

УДК 004.352

АЛГОРИТМ ИЗВЛЕЧЕНИЯ СКРЫТОЙ ИНФОРМАЦИИ ИЗ ОТСКАНИРОВАННЫХ ПОЛИГРАФИЧЕСКИХ ИЗДЕЛИЙ

© 2008 Н.И. Глумов², В.А. Митекин^{1,2}, А.В. Сергеев², В.А. Федосеев^{1,2}

¹ Самарский государственный аэрокосмический университет;

² Институт систем обработки изображений РАН

Предлагается метод стегоанализа алгоритма «Invisible Personal Information», предназначенного для встраивания цифровых водяных знаков (ЦВЗ) в полиграфические изделия и считающегося стеганографически стойким. Предлагаемый метод стегоанализа состоит из двух этапов: выделение из всего множества ключей встраивания подмножества вероятных ключей и препарирование изображения с использованием каждого из выбранных ключей с целью выявления водяного знака. Также в работе исследуется устойчивость работы алгоритма стегоанализа к искажениям, вызванным процессами печати и сканирования стегограммы, содержащей ЦВЗ.

Цифровой водяной знак, стеганографическая система, стегоанализ, полиграфические изделия, линзовый растр, ключ встраивания

Введение

В настоящей работе объектом исследования является стегосистема, известная под названием «Invisible Personal Information», или IPI [1-5], широко применяемая на практике при аутентификации ценных бумаг и удостоверений личности, а также при скрытой передаче информации на бумажном носителе. Данная стегосистема по заявлению ее разработчиков является стеганографически стойкой [2]. В работе делается попытка построения атаки на стегосистему IPI с целью опровержения этого тезиса. Также в работе исследуется устойчивость работы разработанного метода стегоанализа к искажениям стегограммы.

Описание стегосистемы IPI

Рассматриваемая стегосистема предназначена для встраивания невидимого ЦВЗ в полиграфические изделия. Благодаря использованию специфических свойств современных устройств растровой печати она позволяет без значительной потери визуального качества печатаемого изделия встроить в него ЦВЗ, стойкий к печати и повторному сканированию. Широкому распространению данной системы послужил также тот факт, что извлечение информации может осуществляться визуально при помощи простейшей оптической системы – линзового или щелевого растра [6].

Принципы встраивания и извлечения ЦВЗ, используемые в IPI, заключаются в сле-

дующем. *Контейнер*, предназначенный для встраивания ЦВЗ данным методом, представляет собой бинарное изображение, состоящее из множества растровых точек, расположенных в узлах регулярной сетки. Такой тип изображений обычно является результатом предпечатной подготовки полутонных цифровых изображений с использованием растривания. *ЦВЗ* также представляет собой бинарное изображение, равное по размерам изображению-контейнеру. Встраивание ЦВЗ заключается в малом, меньшем, чем период регулярной сетки, смещении растровых точек контейнера (рис. 1а). Величина и направление смещения одинаковы для всех выбранных точек. Данная операция не приводит к изменению средней яркости соответствующей области контейнера, чем объясняется визуальная незаметность встроеного ЦВЗ.

Извлечение ЦВЗ производится путем наложения на стегограмму линзового или щелевого растра, направление и шаг сетки которого согласованы с аналогичными параметрами регулярной сетки контейнера (рис. 1б). Эта операция приводит к изменению средней яркости в областях стегограммы, подвергнутых смещению, что приводит к проявлению ЦВЗ.

В качестве стеганографического ключа выступают шаг и направление смещения.

Метод выбора подмножества приемлемых ключей при стегоанализе

Наименьшие искажения в изображении-контейнер будут вноситься при исполь-

зовании параметров ключа, близких по значению к параметрам растровой сетки. Поэтому задача отыскания вероятных ключей сводится к задаче оценки параметров периодических структур стегограммы. Данная задача может быть решена путем анализа спектральных характеристик изображения–стегограммы. По свойствам ДПФ модуль

Фурье-спектра изображения, содержащего доминирующую периодическую структуру, имеет локальные экстремумы на частотах, соответствующих периодической решетке, а также на кратных частотах (рис. 2). Искомые параметры решетки – период и направление – вычисляются по этим частотам.

