МЕТОДЫ ЗАЩИТЫ АВТОРСКОГО ПРАВА НА ПРОГРАММНЫЕ ПРОДУКТЫ С ПОМОЩЬЮ ВОДЯНЫХ ЗНАКОВ И ОТПЕЧАТКОВ ПАЛЬЦЕВ

Шулицкий Д. С., Водейко А. Э.
Кафедра программного обеспечения информационных технологий, Белорусский государственный университет информатики и радиоэлектороники
Минск, Республика Беларусь
E-mail: dmitrii.shulitskii@gmail.com, avodeikoga@gmail.com

Защита цифровых работ от нелегального использования и распространения является сложной задачей в информационном обществе. Полное предотвращение незаконного использования работ недостижимо за разумную цену. Большинство схем защиты авторского права отпугивают людей от нелегального использования и распространения цифрового контента тем, что позволяют обнаружить незаконное использование. Для этого в оригинальную работу добавляют идентификационную информацию с помощью техники водяных знаков или отпечатков пальцев.

Введение

Цифровой водяной знак – это информация, внедрённая в цифровую работу, позволяющая автору доказать своё авторство. В самом простом случае, водяной знак представляет копирайт-строку. Цифровой отпечаток пальца – водяной знак, содержащий информацию не только о правообладателе, но и о субъекте, которому предоставлено право использования данного экземпляра объекта интеллектуальной собственности.

Технология цифровых водяных знаков давно используется для защиты прав интеллектуальной собственности на графические изображения, видеозаписи, фонограммы. В последние годы происходят попытки использования цифровых водяных знаков для защиты прав собственности на программное обеспечение.

I. Математическая модель

Рассмотрим математическую запись для формального описания наиболее важных понятий, касающихся внедрения водяных знаков в программное обеспечение. Пусть O – компьютерная программа, допускающая выполнение с ней различных манипуляций, S – текущее состояние вычислительной системы. S[O, ...] означает состояние вычислительной системы S, в котором существует только одна копия программы O. S'[O, O, ...] – состояние системы S', в котором существует 2 идентичные копии O. Пусть ω -– водяной знак, а E -– функция, описывающая внедрение водяного знака в программу, тогда

$$E(S,\ \omega) = S_\omega,$$

где S[O, ...] – состояние вычислительной среды, содержащий объект O, в который внедряется водяной знак, ω – желаемый водяной знак. Обозначим как $S_\omega = [O_\omega,\ ...]$ состояние вычислительной системы, содержащей объект с внедрённым водяным знаком. Соответствующая E Функция извлечения водяного знака R имеет следующее сойство:

$$\forall S_\omega : R(S_\omega) = \omega.$$

Ложное распознование водяного знака нежелательно, поэтому:

$$\forall S_\omega, \omega' \neq \omega : R(S_\omega) \neq \omega'.$$

Конкретный алгоритм водяного знака состоит из функции внедрения и функции распознавания водяного знака. [1]

II. Виды водяных знаков в программном обеспечении

Если функция извлечения водяного знака общедоступна, водяной знак называют видимым. Если эта функция доступна только лицу, внедрившему водяной знак, его называют невидимым.

Водяные знаки в программном обеспечении можно разделить на водяные знаки данных и водяные знаки кода. Водяные знаки данных размещаются в структурах данных программы, которые не используются. Водяные знаки кода внедряются при помощи манипуляций с инструкциями микропроцессора.

Статические водяные знаки извлекаются непосредственно из файла программы. Для извлечения динамического водяного знака необходим запуск программы и получение результата её работы. [2]

III. Отпечатки пальцев в программном обеспечении

Цифровые отпечатки пальцев, в отличие от обычных водяных знаков, содержат не только информацию об авторе программы, но и информацию о покупателе программы. Это позволяют различать копии одной и той же программы. При продаже очередной копии программы, формируется содержимое отпечатка пальца. Далее

эта информация зашифровывается при помощи приватного ключа разработчика. Это позволяет доказать, что информация была зашифрована конкретным лицом. Затем отпечаток пальца внедряется в программное обеспечение. Отпечатки пальца позволяют обнаруживать источники нелегального распространения программы, так как не составляет труда определить покупателя конкретной копии программы.

