ПРОГРЕСИВНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

ПРОГРЕССИВНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

PROGRESSIV INFORMATICS TECHNOLOGIES

УДК 004.056.53:003.26

Андрущенко Д. М.

Младший научный сотрудник, ассистент, Запорожский национальный технический университет, Украина, E-mail: andrush85@mail.ru

ЗАЩИТА АВТОРСКИХ ПРАВ НА ЦИФРОВЫЕ ИЗОБРАЖЕНИЯ

Разработан метод встраивания цифровых водяных знаков с использованием электронных цифровых подписей сторон, участвующих в процессе передачи авторского права. Метод позволяет правообладателю выявить нарушителя при появлении контрафактных копий его продукта, обнаружить и подтвердить факт незаконного использования изображений при возникновении спорных ситуаций в судебном порядке. Кроме того, метод позволяет лицензиату продукта в случае ложного обвинения доказать факт законного использования.

Ключевые слова: метод защиты авторских прав, цифровые изображения, подтверждение авторства, выявление правонарушителя.

ВВЕДЕНИЕ

Цифровое изображение как продукт деятельности высококвалифицированных специалистов часто создается в коммерческих целях и характеризуется большой трудоемкостью и ценностью. Поэтому несанкционированное использование изображений зачастую приносит убытки его правообладателю.

Закон об авторском праве и смежных правах [1] свидетельствует, что авторское право на произведение возникает в результате факта его создания. А для возникновения и осуществления авторского права не требуется регистрация произведения. Однако, несмотря на это, вследствие возникновения споров может понадобиться подтверждение факта создания фотографического произведения настоящим автором в судебном порядке или подтверждение факта заключения лицензионного договора.

Для защиты авторских прав на цифровые изображения в последнее время предложено достаточно много методов, основанных на компьютерной стеганографии [2, 3].

Одни из них предназначены для создания технологических препятствий нарушению авторских и смежных прав на цифровые изображения [2]. При этом они основаны на том, что устройство, на котором воспроизводится цифровой объект, получает информацию о наличии прав у издателя и принимает решение о разрешении доступа к информации пользователю [4]. Однако, такие способы не позволяют предотвратить возможность недобросовестным пользователям, получившим разрешение на доступ к информации, сделать контрафактную копию цифрового объекта. А если количество пользователей достаточно велико, правообладатель не сможет обнаружить правонарушителя.

Другие способы защиты авторских прав изображений основаны на встраивании цифровых водяных знаков (ЦВЗ) путем изменения частотных коэффициентов в пределах матрицы преобразования [5]. Тогда в случае правонарушения наличие ЦВЗ в изображении подтверждает права автора. Однако такие способы не предусматривают возможности определения правонарушителя авторских прав при выявлении факта появления контрафактной копии.

ПОСТАНОВКА ЗАДАЧИ

Цель данной работы состоит в разработке более эффективного способа защиты авторских прав на цифровые изображения, который расширит возможности существующих способов и позволит правообладателю выявлять правонарушителей при появлении контрафактных копий.

DOI 10.15588/1607-3274-2014-1-19

Автором предлагается в процессе встраивания цифрового водяного знака его предварительно разделить на две или более частей так, чтобы каждая из них не могла быть создана отдельно друг от друга [6]. Соответственно, должны быть сформированы два или более ключей для извлечения этих частей цифрового водяного знака.

Для встраивания цифрового водяного знака используется частотная область изображения. Встраивание производится на основе дискретного косинусного преобразования точек изображения в частотные коэффициенты путем изменения этих коэффициентов. При необходимости можно извлечь каждую часть цифрового водяного знака, используя соответствующее дискретное косинусное преобразование, путем сравнения значений частотных коэффициентов с известными значениями.

Наличие двух или более частей цифрового водяного знака в копии цифрового изображения, не дублирующихся, а согласованных между собой так, что каждая из них не может быть создана отдельно от других частей, позволяет владельцам ключей отдельно друг от друга идентифицировать копию изображения и выявлять факт нарушения без знания других ключей. Согласование различных частей цифрового водяного знака между собой и невозможность создания различных частей отдельно друг от друга позволяют владельцу при выявлении факта правонарушения идентифицировать правонарушителя.