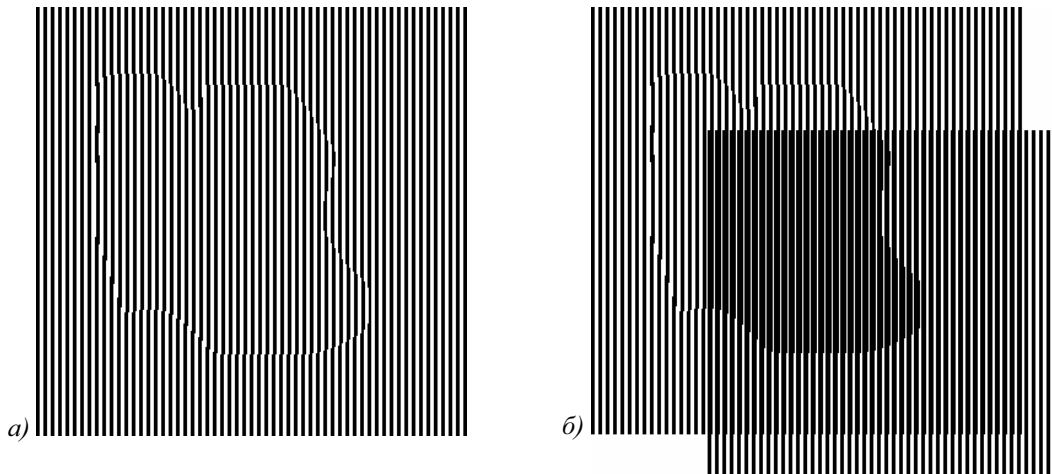


Рис. 1. Принцип встраивания (а) и извлечения (б) водяного знака методом IPI

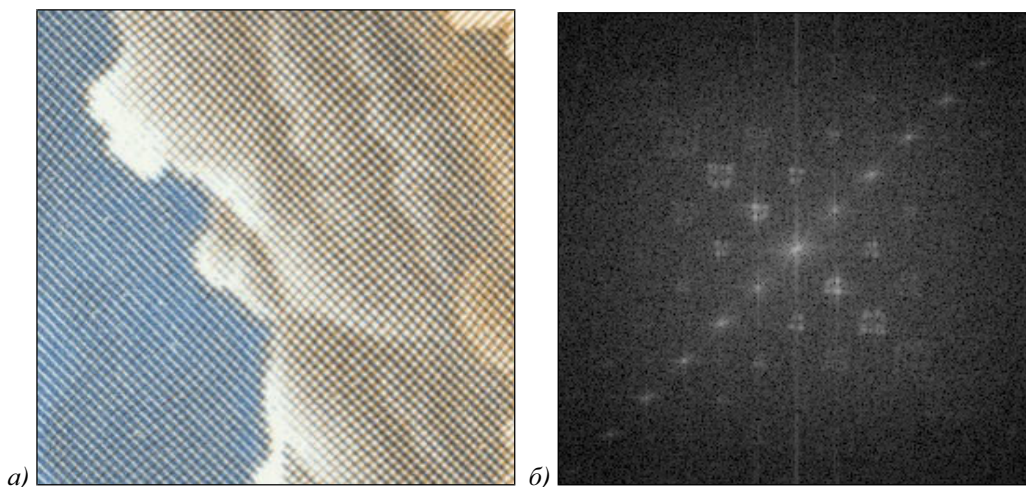


Рис. 2. Фрагмент изображения стегограммы (а) и ее спектр мощности (б)

Алгоритм препарирования стегограммы

Очевидно, вследствие двумерности природы изображения после работы процедуры, описанной в предыдущем разделе, количество приемлемых ключей не превышает двух. Для проверки каждого из них был реализован алгоритм препарирования стегограммы, делающий ЦВЗ визуально видимым в случае его наличия.

Алгоритм препарирования имитирует эффект наложения линзового раstra и со-

стоит из двух этапов. На первом этапе применяется линейный полосовой фильтр для усиления спектральных компонент стегограммы, соответствующих найденной периодической структуре. На втором этапе для подавления сетки раstra производится вычисление поля локальной дисперсии полученного изображения.

Пример стегограммы до и после применения описанной процедуры препарирования приведен на рис. 3.



Рис. 3. Стегограмма «Облака» до (а) и после (б) применения процедуры препарирования

Построение математической модели «принтер-сканер»

Для оценки устойчивости работы алгоритма стегоанализа к искажениям, возникающим при печати изображения и последующем сканировании, построена следующая математическая модель искажающей системы "принтер-сканер":

- (1) исходное изображение $x(n_1, n_2)$ подвергается сглаживанию фильтром с гауссовской импульсной характеристикой:

$$y_{\sigma}(n_1, n_2) = x(n_1, n_2) ** h(n_1, n_2),$$

$$h(n_1, n_2) = \frac{1}{2\pi\sigma_s^2} \exp\left\{-\frac{n_1^2 + n_2^2}{2\sigma_s^2}\right\},$$

где $y_{\sigma}(n_1, n_2)$ – сглаженное изображение, σ_s – СКО гауссовского распределения.

