ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ОБРАЗОВАНИИ, ЭКОНОМИКЕ И МЕНЕДЖМЕНТЕ

УДК 338
Код РИНЦ 06.00.00

ВЛИЯНИЕ ИНФОРМАЦИОННЫХ И ЦИФРОВЫХ ТЕХНОЛОГИЙ НА ИНТЕЛЛЕКТУАЛЬНУЮ СОБСТВЕННОСТЬ

© 2020 Булавко Ольга Александровна
доктор экономических наук, профессор
© 2020 Туктарова Лилия Равильевна
кандидат экономических наук, доцент
Самарский государственный экономический университет
E-mail: Vikigor163@mail.ru

Ключевые слова: интеллектуальная собственность, информационные технологии, цифровые технологии, компьютерная стенография, цифровые водяные знаки.

Статья посвящена рассмотрению аспектов влияния информационных и цифровых технологий на вопросы, связанные с авторским правом и интеллектуальной собственностью. Авторы рассматривают возможность эффективного развития экономики и распространения гиперконкурентных технологий с позиции информационно-сетевой и интеллектуально-психологической направленности.

Глобальная современная экономика является информационно-сетевой, интеллектуально-психологической с присущими ей гиперконкурентными технологиями и методами информационно-психологического, программируемо-управляемого воздействия на сознание, психику и волю людей (производителей и потребителей), регулирования рынка и формирования механизма защиты прав на интеллектуальную собственность получать больше прибыли.[1]

В настоящее время развитие информационных технологий происходит очень стремительно, а количество пользователей в сети интернет растет каждый день. Любой файл, представленный в цифровой форме, может быть скопирован, модифицирован и распространен.

По мнению Ю.А. Семенова, "распространение цифровых технологий дает повод к рассуждению о формировании новых социально-экономических отношений, цифровой экономики".[2]

Именно поэтому мультимедийная продукция уязвима в плане ее нелегального использования. В связи с этой проблемой разрабатываются различные методы защиты информации.

Защиту цифровых данных обеспечивают методы криптографии и стеганографии. Основное отличие этих методов заключается в том, что криптографические методы скрывают содержимое файла путем шифрования, а в стеганографических методах скрывается сам факт передачи какой-либо информации.

Компьютерная стеганография - раздел стеганографии, который изучает системы скрытой передачи информации, в которых в качестве контейнера выступают аппаратное или программное обеспечение компьютера, цифровые данные. Популярность исследований в области стеганографии обусловлены ростом потребности передачи скрытой информации в общедоступных каналах связи, так как стеганографические системы позволяют вносить незаметные для третьих лиц изменения в файл-контейнер.

Основные направления компьютерной стеганографии: методы текстовой стеганография, методы цифровой стеганографии и методы, ориентированные на формат данных. В методах цифровой стеганографии контейнером выступают одномерные или многомерные цифровые сигнала, имеющие физическую природу. Под такими сигналами понимаются изображения, видеоданные и звуковые файлы.

Один из наиболее популярных и эффективных методов в области стеганографии для защиты авторских прав и защиты от несанкционированного копирования заключается во встраивании в защищаемый объект стеганографических вставок - меток, которые несут в себе некий идентификатор правообладателя. Такие метки называют цифровыми водяными знаками.

Целью данной статьи является разработка и реализация алгоритма, осуществляющего внедрение в видеоданные и детектирование водяных знаков, стойких к геометрическим преобразованиям и фильтрации.

Были поставлены следующие задачи:

- Исследование проблемы встраивания стойких ЦВЗ;
- Обзор существующих алгоритмов встраивания стойких ЦВЗ;
- Разработка алгоритма на основе создания стойкого пространственного шаблона ЦВЗ;
- Реализация алгоритма в программной среде Matlab.

В настоящее время в проблеме защиты авторского права особое внимание уделяется защите нематериального имущества. Главным составляющим нематериального имущества является интеллектуальная собственность. Это проблема приобрела особую значимость с развитием цифровых технологий и интернета. Одним из способов решения данной проблемы является встраивание цифровых водяных знаков в мультимедиа файлы, в частности в цифровые изображения и видеоданные.