УСОВЕРШЕНСТВОВАННЫЙ МЕТОД ЗАЩИТЫ

Метод, предложенный в данной работе, заключается в следующем:

1. При передаче имущественного права на объект авторских прав составляется лицензионное соглашение, которое подписывается электронными цифровыми подписями разных сторон. Таким образом, они подтверждают согласие друг с другом.

2. Из поочередно идущих битов электронных цифровых подписей составляется ЦВЗ. При этом каждая из цифровых подписей формирует отдельную часть ЦВЗ.

3. Для сокрытия данных используют частотную область контейнера. Для этого изображение разбивается на блоки размерностью 8×8 пикселей, и к каждому блоку применяется двумерное дискретное косинусное преобразование (ДКП). Каждый блок пригоден для записи одного бита информации. Перед встраиванием ЦВЗ произвольным образом выбирается столько блоков ДКП, сколько битов в ЦВЗ.

4. Доверенное лицо или аппаратное устройство встраивает в оригинал изображения цифровой водяной знак, состоящий из этих электронных цифровых подписей. Для встраивания каждого бита ЦВЗ используется очередной блок ДКП, входящий в выбранную группу блоков. Выбираются N произвольных коэффициентов ДКП из полосы средних и низких частот, которые задаются координатами (υ_1, ν_1), (υ_2, ν_2), …, (υ_N, ν_N). Также выбираются две фиксированные величины S и P. Для передачи бита «0» коэффициенты с координатами (υ_1, ν_1), (υ_2, ν_2), …, (υ_N, ν_N) меняются так, чтобы среднее арифметическое этих коэффициентов стало не ниже величины $S + P$. А для передачи бита «1» меняются так, чтобы их среднее арифметическое стало не выше, чем $(S - P)$.

5. После встраивания ЦВЗ каждая из сторон, участвующая в лицензионном соглашении, получает ключ, который состоит из величин K_{bi}, необходимых для извлечения битов электронной цифровой подписи одного из участников. Величина K_{bi} включает в себя номер блока ДКП, в который встроен i-ый бит данных ЦВЗ, и координаты (υ_1, ν_1), (υ_2, ν_2), …, (υ_N, ν_N), необходимые для извлечения i-ого бита.

6. При извлечении битов цифрового водяного знака из известного блока ДКП и известных коэффициентов, заданных координатами (υ_1, ν_1), (υ_2, ν_2), …, (υ_N, ν_N), если среднее арифметическое значение коэффициентов больше S, то извлекается значение 0, иначе извлекается значение 1.

Оптимальное значение S равно математическому ожиданию среднего значения коэффициентов с координатами (υ_1, ν_1), (υ_2, ν_2), …, (υ_N, ν_N), вычисленному на основе выборки из некоторого количества блоков ДКП.

Порог встраивания P влияет на устойчивость стеганосистемы. Чем больше значение P, тем более стеганосистема устойчива к искажениям изображения, но тем хуже становится качество изображения при встраивании информации.

Количество выбранных коэффициентов N лежит в диапазоне от 1 до 15 и влияет на скрытность стеганографической системы, чем больше значение N, тем сложнее проводить ее стеганоанализ.

ПРИМЕР ИСПОЛЬЗОВАНИЯ ПРОТОКОЛА

Приведем пример использования предлагаемого метода на практике.

Пусть издательству (лицензиат L) необходимо приобрести имущественные права на фотографию (рис. 1), владельцем которой является фотостудия или частный фотограф (лицензиар F). Для этого представители обеих сторон подписывают лицензионный договор своими

Рис. 1. Изображение пчелы (оригинал) и выбранный фрагмент для встраивания ЦВЗ

электронными цифровыми подписями. При этом в договоре содержатся уменьшенная копия изображения, права и обязанности сторон.

При использовании предложенного метода защиты каждым участником генерируются электронные коды: $E1$ – электронная цифровая подпись лицензиата L и $E2$ – электронная цифровая подпись лицензиара F. После того электронный нотариус M создает метку времени [7] для подписанного лицензионного договора и заверяет ее своей электронной цифровой подписью, получая тем самым электронный код $E3$. Далее доверенное лицо T или аппаратное устройство получает оригинал изображения и электронные коды $E1$, $E2$, $E3$ и встраивает цифровой водяной знак, представляющий собой чередующиеся биты электронных кодов $E1$, $E2$ и $E3$.

