УДК 347.78:004.9

Д.М. Романенко, Н.П. Шутько, Вахаб Алаа
Белорусский государственный технологический университет

ЗАЩИТА АВТОРСКИХ ПРАВ НА ЭЛЕКТРОННЫЕ ИЗДАНИЯ

Защита авторских прав становится менее надежной по мере того, как компьютерные сети все чаще используются для передачи электронных документов. Рассылка документов по сети предполагает, что их может получить большое число адресатов. Это также дает возможность недобросовестным пользователям адаптировать или перерабатывать информацию с целью извлечения коммерческой выгоды. В современном мире угроза информационного пиратства стала реальностью. Одним из направлений решения указанной проблемы является применение методов современной стеганографии. Стеганография это искусство передачи скрытого сообщения. Причем, в отличие от криптографии, скрывается сам факт передачи информации.

Основной частью большинства электронных изданий являются текстовые фрагменты и изображения. Некоторые издания вообще целиком текстовые. В то же самое время для электронных изданий нет серьезных причин для ограничения количества иллюстративного материала, т. е. следует использовать такое количество иллюстраций, которое требуется для наилучшего восприятия и понимания материала.

Неотъемлемой частью многих изданий также является звуковое сопровождение. Звуковое сопровождение может представлять собой авторский текст или ремарки, шумовые эффекты, иллюстрирующие происходящие события и делающие их описание более реалистичным. Скорость восприятия человеком звуковой информации имеет тот же порядок величин, что и для текста. Электронные издания также могут наполняться видеоконтентом.

Таким образом защита авторских прав на электронные издания сводится к нескольким этапам:

1. Внедрение секретной авторской информации в различные элементы (текст, изображения, аудио- и видеоконтент) электронных изданий. Предполагается, что злоумышленник, желающий воспользоваться чужими материалами, не сможет может увидеть (обнаружить) внедренные авторские данные.

2. Извлечение авторской информации для подтверждения авторства. Причем важно, чтобы данная информация извлекалась, даже если злоумышленник воспользовался лишь фрагментами электронного издания.

3. Важной стороной решения данной проблемы является нормативная база, в соответствии с которой и будет осуществляться подтверждение

авторства, а также наличие единого центра, выполняющего внедрение авторской информации, причем внедрение должно быть возможно только при отсутствии в объекте какой-либо информации, даже остаточной, указывающей на другого автора.

Отметим, что в рамках данного исследования будут затронуты лишь вопросы скрытного осаждения и извлечения авторской информации, а нормативно-правовые и технические вопросы не рассматривались.

Для защиты текстовой информации электронных изданий были предложены новые синтаксические методы текстовой стеганографии, основанные на использовании пространственных или пространственно-геометрических (таких, как апрош) и цветовых параметров символов текста, формируемого растром, для размещения тайной (авторской) информации. Ввиду того, что электронные документы выводятся на экран монитора, цвет символов в текстовой части электронного издания представлены в цветовой модели RGB. В ходе исследований различных методов текстовой стеганографии было предложено изменять значения трех цветовых каналов – красного, зеленого и синего. Необходимо отметить, что скрытие данных в случае встраивания секретной информации в электронный документ производится не только в обычных, но и в специальных (мягкий перенос, разрыв строки и др.) символах и пробелах.

Таким образом, основной постулат рассматриваемого метода можно сформулировать так: цвет пикселей, формирующих символы текста-контейнера, можно изменить так, что это остается незаметным для других лиц в силу специфики человеческого зрения [1]. Кстати, этот постулат будет справедлив и для методов, направленных на модификацию пространственно-геометрических параметров текста.

Другой метод встраивания стегосообщения в текстовый контейнер основан на модификации базового (устанавливаемого текстовым процессором по умолчанию) значения апроша, его изменением от базового до некоторого максимального (или минимального), которое зрительно не должно отличаться от стандартного. Такое изменение производится дискретно, каждому значению шага присваивается определенный бит или определенная комбинация бит. На рисунке 1 приведен пример осаждения тайной информации на основе данного метода. Как видно из примера, использование различного значения (лучше и положительного, и отрицательного) апроша от 0,1 до примерно 1 пт без пристального анализа заметить визуально невозможно (верхние строки).

Наиболее известным способом внедрения секретной информации в растровые изображения является метод LSB (Least Significant Bit), главным недостатком которого является низкая стойкость к стегоанализу.