- (2) сглаженное изображение $y_{\sigma}(n_1, n_2)$ подвергается аддитивному зашумлению гауссовским белым шумом $\xi(n_1, n_2)$ с нулевым математическим ожиданием и АКФ $B_{\xi}(m_1, m_2) = \sigma_{\xi}^2 \delta(m_1, m_2)$, где σ_{ξ} – СКО шума, а $\delta(m_1, m_2)$ – дельта-функция:

$$y_{\xi}(n_1, n_2) = x(n_1, n_2) + \xi(n_1, n_2).$$

Моделирование работы алгоритма при искажении стегограмм

В работе было проведено моделирование влияния искажающей системы (1)-(2) на работу алгоритма стегоанализа. В качестве показателя качества Q применялся модуль коэффициента корреляции между исходным и извлеченным ЦВЗ. На рис. 4 приведен график зависимости показателя качества Q от параметра σ_s при различных σ_{ξ} .

Анализируя полученные результаты, можно сделать ряд выводов о влиянии искажающих факторов на устойчивость работы алгоритма стегоанализа:

- 1) влияние шумового фактора в исследованном диапазоне параметра σ_{ξ} крайне незначительно (не выше 0.5%) для всех значений параметра σ_s ;
- 2) в исследованном диапазоне значений параметра расфокусировки наблюдается незначительное ухудшение качества (не выше 5%).

Таким образом, полученные в ходе вычислительного эксперимента результаты позволяют сделать вывод о незначительном влиянии искажающей системы "принтер-сканер" на качество выделения ЦВЗ разработанным алгоритмом стегоанализа.

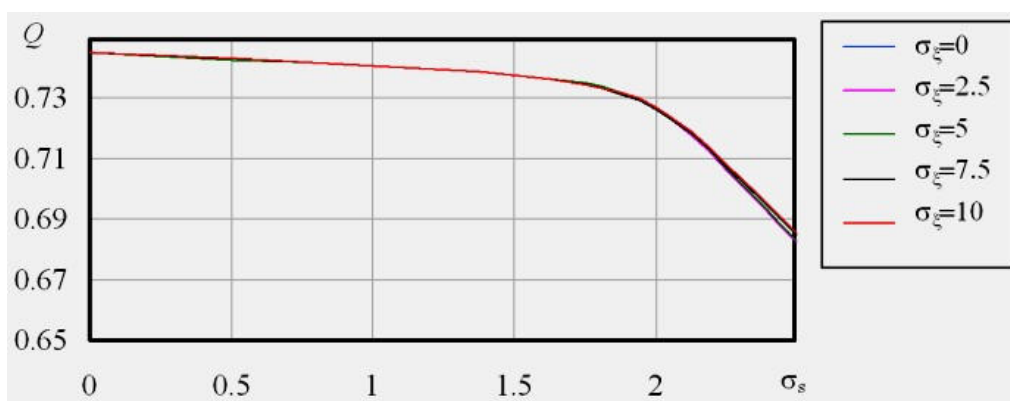


Рис. 4. График влияния искажений на качество выделения ЦВЗ

Заключение

Предложенный в работе двухэтапный метод стегоанализа алгоритма «Invisible Personal Information» позволяет приближенно вычислять ключи встраивания и выделять визуально различимые ЦВЗ на отсканированных изображениях стегограмм. Исследования показали, что разработанный алгоритм устойчив к искажениям стегограммы, не приводящим к разрушению растровой сетки. Вышесказанное позволяет сделать вывод о том, что система IPi не является стеганографически стойкой.

Библиографический список

1. **Anan, T.** Watermarking Technologies for Security-Enhanced Printed Documents [Текст] / T. Anan, Kuraki, K., Nakagata, S. // Magazine FUJITSU (vol. 58, No.3),

Abstracts of Research and Development special issue. – 2007. – P.197-203.

2. **Masahiko, S.** A Watermark Embedding and Extracting Method for Printed Documents [Текст] / S. Masahiko // Transactions of the institute of electronics, information and communication engineers. – 2004. – N.6. – P. 778-786.