Под ЦВЗ принято понимать специальные метки, которые используются для аутентификации цифровых данных, а также для защиты от их нелегального использования. Встраиваемый знак может быть как видимым, так и невидимым человеческому глазу.

Второй вариант в свою очередь делится на хрупкие, полухрупкие и стойкие цифровые водяные знаки.

Хрупкие ЦВЗ разрушаются после любых незначительных преобразований контейнера. В случае полухрупких систем ЦВЗ, водяной знак обладает избирательной стойкостью, он может быть устойчив к одним преобразованиям и неустойчив к другим. В противоположность хрупким ЦВЗ, стойкие знаки должны быть устойчивы к различным видам атак: геометрическим преобразованиям, сжатию и т.д. Основные задачи, которые можно решить с помощью ЦВЗ - систем:

- защита от несанкционированного копирования;
- защита авторских прав;

- защита от изменений;
- защита от подделки.

Задача защиты авторских прав может быть решена с помощью сценария "Демонстрация права собственности" [1Barni]. Если автор произведения хочет доказать, что является единственным законным владельцем произведения, то после создания этого произведения, он встраивает в него стойкий водяной знак, который может однозначно определить его как владельца.

В силу специфики данной области применения ЦВЗ должен быть максимально устойчив к широкому набору искажений контейнера, таких как линейная и нелинейная фильтрации, сжатие с потерями, кадрирование и другим. Также у алгоритмов встраивания ЦВЗ должна быть низкая вычислительная сложность.

Стоит отметить, что не существует алгоритма, который был бы устойчив ко всем видам атак. Каждый существующий подход создания системы встраивания цифровых водяных знаков создавался для противостояния определенным атакам или противостояния определенному набору атак.

Целями атаки на систему встраивания информации в видеоданные могут быть не только извлечение или удаление встроенной информации, но и искажение ее таким образом, чтобы детектирование или извлечение этой информации законным правообладателем стало невозможно.

Атаками такого рода являются геометрические атаки в виде сдвига каждого видеокадра на неопределенное число пикселов вдоль пространственных координатных осей, или в виде поворота каждого видеокадра на неопределенный угол, или изменения на неопределенную величину масштаба кадров.

При сдвиге на фиксированную величину все точки пространственной области изображения-контейнера смещаются по некоторому правилу.

Положение отсчетов контейнера после сдвига определяется по следующим формулам:

$$x' = x + t_{x'} \quad 1$$

$$y' = y + t_{y'} \quad 2$$

где x - начальное положение отсчета на оси абсцисс;

y - начальное положение отсчета на оси ординат;

t_x - сдвиг вдоль оси абсцисс;

t_y - сдвиг вдоль оси ординат;

x' - положение точки отсчета на оси абсцисс после сдвига;

y' - положение точки отсчета на оси ординат после сдвига.

Если встраивание водяного знака выполнялось в пространственной области, то, соответственно, ЦВЗ будет подвергаться преобразованиям по такому же правилу, как и все точки изображения-контейнера. В таком случае задача детектора сводится к восстановлению синхронизации, так как ЦВЗ не ухудшается, а перемещается в неизвестные точки пространственной области контейнера.

При масштабировании соответствующие координаты точек в пространственной области будут умножаться на коэффициенты масштабирования:

$$x' = a_x \times x, \quad 3$$

$$y' = a_y \times y, \quad 4$$

где a_x - коэффициент масштабирования для оси абсцисс;

a_y - коэффициент масштабирования для оси ординат.

Масштабирование приводит к потере синхронизации между ЦВЗ и детектором.

При повороте относительно начала координат для задания вращения используется угол φ. Допустим, что есть некоторый вектор r, который задает некоторую точку из пространственной области контейнера. Тогда координаты этой точкой можно описать следующей формулой:

$$x=|r|\times\cos\ \alpha\ , \qquad 5$$

$$y=|r|\times\sin\ \alpha\ , \qquad 6$$

где α - угол, описывающий положение точки в пространственной области.

