Розділ 26

СУЧАСНІ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ У ПРАВОВІЙ СФЕРІ

КОЗИН А. Б.

Национальный университет «Одесская юридическая академия»,
и. о. заведующего кафедрой информационных технологий,
кандидат физико-математических наук, доцент

АЛГОРИТМ ЦИФРОВОЙ СТЕГАНОГРАФИИ С ЗАЩИТОЙ ДАННЫХ

При решении задач защиты информации сегодня, выделяют два основных направления, такие как криптография и стеганография. Целью криптографии является сокрытие секретного сообщения за счет его шифрования. В отличие от шифрования, стеганография скрывает сам факт существования тайного сообщения (Грибунин В. Г. Цифровая стеганография / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев. — М.: СОЛОН-Пресс, 2002. — 272 с.).

Одним из важных факторов, послуживших развитию метода стеганографии явились ограничения на использовании криптографии, которые имеют место во многих странах мира.

Так, например, существуют требования предоставления ключей используемых систем шифрования государству и пр. Кроме того, лицензирование криптографических систем так же, как и их регистрация являются во многих странах обязательными, невзирая на их принадлежность к программным или аппаратным средствам. Данные ограничения не касаются стеганографии и поэтому, не ограничивают ее применение.

Для графических изображений, с точки зрения защиты авторского права, необходимо реализовать публикацию информации об авторе. Это может быть текст или графическая информация, которая однозначно ассоциируется с личностью автора — правообладателя. Такие «знаки» служат ссылкой на источник, предоставивший конкретный графический файл. Таким образом, разработка новых методов стеганографической защиты представляет сегодня актуальную задачу, позволяющую подтвердить права разработчика на данную цифровую информацию.

Существующие методы, которые решают задачу авторского права путем внедрения цифровых водяных знаков (ЦВЗ), можно разделить на две группы: группа методов, которые внедряют ЦВЗ в пространственную область, а также изображения и методы, которые внедряют ЦВЗ в частотную область (Конахович Г. Ф., Пузыренко А. Ю. Компьютерная стеганография. Теория и практика. — К.: «МК-Пресс », 2006. — 288 с.).

Методы первой группы встраивают информацию непосредственно в исходную область изображения, что делает их неустойчивыми к многим искажениям. Наиболее стойкие, к различного рода искажениям, являются методы второй группы.

На сегодняшний день существуют различные способы представления изображения в частотной области. Наиболее часто используемые следующие: дискретное преобразование Фурье (ДПФ), дискретное косинус-преобразование, или вейвлет-преобразование.

В докладе рассматривается стеганографический алгоритм, который обеспечивает скрытость дополнительной информации благодаря ее внедрению в частотные коэффициенты матрицы цифрового изображения (контейнера). Для перехода в частотную область используется дискретное преобразование Фурье.

В качестве исходной матрицы контейнера, рассматриваются произвольные данные, имеющие цифровой формат, такие как цифровые изображения, аудио, видео последовательности и т.п.

Предлагается применять стеганопреобразование (СП) для коэффициентов, используя ДПФ, предварительно разбивая исходное изображение на блоки размером 2*2. Предобработкой блоков матрицы контейнера служит перевод ее из пространственной области в область преобразования, т.е. в частотную область.

Предлагается использовать ДПФ для блоков разбиения 2*2 в виде:

$$F(u,v)=\frac{1}{L}\sum_{x=0}^{L-1}\sum_{y=0}^{L-1}f(x,y)e^{-j2\pi(\frac{ux}{L}+\frac{vy}{L})}, \text{ где } u,v=\overline{0,L-1};$$

$$f(x,y)=\frac{1}{L}\sum_{u=0}^{L-1}\sum_{v=0}^{L-1}F(u,v)e^{j2\pi(\frac{ux}{L}+\frac{vy}{L})}, \text{ где } u,v=\overline{0,L-1}.$$

Здесь обозначено: f(x,y) — элемент блока пространственной области матрицы, F(u,v) — элемент блока частотной области матрицы, L — размер блока.

Особенности машинной арифметики накладывают свое влияние на точность вычислений, производимых в системах с плавающей точкой. Нельзя не учитывать тот факт, что вычисления, связанные с переходом в область преобразования цифровой информации, вносят дополнительную погрешность в процесс, связанный с возвращением в пространственную область, что обязательно происходит при применении

СП (Костырка О. В. Анализ преимуществ пространственной области цифрового изображения-контейнера для стеганопреобразования / О. В. Костырка — IMMM, 2013, Том 3, № 3. — С. 275–282.).

В связи с этим в данном алгоритме предусмотрена минимизация дробных вычислений при помощи коэффициентов ДПФ.

Таким образом, совершенствуя существующие методы стеганографии, мы создаем новые, все более эффективные программные способы защиты интеллектуальной собственности цифровых данных.

Разработанный алгоритм с переходом из пространственной области в частотную и обратно, может рассматриваться, как устойчивый стеганографический алгоритм защиты цифровых данных. Внедренная информация подтвердит авторство цифрового изображения или права собственности на это защищаемое изображение.

Одним из эффективных средств защиты авторского права цифровых данных в нашей стране, на наш взгляд, будет являться использование комплексного подхода, который включает правовые методы, основанные на новых эффективных программно-технических средствах защиты. К этим средствам мы и относим данный алгоритм.

ЯКУТКО В. Ф.

Национальный университет «Одесская юридическая академия»,
доцент кафедры информационных технологий,
кандидат технических наук, доцент

СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ В ЮРИСПРУДЕНЦИИ

Информационные технологии в юридической деятельности призваны решать задачи, обусловленные спецификой работы юриста. Такими задачами в первую очередь являются: поиск, обработка и анализ правовой информации.

Интеграция информационных технологий в юридическую сферу должна обеспечить значительное снижение временных затрат на принятие решения в рамках конкретной правовой ситуации, улучшить качество и проработанность принимаемого решения.

Для реализации своей деятельности юристу необходимо не только правовая информация, но и различные статистические данные, аналитические материалы и общая информация в различных сферах человеческой деятельности. Эти данные юристы, в большинстве случаев, получают из справочных правовых систем (СПС), специализированных баз данных, а также сети Интернет. В настоящее время в Украине

