s стегоключи должны генерироваться таким образом, чтобы $M_1 \cap M_2 = \varnothing$, чтобы при встраивании ЦВЗ2 не разрушался уже встроенный ЦВЗ1.

Предложенный протокол распределения стегоключей для встраивания двухуровневого ЦВЗ выглядит следующим образом:

$$A \rightarrow C: K_{ea}$$
$$C \rightarrow A: K_{ec}$$
$$A \rightarrow C: \{d\}K_{ec}$$
$$C \rightarrow A: K_p, \{K_s\}K_{ea}$$

где C – Стеганографический центр защиты авторских прав; A – Автор; K_{ec} – открытый ключ шифрования СЦЗАП; K_{ea} – открытый ключ шифрования Автора; d – данные об авторских правах на медиафайл, которые содержат ФИО автора, название медиафайла, краткое описание медиафайла (при необходимости) и содержание ЦВЗ (графическая и/или текстовая информация об авторе и медиафайле, которую необходимо встроить в стегоконтейнер). $\{d\}K_{ec}$ – данные об авторских правах d, зашифрованные ключом K_{ec}, $\{K_s\}K_{ea}$ – секретный стегоключ K_s, зашифрованный ключом K_{ea}.

Для получения ЦВЗ W_d над данными об авторских правах необходимо осуществить некоторые преобразования:

$$W_p = T_1(d); \quad (5)$$
$$W_s = T_2(d), \quad (6)$$

где T_1 – преобразование содержимого публичного ЦВЗ1 перед встраиванием; на этом этапе можно добавить информацию о последствиях нарушения авторских прав, выполнить помехоустойчивое кодирование данных; T_2 – преобразование содержимого секретного ЦВЗ2 перед встраиванием; на этом этапе можно выполнить шифрование и/или помехоустойчивое кодирование данных.

Рассмотрим схему реализации предложенных метода встраивания двухуровневого ЦВЗ и протокола распределения стегоключей, представленную на рис. 1. В разработанном протоколе распределения стегоключей между собой взаимодействуют следующие субъекты: создающие медиаконтент авторы, Стеганографический центр защиты авторских прав, легитимные пользователи и злоумышленники, пытающиеся присвоить чужой контент и/или выдать себя за автора.

Для создания и внедрения ЦВЗ выполняются следующие шаги:

1. Автор отправляет в СЦЗАП запрос на создание стегоключей для внедрения ЦВЗ.

2. Автор генерирует открытый K_{ea} и закрытый K_{da} ключи шифрования.