При повороте контейнера на угол φ конечные координаты изображения могут быть заданы следующим образом:

$$x'=|r|\times\cos\ \alpha+\varphi\ =|r|\times\ \cos\ \alpha\ \times\cos\ \varphi\ -\sin\ \alpha\ \times\sin\ \varphi\ =$$

$$=x\times cos\ \varphi\ -y\times sin\ \varphi\ , \qquad 7)$$

$$y'=|r|\times\sin\ \alpha+\varphi\ =|r|\times\ \sin\ \alpha\ \times\cos\ \varphi\ +\cos\ \alpha\ \times\sin\ \varphi\ =$$

$$=x\times sin\ \varphi\ +y\times cos\ \varphi\ . \qquad 8)$$

После поворота контейнера ЦВЗ, как и в случае сдвига, перемещается в отсчеты пространственной области, координаты которой неизвестны детектору. Потери информации не происходит, но нарушается синхронизация детектора и водяного знака.

В связи с возможностью проведения описанных сценариев атак, для разрабатываемого алгоритма встраивания стойких ЦВЗ должны быть предъявлены следующие требования:

- устойчивость к сжатию с потерями;
- устойчивость к кадрированию контейнера;
- устойчивость к повороту контейнера.

Для того, чтобы разобраться в сложности обеспечения устойчивости алгоритма необходимо рассмотреть проблемы последствий искажений и существующие подходы противодействия.

Одним из методов противодействия геометрическим искажениям является прямой перебор. Так как при геометрических искажениях основной проблемой является не потеря информации, а рассинхронизация детектора и ЦВЗ, то ее возможным решением является поиск водяного знака при всех возможных сдвигах, коэффициентах масштабирования и углах поворота. Значительным недостатком такого подхода является вычислительная сложность. Детектор должен учитывать огромное количество геометрических конфигураций, что приводит к чрезвычайно высокой вычислительной нагрузке.

Еще один способ противостояния геометрическим атакам - это оценивание параметров преобразования и его инвертирование. Для этого некоторый шаблон синхронизации вставляется в фиксированные точки частотной области. Этот шаблон синхронизации может представлять собой набор пиков или иметь более сложную форму. Для повышения безопасности шаблон может зависеть от секретного ключа, который известен только авторизованным пользователям.

Третий способ решения проблемы геометрических искажений - использование самосинхронизирующихся водяных знаков. Один и тот же водяной знак периодически

встраивается в пространственную или частотную область, при этом период повторения ЦВЗ известен. Затем этот период оценивается детектором путем анализа пиков автокорреляции Сравнивая этот период с ожидаемым детектор может определить коэффициенты масштабирования и угол поворота, которые были применены к носителю в процессе преобразования.

С помощью найденных коэффициентов геометрические преобразования инвертируется, а исходное положение отсчетов восстанавливается.

Еще одно решение для того, чтобы справиться с проблемой геометрических преобразований - это встраивание в области, которые не зависят от геометрических преобразований.

Например, для обеспечения устойчивости к сдвигам наиболее распространенное решение состоит в встраивании ЦВЗ в коэффициенты ДПФ контейнера.

Следующий тип алгоритмов, направленных на решение задачи геометрических искажений основан на геометрической нормализации на основе признаков. Идея этого метода состоит в том, чтобы встраивать и декодировать или детектировать водяной знак, когда контейнер принимает некоторое эталонное геометрическое положение, то есть имеет некоторые эталонные значения коэффициентов масштабирование, угла поворота. Эталонное геометрическое положение должно быть принято относительно системы координат, которая известна кодеру и детектору. Для этого эталонное геометрическое положение принимается относительно каких-либо признаков контейнера. Такими признаками могут выступать углы или края, если контейнером является изображение.

Надежность этого метода зависит от стабильности признаков, используемых для нормализации изображения. Такие алгоритмы, как правило, могут быть очень чувствительны к кадрированию, так как при кадрировании опорные признаки могут быть потеряны.

