СРАВНИТЕЛЬНЫЙ АНАЛИЗ УСТОЙЧИВОСТИ К АТАКАМ СТЕГАНОГРАФИЧЕСКИХ МЕТОДОВ СКРЫТИЯ ИНФОРМАЦИИ

Вовк О. О., Астраханцев А. А.
Харьковский национальный университет радиоэлектроники, Украина
E–mail: olesia.vovk@gmail.com

Аннотация — Рассмотрены влияния различных видов атак на изображения с встроенным ЦВЗ (цифровым водяным знаком). Произведен сравнительный анализ устойчивости к искажениям наиболее популярных методов встраивания ЦВЗ в пространственной и частотной областях изображения.

1. Введение

Отличительной чертой стеганографии является скрытие самого наличия стегоканала. Но полноправный пользователь, не зная о наличии встроенных данных, может совершать атаки на ЦВЗ, не осознавая этого.

В связи с этим, целью работы является рассмотрение различных видов атак на изображение со встроенным ЦВЗ. При этом необходимо выполнить сравнительный анализ различных алгоритмов встраивания, определить их наибольшую устойчивость и невозможность применения некоторых модификаций над изображением с вложенными данными. В этом случае файл, заполненный встраиваемой информацией, должен удовлетворять требованию визуальной незаметности.

2. Основная часть

На данный момент создано множество алгоритмов по встраиванию скрытых сообщений в графические файлы. Проведя небольшой мониторинг, мы определили наиболее актуальные и перспективные из них для более детального рассмотрения. В качестве исследуемых были выбраны по два алгоритма, использующие для встраивания пространственную и частотную область изображений, а именно: метод Куттера– Джордана–Боссена (КДБ), метод Дармстедтера– Делейгла–Квисквотера–Макка (ДДКМ), метод Коха–Жао (КЖ), метод Бенгама–Мемона–Ео–Юнга (БМЕЮ).

Согласно различным классификациям существует несколько типов атак, направленных на системы с встроенным ЦВЗ. В работе в первую очередь мы будем рассматривать геометрические атаки, так как именно их чаще всего применяют к изображениям среднестатистические пользователи исходя из личных целей. Геометрические атаки математически моделируются как аффинные преобразования неизвестные детектору. Атаки были реализованы с помощью программных средств *Adobe Photoshop и Microsoft Office Picture Manager*.

Результаты геометрических атак на правильность срабатывания детектора ЦВЗ приведены в Таблице 1 (в % указана максимально допустимая величина изменений).

После анализа изображений, можно сделать вывод, что атаки против стегодетектора, основанные на масштабировании, повороте и отсечении изображения, приводят к несрабатыванию детектора. Ни один из исследуемых методов не проявил к ним устойчивости.

Таблица 1

Виды геом. атак	В простр. обл.		В частот. обл.	
	КДБ	ДДКМ	КЖ	БМЕЮ
1. Масштаб.	–	–	–	–
3. Повороты	–	–	–	–
4. Отсечение	–	–	–	–
6. Яркость	17%	5%	18%	15%
7. Контраст.	52%	–	55%	5%

Также в работе было исследовано влияние атак против встроенного сообщения посредством переформатирования и сжатия изображения с вложенным ЦВЗ (Таблица 2).

Таблица 2

Виды геом. атак	В простр. обл.		В частот. обл.	
	КДБ	ДДКМ	КЖ	БМЕЮ
Переформат./ сжатие	640×640			
bmp–png	+	+	+	+
bmp–tiff	+	+	+	+
bmp–jpeg(rgb)	–	–	+	+
bmp–jpeg (Ycbcr)	–	–	–	–
bmp–jpeg (CMYK)	+	–	+	+

3. Заключение

Таким образом, был сделан вывод, что метод КДБ показал наивысший уровень надежности и устойчивости к атакам. В то время как блочный метод ДДКМ позволяет достичь компромисса между стойкостью стеганосистемы к искажениям, качеством встраивания и вычислительной сложностью алгоритма.

Если сравнивать методы скрытия в БМЕЮ превосходит метод КЖ по скрытности, за счет возможности отобрать только те блоки изображения, встраивание в которые наименее заметно. Однако, пропускная способность и устойчивость к атакам лучше у метода КЖ.

Методы, которые используют для встраивания частотную область, являются более стойкими к различным искажениям, в том числе и компрессии, чем пространственные методы.

COMPARATIVE ANALYSIS OF HIDING INFORMATION STABILITY TO ATTACKS FOR STEGANOGRAPHIC METHODS

Vovk O.O., Astrahancev A.A.
Kharkiv National University of Radioelectronics, Ukraine

Abstract — The influence of different types of attacks on images embedded with DW (digital watermark) was considered. A comparative analysis of stability to distortion of the most popular methods of embedding DW in a spatial and frequency domain image was done.