В. Г. Иваненко, Я. Р. Шабаева

ЗАЩИТА ИЗОБРАЖЕНИЙ ОТ МОДИФИКАЦИИ С ПОМОЩЬЮ ЗАМЕНЫ НАИМЕНЕЕ ЗНАЧАЩИХ БИТ

В настоящее время многие предприятия и организации активно переходят на электронный документооборот. При этом данные, которые раньше хранились на полках в бумажном виде, переносятся в базы данных и в электронные архивы. Одним из наиболее эффективных способов исключения несанкционированной модификации документа может служить встраивание в него так называемых цифровых водяных знаков (ЦВЗ).

Цифровой водяной знак — это специальная метка, встраиваемая в цифровое изображение (называемое контейнером) с целью защиты авторских прав или подтверждения целостности документа [1]. ЦВЗ могут быть трех типов: робастные, хрупкие и полухрупкие. Под робастностью понимается устойчивость ЦВЗ к различного рода воздействиям на него. Хрупкие ЦВЗ разрушаются при незначительной модификации заполненного контейнера. Они эффективны при решении задачи контроля целостности и защиты от фальсификации. При этом следует встраивать в документ хрупкий ЦВЗ, и, если документ подвергся модификации, водяной знак разрушится, что и будет подтверждением нарушения целостности. Еще одна причина встраивать ЦВЗ для проверки целостности — это износ носителей данных. Каким бы ни был архивный носитель, целостность хранимых на нем данных со временем может подвергнуться изменению, и при переносе файлов могут возникнуть ошибки. Компоненты DVD-диска постепенно разлагаются, ленты и диски размагничиваются, а флэш-память теряет заряд. Чтобы заметить подобные повреждения, нужно проверять специфические области в изображении в масштабе 100 %, и даже тогда на отпечатке их будет легко заметить. Это не применимо для архива с тысячами документов, когда обнаружить все повреждения при очень больших объемах данных нереально. Далее повреждения изображений распространяются на все последующие резервные копии и могут оставаться незамеченными до тех пор, пока их не попытаются напечатать спустя некоторое время. Использование методов хранения, которые контролируют целостность данных, является единственным способом систематически обнаруживать подобные проблемы прежде, чем они необратимо изменят целостность архива.

Существует множество программных методов, которые проверяют целостность файловой системы, например, методы вычисления контрольной суммы, с помощью различных алгоритмов хеширования. Но для проверки архива с документами эти вычисления слишком громоздки и не оправдывают затрат, поэтому целесообразно для проверки их целостности использовать ЦВЗ.

Алгоритмы внедрения ЦВЗ характеризуются, главным образом, такими показателями, как количество информации, которое можно внедрить в изображение, отсутствие появления признаков внедрения в исходном изображении и др. Естественно, что эти критерии конкурируют друг с другом, т. е. достижение эффективности по одному из них приводит к ухудшению по другим.

Внедрение скрытого сообщения в изображение непосредственно связано со свойством избыточности в изображениях. В изображениях присутствует информация (шум), непосредственно не влияющая на восприятие человеком картинки. На замене части такого шума в изображении на внедряемое сообщение и основаны алгоритмы ЦВЗ.

Метод замены наименьшего значащего бита (НЗБ, или LSB — Least Significant Bit) — один из наиболее часто используемых способов стеганографического сокрытия [2]. Младшие биты оцифрованных изображений могут иметь различное распределение в зависимости от применявшихся параметров преобразования, от дополнительной компьютерной обработки и прочих факторов. Эта особенность делает метод наименее значащих битов наиболее защищенным от обнаружения вложения.

Его достоинствами также являются простота реализации, неизменность размера файла-контейнера, возможность скрывать в относительно небольших файлах большие объемы информации. Кроме того, доказано, что данный метод позволяет получить наименьший уровень визуальных искажений [3].

Сущность этого метода отображена в самом его названии и заключается в замене наименее значащих бит контейнера — файла, в который будет встраиваться скрытая информация.

Известно, что человек воспринимает не всю информацию, заложенную в изображении, и если заменить у цветовых компонентов пикселя менее значащие биты на биты скрываемого сообщения, то выявить человек этого на глаз не сможет. Проводя последовательно подобную замену, начиная с заранее оговоренного пикселя, мы можем внедрить сообщение в файл-изображение. В качестве преимуществ этого метода сокрытия можно выделить его простоту реализации и большой объем данных, встраиваемый в передаваемый файл. Простой в реализации метод замены наименее значащего бита эффективен при решении задачи контроля целостности и защиты от фальсификации, при этом не требуется больших вычислительных ресурсов.

Таким образом, внедрение ЦВЗ методом замены наименее значащего бита решает проблему проверки целостности электронных документов в архиве, а восприимчивость этого метода к любым искажениям в этом применении является его главным достоинством.

СПИСОК ЛИТЕРАТУРЫ:

1. *Грибунин В. Г., Оков И. Н., Туринцев И. В.* Цифровая стеганография. М.: Солон-Пресс, 2002. С. 6–8.
2. *Кованович Г. Ф., Пузыренко А. Ю.* Компьютерная стеганография. Теория и практика. К.: МК-Пресс, 2006. С. 76–89.
3. *Вовк О. О., Астраханцев А. А., Дорожан А. В.* Исследование стойкости методов скрытия информации в неподвижных изображениях // Радиоэлектронные и компьютерные системы 2012, № 2 (54). С. 104-105.

К. В. Иванов

ПРОБЛЕМНО-ОРИЕНТИРОВАННАЯ МЕТОДИКА ЗАЩИТЫ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ УЧЕТА И КОНТРОЛЯ ЯДЕРНЫХ МАТЕРИАЛОВ

Ввиду особенностей информации, обрабатываемой в автоматизированных системах учета и контроля ядерных материалов (АСУиК ЯМ), одним из ключевых требований, предъявляемых к системам данного класса, является требование обеспечения высокого уровня защиты информации от несанкционированного доступа. Наиболее сложные задачи, связанные с обеспечением информационной безопасности, возникают при создании систем, допускающих одновременную работу пользователей, обладающих различными правами на доступ к информации разных уровней конфиденциальности.

В работе рассмотрена проблемно-ориентированная методика построения систем защиты информации от несанкционированного доступа в АСУиК ЯМ, допускающих одновременную работу пользователей, обладающих различными правами на доступ к информации разных уровней конфиденциальности:

– не требующая сертификации средств защиты информации ОС и СУБД;

– предусматривающая модификацию программного обеспечения в интересах конкретного предприятия без модификации комплекса средств защиты информации.