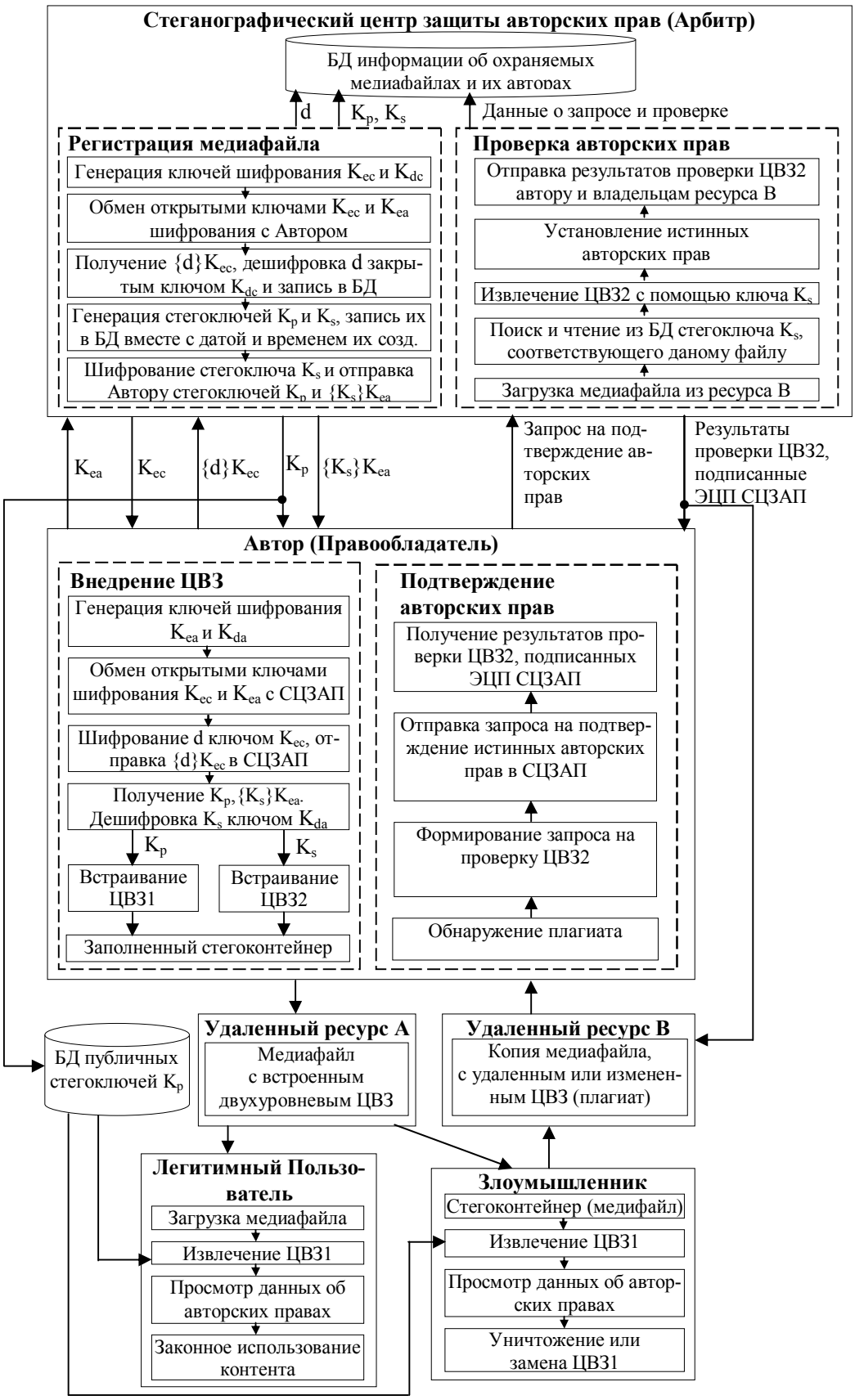

Рис. 1. Схема встраивания двухуровневого ЦВЗ и распределения стегоключей

3. СЦЗАП генерирует открытый K_{ec} и закрытый K_{da} ключи шифрования.

4. Происходит обмен открытыми ключами шифрования K_{ea} и K_{ec} между Автором и СЦЗАП.

5. Автор формирует данные о медиафайле d для СЦЗАП, содержащие его ФИО, название медиафайла, возможно краткое описание файла и содержание ЦВЗ. Под содержанием ЦВЗ, в данном

случае, понимается текстовая информация об авторе контента и/или графический логотип, постер и т.п.

6. Автор шифрует данные о медиафайле d открытым ключом шифрования СЦЗАП K_{ec} и отправляет их в СЦЗАП.

7. СЦЗАП получает данные d, генерирует уникальные публичный и секретный стегоключи и формирует учетную запись о медиафайле в своей БД, содержащую: ФИО автора, название медиафайла, его краткое описание (если есть), дату и время подачи заявки, содержимое ЦВЗ и сгенерированные стегоключи.

8. СЦЗАП шифрует секретный стегоключ K_s открытым ключом Автора K_{ea}, и отправляет его Автору.

9. СЦЗАП отправляет публичный стегоключ K_p Автору, а также размещает его в базе данных публичных стегоключей, доступной всем пользователям системы.

10. Автор получает стегоключи K_s и K_p. Зашифрованный секретный стегоключ K_s он дешифрует своим закрытым ключом шифрования K_{da}.

11. Автор встраивает в медиафайл ЦВЗ1 стегоалгоритмом S_1, используя стегоключ K_p, а также ЦВЗ2 стегоалгоритмом S_2, используя стегоключ K_s.

После осуществления встраивания ЦВЗ Автор размещает свой мультимедиа-контент на ресурсе А в свободный или платный доступ в зависимости от своих целей.

Легитимные пользователи, скачивающие медиафайл из ресурса А, могут просмотреть публичный ЦВЗ1, в который кроме данных об авторстве можно также встроить информацию о последствиях нарушения авторских прав.

Злоумышленники, которые также скачивают медиафайл из ресурса А, могут установив принцип работы стегоалгоритма S_1 удалить или изменить публичный ЦВЗ1. Но если они узнают как работает стегоалгоритм S_2, то не смогут осуществить те же операции с секретным ЦВЗ2, поскольку для того, чтобы знать какие биты файла нужно удалить или изменить нужно знать секретный стегоключ K_s.

Если злоумышленник попытается удалить публичный ЦВЗ1 и разместить медиафайл на ресурсе В без данных об авторе, или с ложными данными, то, в случае обращения в СЦЗАП настоящего автора (или его представителей), можно будет установить и подтвердить настоящее авторство.