Для извлечения цифрового водяного знака доверенное лицо T формирует ключи $K1$, $K2$ и $K3$. При этом ключ $K1$ позволяет извлекать только электронный код $E1$, ключ $K2$ позволяет извлекать только электронный код $E2$, ключ $K3$ позволяет извлекать только электронный код $E3$.

Лицензиат L получает ключ $K2$, который позволяет извлечь из изображения электронную цифровую подпись лицензиара F (код $E2$), лицензиар F получает ключ $K1$, который позволяет извлекать электронную цифровую подпись лицензиата L (код $E1$). Ключ $K3$ получает электронный нотариус M.

При возникновении спора о нарушении авторского права как стороне, получившей лицензию, так и самому лицензиару может понадобиться подтверждение факта заключения лицензионного соглашения в судебном процессе.

В таком случае для защиты своих прав при легальном использовании изображения лицензиат L может предъявить в судебном процессе лицензионный договор вместе со своим ключом $K1$ для извлечения электронной цифровой подписи лицензиара $E2$. А для защиты прав лицензиара F в случае выявления правонарушения он может предъявить в судебном процессе лицензионный договор вместе со своим ключом $K2$ для извлечения электронной цифровой подписи лицензиата $E1$. Кроме того, может быть привлечен электронный нотариус M для подтверждения метки времени.

ПРОГРАММНАЯ РЕАЛИЗАЦИЯ МЕТОДА

Программная реализация метода выполнена на языке программирования C#.

Пример реализации функции, осуществляющей встраивание, представлен в листинге 1, фрагмент реализации функции, осуществляющей извлечение данных, представлен в листинге 2.

Листинг 1. Фрагмент программы для встраивания битов ЦВЗ в изображение на языке программирования C#:

```
public const int N = 8;
public float[,][,] EmbedWatermark(float[,][,] DCT, int imax,
int jmax, float Sum, float P)
{
      float[,][,] DCT_emb = new float[imax,jmax][,];
        for (int i = 0; i < imax; i++)
       {
        for (int j = 0; j < jmax; j++)
        {
         DCT_emb[i, j] = new float[8,8];
         for (int ii = 0; ii < 8; ii++)
           for (int jj = 0; jj < 8; jj++)
             DCT_emb[i, j][ii, jj] = DCT[i, j][ii, jj]
              float PP = Sum + P - (DCT_emb[i, j][3, 4]
+ DCT_emb[i, j][4, 3]) / 2;
               if (P > 0 && PP > 0)
               {
          DCT_emb[i, j][3, 4] = DCT_emb[i, j][3, 4] + PP;
          DCT_emb[i, j][4, 3] = DCT_emb[i, j][4, 3] + PP;
               }
              if (P < 0 && PP < 0)
               {
          DCT_emb[i, j][3, 4] = DCT_emb[i, j][3, 4] + PP;
          DCT_emb[i, j][4, 3] = DCT_emb[i, j][4, 3] + PP;
               }
        }
       }
     public static float[,] DirectDct(float [,] image)
     {
       float[,] DctResult = new float[N, N];
       for (int u = 0; u < N; u++) {
         for (int v = 0; v < N; v++) {
           double matrixSum = 0;
           for (int x = 0; x < N; x++)
             {
              double rowSum = 0;
              for (int y = 0; y < N; y++)
              {
               rowSum += C(x) * C(y) * image[x,y] *
             Math.Cos((2 * u + 1) * x * Math.PI / 2 / N) *
             Math.Cos((2 * v + 1) * y * Math.PI / 2 / N);
              }
             matrixSum += rowSum;
            }
   DctResult[u,v] = (float)(matrixSum / Math.Sqrt(2 * N));
          }
        }
        return DctResult;
      }
```