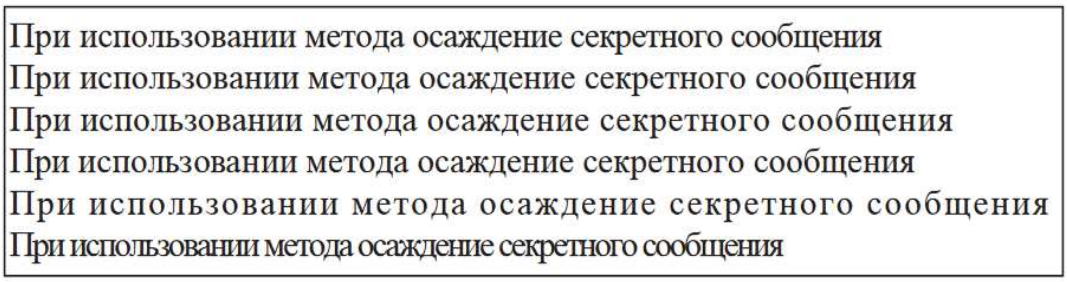

Рисунок 1 – Пример использования различного апроша

В рамках представленного исследования предлагается модификация техники осаждения секретной информации в растровые изображения методом LSB с целью минимизации отклонения цветовых значений модифицированных бит от начальных значений, что позволит достичь большей стегостойкости метода осаждения [2]. Суть модификации заключается в следующем. На начальном этапе с помощью секретного ключа определяется выборка бит изображения, в которые будет осаждаться секретная информация. Длина выборки равна количеству символов в применяемом алфавите. Количество выборок будет равно количеству осаждаемых символов. В выборку попадают только те биты, младший разряд которых соответствует требованиям ключа, например, предполагается увеличивать младшие разряды, равные 7, на 1. В таком случае в области осаждения должны быть изначально изменены младшие разряды бит, равные 8 на ближайшее значение, например, 9. В выборке на 1 увеличивается тот бит, абсолютный номер которого соответствует номеру осаждаемого символа в алфавите, например, при осаждении буквы «*Н*» из латинского алфавита (26 символов) необходимо на единицу изменить 8-ой бит в выборке.

Предложенный метод осаждения требует использования составного ключа, состоящего как минимум из следующих параметров: используемый канал (красный, зеленый, синий) или их комбинация; адрес начального бита выборки; метод формирования выборки; младший разряд, подлежащий модификации на 1 при осаждении; младший разряд, подлежащий изменению в исходной выборке (маскирующийся разряд). В целом можно отметить, что предложенный метод позволяет осаждать секретную авторскую информацию, и при этом начальные значения пикселей будет изменяться только лишь на 1, что должно повысить стегостойкость контейнера.

Для защиты аудиоконтента предлагается использовать следующую идею: незначительные изменения битрейта должны оказать незначительное воздействие на звуковые данные, что обычный человек при прослушивании аудио- контента электронного издания не заметит каких-либо

искажений, т. е. стегоконтейнер останется нераскрытым. Распределение информации по случайным фреймам поможет скрыть факт наличия осажденной информации. Многократное осаждение информации, в том числе и с дополнительными (маскирующими) данными поможет решить проблемы повреждения данных при передаче и намеренного изменения или удаления осажденных данных.

Таким образом в рамках исследования авторами предложены различные стеганографические методы, позволяющие внедрять авторскую информацию практически в любую часть электронного издания. Комплексное же их использование, а также развитие нормативно-правовой базы, касающейся процедуры установления авторства, позволит в некоторой степени решить одну из сложнейших проблем современного общества – информационного пиратства.

Список использованных источников

1. Urbanovich, N. The use of steganographic techniques for protection of intellectual property rights / N. Urbanovich, V. Plaskovitsky // Electrical Review (Przeglad elektrotechniczny). – 2012. – № 11b. – S. 342–344.

2. Романенко, Д.М. Методы цифровой стеганографии на основе модификации цветовых параметров изображения / Д. М. Романенко, Алаа Вахаб // Труды БГТУ. – 2018. – № 1 (206). – С. 94–99.

УДК 336.227

Е.С. Русак
Академия управления при Президенте Республики Беларусь

ФОРМИРОВАНИЕ ЕДИНОЙ НАЛОГОВОЙ ПОЛИТИКИ НА ТЕРРИТОРИИ ЕВРАЗИЙСКОГО ЭКОНОМИЧЕСКОГО СОЮЗА

Межгосударственное сотрудничество в рамках Евразийского экономического союза вызывает необходимость проведения скоординированной, согласованной или единой промышленной политики в отраслях экономики, а также гармонизации налогового законодательства как основополагающего инструмента его функционирования и развития.

В Договоре о Евразийском экономическом союзе в разделе XVII «Налоги и налогообложение» отмечается, что «Государства-члены определяют направления, а также формы и порядок осуществления гармонизации законодательства в отношении налогов, которые оказывают