Для установления подлинного авторства выполняются следующие шаги:

1. Автор (или представитель Автора), обнаруживший авторский контент на стороннем ресурсе с неправдивыми данными об авторстве, отсылает запрос в СЦЗАП, который должен содержать: ссылку на файл (или сам файл), имя подлинного автора, оригинальное название файла и другие необходимые данные.

2. СЦЗАП находит в своей базе данных запись об этом медиафайле, и если соответствующая запись есть, берет из нее уникальный, соответствующий этому файлу, секретный стегоключ K_s.

3. С помощью данного стегоключа осуществляется извлечение секретного ЦВЗ2 из медиафайла. Если извлеченные данные соответствуют данным автора, подавшего жалобу, значит он действительно настоящий автор, в противном случае жалоба отклоняется.

4. СЦЗАП подписывает результаты проверки секретного ЦВЗ2 своей электронной цифровой подписью.

5. СЦЗАП отправляет результаты проверки ЦВЗ2, подписанные своей цифровой подписью, Автору и владельцам ресурса В (при подтверждении нарушения авторских прав).

Для работоспособности данного протокола должны существовать механизмы блокировки незаконно размещенного контента и методы воздействия на злоумышленника, а заключение СЦЗАП о подлинном авторстве контента должно иметь юридическую силу. Необходимы соответствующие законы, и официальная регистрация СЦЗАП по аналогии с Центрами сертификации ключей для цифровых подписей. Эти задачи выходят за рамки данного исследования и лежат в юридической плоскости.

Предложенный метод встраивания двухуровневого ЦВЗ обладает следующими достоинствами:

1. Позволяет пользователям просматривать содержимое публичного ЦВЗ1 для получения информации об авторских правах на файл, но не дает доступа к секретному ЦВЗ2, предназначенному для просмотра арбитром (СЦЗАП), на случай попытки уничтожения или замены данных об авторе.

2. Позволяет установить дату и время регистрации файла, т.к. для каждого нового созданного файла автор получает новый секретный и публичный стегоключи, которые записываются в БД вместе с соответствующими датой и временем, что позволяет исключить некоторые виды мошенничества со стороны владельца стегоключа – не позволяет встроить в чужой файл свой ЦВЗ; а также информация о времени может быть решающей, так как файл мог ранее уже быть опубликованным кем-то другим, и важно установить, кто на самом деле впервые опубликовал файл.

3. Не нужно передавать сам медиафайл в СЦЗАП, что исключает вероятность перехвата файла злоумышленником еще до встраивания ЦВЗ, возможности воровства файла самими сотрудниками СЦЗАП, а также сокращает необходимый объем базы данных СЦЗАП.

Недостатком данного протокола является невозможность узнать о нарушении авторских прав, если автор (или другой пользователь) не заявит о незаконном использовании контента или плагиате, а злоумышленник удалит публичный ЦВЗ1, т.к. автоматической проверки файлов не ведется.

Выводы

В данной статье предложены метод встраивания двухуровневого ЦЗВ и протокол распределения стегоключей в системах защиты авторских прав, позво-

ляющие противостоять активным атакам злоумышленников, нацеленным на уничтожение ЦВЗ. Разработанный метод отличается от существующих двухуровневой системой защиты, состоящей из публичного ЦВЗ1 и секретного ЦВЗ2, наличием арбитра (СЦЗАП), проверяющего ЦВЗ2, фиксированием даты и времени получения запроса от автора на регистрацию медиафайла и защиту его ЦВЗ. Предложенный метод позволяет решать ряд задач, которые не позволяют решить стандартные алгоритмы встраивания ЦВЗ, однако все же обладает рядом недостатков, например, отсутствием возможности автоматической проверки медиаконтента на соблюдение авторских прав. Также проблемой является отсутствие юридических законов относительно ЦВЗ вообще и предложенного СЦЗАП в частности, но устранение этой проблемы лежит в юридической, а не в программной сфере.

Дальнейшая разработка и усовершенствование протоколов распределения стегоключей для ЦВЗ является очень актуальной задачей, так как с каждым годом все больше возрастает потребность в действенной защите авторских прав на цифровой контент в компьютерных сетях, а адекватные сегодняшней реальности методы (в достаточной мере приспособленные к цифровым медиа-ресурсам) отсутствуют.

Список литературы

1. Дудатьєв А.В. Розробка алгоритму приховування цифрових водяних знаків у аудіофайлах формату wav / А.В. Дудатьєв, П.В. Козлюк, Д.С. Оксимчук // Наукові праці Вінницького національного технічного університету. – 2011 –№1. – С. 3-11.