3. Anti-counterfeiting method and apparatus using digital screening [Текст] – US Patent 6,104,812.

4. Digital anti-counterfeiting software method and apparatus [Текст] – US Patent 5,708,717.

5. Anti-counterfeiting process using lenticular optics and color masking [Текст] – US Patent 5303370.

6. **Валюс, Н.А.** Стереоскопия. [Текст] / Н.А. Валюс – М.: Издательство АН СССР, 1962. – 380 с.

References

1. **Anan, T.** Watermarking Technologies for Security-Enhanced Printed Documents / T. Anan, Kuraki, K., Nakagata, S. // Magazine FUJITSU (vol. 58, No.3), Abstracts of Research and Development special issue. – 2007. – P.197-203.

2. **Masahiko, S.** A Watermark Embedding and Extracting Method for Printed Documents / S. Masahiko // Transactions of the insti-

tute of electronics, information and communication engineers. – 2004. – N.6. – P. 778-786.

3. Anti-counterfeiting method and apparatus using digital screening – US Patent 6,104,812.

4. Digital anti-counterfeiting software method and apparatus – US Patent 5,708,717.

5. Anti-counterfeiting process using lenticular optics and color masking – US Patent 5303370.

6. **Valyus, N.A.** Stereoscopy / N.A. Valyus – Moscow: USSR Academy of Sciences Publishers, 1962. – 380 p.

AN ALGORITHM FOR EXTRACTING INVISIBLE INFORMATION FROM SCANNED POLYGRAPHIC PRODUCTS

© 2008 N.I. Glumov², V.A. Mitekin^{1,2}, A.V. Sergeev², V.A. Fedoseev^{1,2}

¹ Samara State Aerospace University

² Image Processing Systems Institute of the RAS

We propose a steganalysis technique for the Invisible Personal Information algorithm intended for embedding digital watermarks (DWM) in polygraphic products and considered steganographically robust. The steganalysis technique in question involves two stages: first, out of the entire set of embedding keys a probable key subset is extracted and, then, the image is being prepared using each of the keys chosen so that a watermark can be discovered. Also, we investigate the robustness of the steganalysis algorithm relative to distortions due to printing and scanning of stegagrams with DWMs.

Digital water mark, steganographic system, polygraphic products, lens array, embedding key

Сведения об авторах

Глумов Николай Иванович. В 1985 г. окончил Куйбышевский авиационный институт по специальности «Прикладная математика». В настоящее время старший научный сотрудник лаборатории математических методов обработки изображений ИСО РАН. Кандидат технических наук. Область интересов - математические методы обработки и распознавания цифровых изображений.

Митекин Виталий Анатольевич в 2006 году закончил факультет информатики СГАУ. В данный момент является аспирантом кафедры геоинформатики СГАУ и стажером-исследователем ИСОИ РАН. В область научных интересов входят стеганография и стегоанализ.

Сергеев Александр Владиславович в 2007 году защитил диплом бакалавра факультета информатики СГАУ. В данный момент работает техником в ИСОИ РАН. В область научных интересов входят стеганография, компрессия изображений, алгоритмы обработки и анализа изображений.

Федосеев Виктор Андреевич в 2007 году защитил диплом бакалавра в Самарском государственном аэрокосмическом университете (СГАУ). В настоящее время продолжает обучение в СГАУ, а также работает техником в Институте систем обработки изображений РАН. Круг научных интересов включает обработку изображений, компьютерную графику, стеганографию, криптографию.

Glumov Nikolay Ivanovich, in 1985 graduated from Kuibyshev Aviation Institute, majoring in Applied Mathematics. Currently he is a senior researcher at IPSI RAS, Mathematical Methods of Image Processing laboratory. He is a candidate in Engineering. Research interests: mathematical methods of digital image processing and recognition.

Mityekin Vitaliy Anatolievich, in 2006 graduated from SSAU's Informatics department. Currently, he is a post-graduate student at SSAU's Geo-Informatics sub-department and a trainee researcher at IPSI RAS. Research interests: steganography and steganalysis.

Sergeev Alexandr Vladislavovich, in 2007 received BSc degree from SSAU's Informatics department. He works as a technician at IPSI RAS. Research interests include steganography, image compression, algorithms for image processing and analysis.

Fedoseev Victor Andreevich, in 2007 received BSc degree from SSAU. Currently, he continues his studies at SSAU and works as a technician at IPSI RAS. Research interests include image processing, computer graphics, steganography, cryptography.