DETERMINATION OF LEVEL OF STEADINESS AGAINST DATA ENCAPSULATION STEGANOGRAPHIC METHODS ATTACKS

Vovk O.O., Astrakhantsev A.A.
Kharkiv National University of Radioelecteonics
14, Lenin Ave., Kharkiv, 61171, Ukraine
Ph.: (+38 093) 5476491, e–mail: olesia.vovk@gmail.com

Abstract — The influence of different types of attacks against the images embedded with DW (digital watermark) was considered. The comparative analysis of stability to distortion of the most popular methods of embedding DW in spatial and frequency domain images and using wavelet transform was carried out.

ОПРЕДЕЛЕНИЕ УРОВНЯ СТОЙКОСТИ К АТАКАМ СТЕГАНОГРАФИЧЕСКИХ МЕТОДОВ СКРЫТИЯ ИНФОРМАЦИИ

Вовк О. О., Астраханцев А. А.
Харьковский национальный университет радиоэлектроники
пр. Ленина 14, Харьков, 61171, Украина
тел.: (+38 093) 5476491, 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, а также в области вейвлет-преобразования.

I. Введение

Отличительной чертой стеганографии является постановка основной задачи — скрытие самого наличия стегоканала. Но в случае злоумышленных действий нарушитель может предполагать его наличие и применять к изображению различные атаки с целью разрушения или удаления ЦВЗ. В то же время, полноправный пользователь, не зная о наличии встроенных данных, также может совершать атаки на ЦВЗ, не осознавая этого. С помощью распространенных на сегодняшний день операций над изображением довольно легко можно сделать так, что детектирование ЦВЗ станет не возможным.

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

II. 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, — это метод Куттера-Джордана-Боссена (КДБ), метод Дармстедтера-Делейгла-Квисквотера-Макка (ДДКМ), метод Кохa-Жао (КЖ), метод Бенгама-Мемона-Ео-Юнга (БМЕЮ). А также, метод встраивания в область вейвлет-преобразования (ДВП).

Согласно различным классификациям существует несколько типов атак направленных на системы со встроенным ЦВЗ. В работе в первую очередь мы будем рассматривать геометрические атаки, т.к. именно их чаще всего применяют к изображениям среднестатистические пользователи преследуя личные цели. Геометрические атаки математически моделируются как аффинные преобразования неизвестные детектору. Они приводят к потере синхронизации в детекторе, при этом водяной знак в изображении остается, но теряется возможность правильного его детектирования. Атаки были реализованы с помощью программных средств Adobe Photoshop и Microsoft Office Picture Manager.

Результаты геометрических влияний на способность правильно детектировать ЦВЗ приведены в Таблице 1, в % указана максимально допустимая величина изменений.

Табл. 1.
Table 1.

Виды геомет. атак	В простр. обл.		В частот. обл.		В обл. преобр.
	КДБ	ДДКМ	КЖ	КДБ	ДВП
1. Масштаб. (рис. 1, г)	–	–	–	–	–
2. Изменение пропорций	17%	–	1%	–	–
3. Повороты (рис. 1, д)	–	–	–	–	+
4. Отсечение (рис. 1, е)	–	–	–	–	+
6. Яркость (рис. 1, в)	17%	5%	18%	15%	20%
7. Контраст. (рис. 1, б)	52%	–	55%	5%	60%

После анализа изображений (рис. 1, а), сделаем вывод, что атаки против стегодетектора основанные на масштабировании, повороте и отсечении изображения (рис. 1 г, д, е) приводят к несрабатыванию детектора. Ни один из используемых методов не проявил к ним устойчивости.

Результаты влияния атак против встроенного сообщения и против стегодетектора показаны на рис. 1.

2013 23rd Int. Crimean Conference "Microwave & Telecommunication Technology" (CriMiCo'2013). 9—13 September, Sevastopol, Crimea, Ukraine
 ISBN: 978-966-335-395-1. IEEE Catalog Number: CFP13788

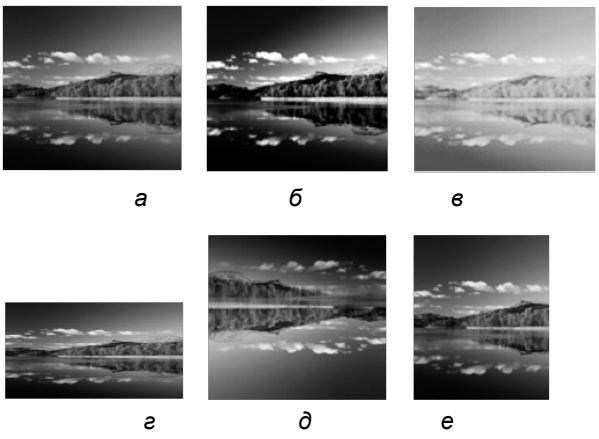

Рис. 1. Реализация атак на встроенное сообщение и стегодетектор (а — исходное изображение, б — изменение контрастности (50%), в — изменение яркости (20%), г — масштабирование, д — поворот, е — отсечение).