Листинг 2. Фрагмент программы для извлечения битов ЦВЗ из изображения на языке программирования C#:

```
      public string ExtractWatermark(float[,][,] DCT_emb,
int imax, int jmax, float Sum)
      {
        string result = "";
       for (int i = 0; i < imax; i++)
        {
         for (int j = 0; j < jmax; j++)
          {
  if ((DCT_emb[i, j][3, 4] + DCT_emb[i, j][4, 3]) / 2 > Sum)
result += "1";
```

```
                else result += "0";
            }
        }
        return result;
    }
```

Примеры работы программы для различных значений порога встраивания *P* представлены на рис. 2. На рис. 2, *а* показан фрагмент канала синего цвета для изображения пчелы со встроенным ЦВЗ с порогом встраивания *P*=5, на рис. 2, *б* – ЦВЗ с порогом встраивания *P*=25, а на рис. 2, *в* – с порогом встраивания *P*=45. Примеры показывают, что чем больше порог встраивания, тем сильнее ухудшается качество изображения при встраивании ЦВЗ.

ВЫВОДЫ

Разработан метод защиты авторских прав на цифровые изображения, который позволяет расширить возможности существующих методов. Размещение электронных цифровых подписей лицензиата, лицензиара и электронного нотариуса непосредственно в статическом изображении в виде цифрового водяного знака исключает возможность использования объекта авторского права отдельно от лицензионного договора. Тем самым, при появлении контрафактной копии изображения правообладатель может быстро идентифицировать правонарушителя, а нарушение условий лицензионного договора может быть выявлено и доказано в судебном процессе. Кроме того, неоправданное обвинение может быть опровергнуто лицензиатом благодаря извлечению электронной цифровой подписи лицензиара. А при появлении спора может быть привлечен электронный нотариус для подтверждения факта заключения договора, благодаря извлечению электронной цифровой подписи нотариуса.

а)

б)

в)

Рис. 2. Канал синего цвета фрагмента изображения пчелы со встроенным водяным знаком и порогом встраивания а) *P*=5; б) *P*=25; в) *P*=45

Расчет экономической эффективности и теоретической окупаемости использования метода в стеганографических системах показал целесообразность его реализации.

В дальнейшем планируется разработать программный комплекс для защиты авторских прав на цифровые изображения путем использования предложенного метода, а также провести анализ стойкости этого метода и сравнить ее со стойкостью других известных методов.

СПИСОК ЛИТЕРАТУРЫ

1. Закон України про авторське право і суміжні права [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/3792-12.
2. Стеганография, цифровые водяные знаки и стеганоанализ [Текст] / [Аграновский А. В., Балакин А. В., Грибунин В. Г., Сапожников С. А.]. – М. : Вузовская книга, 2009. – 220 с.
3. *Коханович, Г. Ф.* Компьютерная стеганография. Теория и практика. [Текст] / Г. Ф. Коханович, А. Ю. Пузыренко. – К. : МК-Пресс, 2006. – 288 с.
4. Пат. 2347266 Росія, МПК G06F17/00. Способ и устройство для получения и удаления информации относительно объектов цифровых прав [Електронний ресурс] / ЛИ Биунг-рае, КИМ Тае-сунг, ДЗУНГ Киунг-им та ін. – 2006138021/09; заявл. 15.03.2005; опубл. 10.05.2008 р. – 42 с.: ил. . – Режим доступу: http://www.findpatent.ru/patent/234/2347266.html.
5. Пат. 57243 Україна, МПК H03M 13/37. Спосіб захисту авторських прав векторних зображень цифровими водяними знаками у вигляді електронного коду [Електронний ресурс] / В.В. Карпінець, Ю.Є. Яремчук. – № u201015193, заявл. 16.12.2010, опубл. 10.02.2011, Бюл.№ 3, 2011 р. – 5 с. – Режим доступу: http://base.uipv.org/searchINV/.
6. Пат. 81168 Україна, МПК H04L 9/8 (2006.01). Спосіб захисту авторського права на цифрові зображення [Текст]/ Д. М. Андрущенко, Г. Л. Козіна, Л. М. Карпуков. – № u2012 14519, заявл. 18.12.2012, опубл. 25.06.2013, Бюл. № 12, 2013 р. – 3 с.
7. Служба мітки часу та цифрового підпису [Електронний ресурс]. – Режим доступу: https://metkavremeni.com/timestamp_pgp_sign_file-ukrainian.html

Стаття надійшла до редакції 18.11.2013.
Після доробки 19.03.2014.