К цифровым отпечаткам пальцев предъявляется дополнительное требование по сравнению с водяными знаками: даже если атакующий имеет доступ к некоторому количеству копий программы, он не должен иметь возможность прочесть, повредить или удалить водяной знак на основе информации, полученной путём сравнения копий.

IV. Водяные знаки на основе инвариантных статистических характеристиках контейнера

Защищаемый водяным знаком объект состоит из множества атомарных элементов. Для растовых изображений такими элементами являются пиксели, для программ – низкоуровневые инструкции. Множество элементов, составляющих объект, обладают некоторыми статистическими характеристиками. Некоторые характеристики инвариантны, то есть не зависят от содержания объекта. Такие характеристики можно использовать для внедрения особого вида водяного знака, называемого признаком авторства. Признак авторства позволяет ответить на вопрос «Является ли рассматриваемый субъект автором данного объекта?».

Рассмотрим величину $S = a_i - b_i$, равную разности яркости двух случайно выбранных пикселей изображения. Эксперименты показывают, что для достаточно большой выборки пар пикселей значение выражения:

$$S_n = \sum_{i=1}^{n}(a_i - b_i)$$

будет очень близким к нулю. Данная характеристика не зависит от содержимого изображения. Авторы «Pathwork» предлагают следующий алгоритм внедрения признака:

1. При помощи генератора псевдослучайных чисел выбираются две точки изображения со значениями яркости (a_i, b_i);
2. значение яркости a_i увеличивается на величину δ;
3. значение яркости b_i уменьшается на величину δ;
4. шаги 1-3 повторяются n раз.

После выполнения модификации, новое значение S'_n увеличится на величину $2\delta n$. Величина δ выбирается такой, чтобы модификации не были различимы человеческим глазом. Для того, чтобы воспрозвести псевдослучайную последовательность координат пикселей, необходимо знать начальное состояние генератора псевдослучайных чисел. Оно и является ключом внедрения признака авторства и держится в секрете. Субъект, претендующий на авторство объекта, предоставляет начальное состояние генератора псевдослучайных чисел, на основе которого генерируются пары пикселей. Авторство подтверждается, если значение характеристики S_n для данного набора пикселей значительно отличается от нуля.

V. Слепая проверка водяных знаков

Концептуальной проблемой обычных водяных знаков является то, что демонстрация присутствия водяного знака как свидетельства раскрывает чувствительную информацию, которая может быть использована для удаления водяного знака. Желательно убедить верификатора в том, что водяной знак присутствует и не раскрыть ему информацию, которая может помочь удалить водяной знак.

Одим из подходов к решению данной проблемы является использование слепой проверки водяных знаков. Слепые протоколы позволяют убедить верификатора, что правообладатель знает секретное значение, и верификатор не узнаёт ничего нового о секретных данных правообладателя.

Например, правообладатель может создать настоящий водяной знак и спрятать его в большом списке поддельных водяных знаков. Затем он предлагает верификатору обнаружить все водяные знаки и доказывает, что, по крайней мере, один из водяных знаков является настоящим, не раскрывая, какой именно. Безопасность данного метода основана на том, что количество водяных знаков в списке должно быть на столько большим, что невозможно удалить их все без серьёзного ухудшения стего-данных. [3]

1. Криптография, стеганография и охрана авторского права / В.Н.Ярмолик, С.С. Портянко, С.В.Ярмолик / Издательский центр БГУ — Минск, 2007. — С. 195–211
2. Watermarking, Tamper-Proofing and Obfuscation – Tools for Software Protection / C. Collberg, C. Thomborson – Department of Computer Science University of Arizone, 2000. – P. 7-11.
3. Zero-Knowledge Watermark Detection and Proof of Ownership / A. Adelsbach, A. Sadeghi – LNCS, 2001. – P. 273-288.