Fig. 1. Implementation of attacks against embedded messages and a stegodetecor (а — original image, б — the contrast changes (50%), в — the brightness changes (20%), г — zoom, д — rotation, е — clipping)

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

III. Заключение

Таким образом, был сделан вывод, что метод Куттера-Джордана-Боссена показал наивысший уровень надежности и устройчивости к атакам. В то время как блочний метод Дармстедтера-Делейгла-Квисквотера-Макка позволяет достичь компромиса между стойкостью стеганосистемы к искажениям, качеством встраивания и, конечно же, вычислительной сложностью алгоритма.

Если сравнивать методы скрытия в частотной области, то метод Бенгама-Мемона-Ео-Юнга значительно преобладает над методом Коха-Жао за счет возможности отобрать только те блоки изображения, встраивание в которые наименее заметно. Но пропускная способность и устойчивость к атакам остаются преимуществом стеганосистем, построенных на основе метода Коха-Жао.

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

Отдельно хотелось бы сказать про встраивание в область преобразования. Исследования показали, что применение вейвлет-преобразования для встраивания скрытой информации является наиболее эффективным и целесообразным при присутствии активного нарушителя, даже в лице законного владельца. Метод оказался наиболее стойким к геометрическим атакам, а также показал отличные характеристики при сжатии изображений. Единственным недостатком такого преобразования является небольшая пропускная способность, обоснованная строгими требованиями к субполосе, в которую происходит встраивание. Т.к. шум изображения должен быть примерно равен шуму обработки, этому требованию не соответствуют высокочастотные и низкочастотные субполосы. Таким образом, пропускная способность ограничена возможностью использования только среднечастотных полос.

IV. References

[1] Gribunin V.G., Okov I.N., Turintsev I.V. *Tsifrovaya steganografiya* [Digital steganography]. Moscow, Solon-Press, 2002. 272 p.

[2] Konakhovich G.F., Puzirenko A.Yu. *Komp'yuternaya steganografiya. Teoriya i praktika* [Computer steganography. Theory and practice]. Kiev, MK-Press, 2006. 288p.

[3] Agranovskii A.V., Balakin. A.V., Gribunin V.G. *Steganografiya, tsifrovye vodyanye znaki i steganoanaliz* [Steganography, digital watermarking and steganalysis]. Moscow, Vuzovskaya kniga, 2009. 220 p.

[4] Mallat S. *A wavelet tour of signal processing: The Sparse Way.* San Diego, Academic Press, 2008. 832 p.

[5] Addison P. *The illustrated wavelet transform handbook: Introductory Theory and Applications in Science, Engineering, Medicine and Finance.* Edinburgh, IoP, 2002. 368 p.

[6] Vovk O.O., Astrakhantsev A.A., Dorozhan A.V. Issledovanie stoikosti metodov skrytiya informatsii v nepodvizhnykh izobrazheniyakh [Investigation of stability of information hiding methods in still images]. *Sistemi obrobki informatsiї*, 2012, No 2 (54), pp.104-109.

[7] Vovk O.O., Astrakhantsev A.A., Dorozhan A.V. Issledovanie kharakteristik metodov skrytiya na osnove NZB na fone additivnogo shuma [The study characteristics of the hiding methods based on LSB in additive noise]. *Visnik natsional'nogo tekhnichnogo universitetu "KhPI",* 2012, No 18, pp. 37-40.

Табл. 2.

Table 2.

Переформатирован./ сжатие	В пространственной области		В частотной области				В области преобразов.
	КДБ	ДДКМ	КЖ		БМЕЮ		ДВП
Размер изображения:	640×640	640×640	2048×2048	640×640	2048×2048	640×640	640×640
bmp-png	+	+	+	+	+	+	+
bmp-tiff	+	+	+	+	+	+	+
bmp-jpeg(rgb)/0%	-	-	+	+	+	+	+
bmp-jpeg(rgb)/25%	-	-	+	+	+	+	+
bmp-jpeg(rgb)/50%	-	-	+	+	+	+	+
bmp-jpeg (Ycbcr)/0%	-	-	+	-	+	-	+
bmp-jpeg (Ycbcr)/25%	-	-	+	-	-	-	+
bmp-jpeg (CMYK)/0%	+	-	+	+	+	+	+
bmp-jpeg (CMYK)/25%	-	-	+	+	+	+	+