Андрущенко Д. М.
Молодший науковий співробітник, асистент, Запорізький національний технічний університет, Україна

ЗАХИСТ АВТОРСЬКИХ ПРАВ НА ЦИФРОВІ ЗОБРАЖЕННЯ

Розроблено метод вбудовування цифрових водяних знаків з використанням електронних цифрових підписів сторін, які беруть участь у процесі передачі авторського права. Метод дозволяє правовласнику виявити порушника при появі контрафактних копій його продукту, з'ясувати і підтвердити факт незаконного використання зображень при виникненні спірних ситуацій в судовому порядку. Крім того, метод дозволяє ліцензіату продукта в разі помилкового звинувачення довести факт законного використання.

Ключові слова: метод захисту авторських прав, цифрові зображення, підтвердження авторства, виявлення правопорушника.

Andrushchenko D. M.
Assistant, Zaporizhzhya National Technical University, Ukraine

METHOD FOR PROTECTION OF DIGITAL IMAGE COPYRIGHT

There are many ways to protect copyright of digital images assigned for creating technological barriers against copyright and neighboring right violation when using digital images. But most of them do not foresee possibility of determination of copyright violator on detecting appearance of counterfeit copies.

The method of digital images copyright protection is offered in the paper. It involves embedding digital watermarks into a digital image and using electronic signatures of the parties that are taking part in assignment of copyright. A discrete cosine transform is used for data hiding.

Using the proposed method will significantly reduce the risk of unauthorized distribution of digital and raster images. When copyright violation occurs, the owner will be able to identify the violator and protect their rights in a court or administrative procedure.

Keywords: method of copyright protection, digital images, proof of authorship, identify the offender.

REFERENCES

1. Zakon Ukrainy pro avtorske pravo i sumizhni prava [Elektronnyi resurs]. – Rezhym dostupu: http://zakon.rada.gov.ua/laws/show/3792-12.
2. Ahranovskii A. V., Balakin A. V., Hribunin V. H., Sapozhnikov S. A. Stehanohrafiia, tsyfrovye vodianie znaki i stehanoanaliz. Moscow, Vuzovskaia kniha, 2009, 220 p.
3. Kokhanovich H. F., Puzyrenko A. Yu. Kompyuternaia stehanohrafiia. Teoriia y praktika. [Tekst]. Kiev, MK-Press, 2006, 288 p.
4. Pat. 2347266 Rosiia, MPK G06F17/00. Sposob y ustroistvo dlia polucheniia i udaleniia informatsii otnositelno obektov tsifrovykh prav [Elektronnyi resurs] / LY Byunh-rae, KYM Tae-sunh, DZUNH Kyunh-ym ta in. – 2006138021/09; zaiavl. 15.03.2005; opubl. 10.05.2008 r. – 42 s.: yl. . – Rezhym dostupu: http://www.findpatent.ru/patent/234/2347266.html.
5. Karpinets V. V., Yaremchuk Yu. Ye. Pat. 57243 Ukraina, MPK H03M 13/37. Sposib zakhystu avtorskykh prav vektornykh zobrazhen tsyfrovymy vodianymy znakamy u vyhliadi elektronnoho kodu [Elektronnyi resurs], № u201015193, zaiavl. 16.12.2010, opubl. 10.02.2011, Byul.№ 3, 2011 r. – 5 p. – Rezhym dostupu: http://base.uipv.org/searchINV/.
6. Pat. 81168 Ukraina, MPK H04L 9/8 (2006.01). Sposib zakhystu avtorskoho prava na tsyfrovi zobrazhennia [Tekst]/ D.M. Andrushchenko, H.L. Kozina, L.M. Karpukov. – № u2012 14519, zaiavl. 18.12.2012, opubl. 25.06.2013, Byul.№ 12, 2013 r. – 3 s.
7. Sluzhba mitky chasu ta tsyfrovoho pidpisu [Elektronnyi resurs]. – Rezhym dostupu: https://metkavremeni.com/timestamp_pgp_sign_file-ukrainian.html