2. Карпінець В.В. Дослідження стеганографічної стійкості методу вбудовування цифрових водяних знаків у векторні зображення / В.В. Карпінець, Ю.Є. Яремчук // Вісник Вінницького політехнічного інституту. – 2011 – № 3. – С. 200-205.

3. Земцов А. Н. Защита авторских прав с помощью дискретного вейвлет-преобразования / А.Н. Земцов, С. МД. Рахман // Известия Волгоградского государственного технического университета. – 2009 – №6, Том 6. – С. 134-136.

4. Глумов Н.И Алгоритм поблочного встраивания стойких ЦВЗ в крупноформатные изображения / Н.И Глумов, В.А. Митекин // Компьютерная оптика. – Самара: ИСОИ РАН. – 2011 – №3. Том 35. – С. 368-372.

5. Кайнов П.А. Внедрение цифровых водяных знаков с использованием сегментации изображения / П.А. Кайнов , Б.Б. Борисенко // Вестник Казанского технологического университета. – 2013 – №4. Том: 16 – С. 286-291 .

6. Семёнов К.П. Алгоритмы встраивания цифровых водяных знаков в растровые изображения / К.П. Семёнов, П.В. Зайцев // Информационная безопасность регионов. – Саратов: СГСЭУ . – 2012 – №1. – С. 46-50.

7. Урывская Д.А. Псевдоголографические развертки и их приложения к задачам защиты информации / Д.А. Урывская // Омский научный вестник. – 2012 –№2-110 . – С. 275-277.

8. Белобокова Ю.А. Метод встраивания цифровых водяных знаков для доказательства подлинности фотоизображений / Ю.А. Белобокова // Известия Тульского государственного университета. Технические науки. – 2013 – № 3 . – С. 106-110.

9. Алексеев А.П. Методы внедрения информации в звуковые файлы формата midi / А.П. Алексеев, А.А. Аленин // Инфокоммуникационные технологии. – Самара: ПГУТИ. – 2011 – №1. Том 9. – С 84-89.

10. Шишкин А.В. Устойчивые цифровые водяные знаки для звуковых сигналов / А.В. Шишкин // Известия высших учебных заведений. Радиоэлектроника. – К.: НТУУ «КПИ». – 2011 – №3. Том 54 – С. 30-38.

11. Бахрушина Г.И. Формирование и применение кусочно-непрерывных функций при защите видеопродукции с помощью цифровых водяных знаков / Г.И. Бахрушина // Вестник Приамурского государственного университета им. Шолом-Алейхема. – Биробиджан: ПГУША. – 2011. – № 2. – С. 30-40 .

12. Стружков Р.С. Цифровые водяные знаки, устойчивые к атаке сговором / Р.С. Стружков , Т.М. Соловьёв , Р.И. Черняк // Прикладная дискретная математика. – Томск: НИТГУ . – 2009 – №1. – С. 56-59 .

13. Cheung S. C., Chiu Dickson K. W. A Watermarking Infrastructure for Enterprise Document Management // Proceedings of the 36th Hawaii International Conference on System Sciences - 2003

14. Hu Yuping, Zhang Jun A Secure and Efficient Buyer-Seller Watermarking Protocol // Journal of Multimedia, Vol 4, No 3 (2009), P.161-168

Поступила в редколлегию 15.11.2013

Рецензент: д-р техн. наук, с.н.с. Г.А. Кучук, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.

МЕТОД ВБУДОВУВАННЯ ДВОРІВНЕВИХ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ У МЕДІАФАЙЛИ ДЛЯ ЗАХИСТУ АВТОРСЬКИХ ПРАВ

Є.В. Мелешко

Пропонується метод вбудовування дворівневих цифрових водяних знаків у медіафайли, а також протокол розподілу стегоключів для захисту авторських прав у комп'ютерних мережах. Даний метод відрізняється від існуючих наявністю публічної та секретної частини цифрового водяного знаку для звичайних користувачів і для арбітра відповідно.

Ключові слова: *стеганографія, цифрові водяні знаки, захист авторських прав, протокол розподілу стегоключів*

METHOD OF EMBEDDING OF TWO-LEVEL DIGITAL WATERMARKS INTO MEDIA FILES FOR COPYRIGHT PROTECTION

E.V. Meleshko

A method of two-level embedding digital watermarks in media files and stego-key distribution protocol is proposed for copyright protection in computer networks. This method differs from the existing ones by presence of a public and secret part of digital watermark for users and for arbiter respectively.

Keywords: *steganography, digital watermark, copyright protection, stego-key distribution protocol.*