Далее будут рассмотрены существующие алгоритмы встраивания стойких цифровых водяных знаков, которые основаны на некоторых из перечисленных методов противодействия геометрическим искажениям.

Алгоритмы встраивания стойких ЦВЗ, существующие на данный момент, можно условно разделить на два класса:

- алгоритмы встраивания ЦВЗ в области преобразования, инвариантного к требуемым видам искажений;

- алгоритмы, использующие "метки синхронизации".

Многие существующие алгоритмы встраивание стойких ЦВЗ обладают существенным недостатком: встраивание в частотные области изображения контейнера. Соответственно, необходимыми этапами встраивания водяного знака являются прямое и обратное ДПФ изображения-контейнера. Такой подход хоть и обеспечивает устойчивость ЦВЗ к геометрическим преобразованиям, но существенно повышает вычислительную сложность алгоритма встраивания.

При встраивании в область преобразований информация встраивается в коэффициенты преобразований контейнера.

Самое распространенное встраивание - это встраивание в частотную область контейнера. Чаще всего при этом к изображению-контейнеру применяется преобразование Фурье или косинусное преобразование.

Обычно методы встраивания ЦВЗ в области преобразований контейнера показывают более высокую стойкость к различным атакам, нежели методы встраивания в пространственную область. В частности, такие методы более устойчивы к кадрированию изображения.

Также встраивание в область преобразования показывает свою устойчивость и к другим видам геометрических преобразований, таким как сдвиг и масштабирование. Это достигается с помощью выбора области преобразований таким образом, чтобы она была инвариантной к требуемым преобразованиям контейнера.

Основными недостатками такого метода, как уже упоминалось выше, является вычислительная сложность. Кроме того, изображение-контейнер в процессе встраивания информации значительно искажается.

При таком подходе до встраивания ЦВЗ в изображение-контейнер встраиваются устойчивые к искажениям метки, которые позволяют оценить степень искажений, внесенных в контейнер при встраивании, а также компенсировать их.

Недостаток таких алгоритмов заключается в их неустойчивости к атакам "watermark template attack". При такой атаке нарушитель, не зная ключа встраивания, может обнаружить и удалить "метки синхронизации". По сути, нарушитель находит пики - "метки синхронизации" и усредняет их с соседними значениями, что делает невозможным дальнейшее обнаружение ЦВЗ.

При грамотном подходе к оценке интеллектуальной собственности и применении цифровых методов предприятия разных форм собственности получают возможность увеличивать свои финансовые ресурсы, управлять платежеспособностью, ликвидностью и соответственно получать больше прибыли. Ценность активов ИС в сравнении с материальными активами возросла по причине важности технологий и творческого труда для современной экономики.[3]

---

[1] Dyatlov S., Bulavko O., Balaovskaya A., Nikitina N., Chudaeva A. Principles of the Organization of the Global Economic System. International Journal of Environmental & Science Education (2016), Vol. 11, No. 10, 3783-3790

[2] Семенов Ю.А. IT-экономика в 2016 году и через 10 лет//Экономические стратегии. 2017. №1 (143), С. 126-135

[3] Булавко О.А., Дятлов С.А., Институционально-правовые аспекты регулирования рынка интеллектуальной собственности. // Экономика и управление собственностью. 2017. № 1. С. 55-64

INFLUENCE OF INFORMATION AND DIGITAL TECHNOLOGIES ON INTELLECTUAL PROPERTY

© 2020 Bulavko Olga Alexandrovna
Doctor of Economics, Professor
© 2020 Tuktarova Lilia Ravilievna
PhD in Economics, Associate Professor
Samara State University of Economics
E-Mail: Vikigor163@Mail.Ru

Keywords: intellectual property, information technology, digital technology, computer shorthand, digital watermarks.

The article is devoted to the consideration of aspects of the influence of information and digital technologies on issues related to copyright and intellectual property. The author considers the possibility of effective development of the economy and the spread of hypercompetitive technologies from the perspective of information-network and intellectual-psychological orientation. solvency assessment on the basis of liquidity.