Стеганографическая защита изображений из PDF документов на основе конвертора PDF-SVG

В.Н. Горбачев[1], И.К. Метелёв[1], Е.М. Кайнарова[1], М.А. Полякова[1]
helenkainarova@gmail.com|polyakovaqueen1998@mail.ru.
[1]СПб Государственный университет промышленных технологий и дизайна, Санкт-Петербург, Россия

В работе рассмотрен вопрос о защите изображений, входящих в состав PDF документа. Основой предложенной стеганографеческой схемы служит конвертор PDF-SVG, который извлекает изображение из документа и возвращает его обратно после встраивания цифровых данных. Обсуждаются два варианта встраивания, использующие дискретное вейвлет преобразование и битовые плоскости полутонового контейнера.

Ключевые слова: *стеганография, PDF, цифровые водяные знаки.*

Steganographic protection of image from PDF document using a convertor PDF-SVG

V.N. Gorbachev[1], I.K. Metelev[1], E.M. Kaynarova[1], M.A. Polyakova[1]
helenkainarova@gmail.com|polyakovaqueen1998@mail.ru.
[1]Saint-Petersburg State University of Industrial Technologies and Design, Saint-Petersburg, Russia

Protection of the images included in PDF document is considered. The basis of the proposed steganographic scheme is a convertor of PDF-SVG, that extracts images from PDF document and returns it back after embedding data. We discussed two embedding methods using a wavelet transform and bit planes of the grayscale cover.

Keywords: *steganography, PDF, watermarks.*

Будучи широко распространенным форматом представления электронных документов, PDF имеет разнообразную криптографическую защиту. Однако задача защиты информации не имеет единственного решения, что является источником новых предложений, в число которых входят стеганографические методы. Богатая структура PDF формата позволяет использовать морфологические и семантические характеристики текста, модификацию операторов визуализации текста. и многое другое [1].

При морфологическом подходе бит информации кодируется текстовой альтернативой: пассивный или активный залог, синонимы [2]. В технике кодирования пробелами, White Space Coding, используют обычный и неразрывный пробел, которые визуально неразличимы, но имеют разные коды [3]. В методе TJ (Text Justified) операторов, выравнивающих текст, данные встраиваются в интервалы между словами. [4]. При выравнивании длины интервалов принимают случайный характер, что дает возможность их модифицировать, используя LSB (Least Significant Bit) методы [5] или размытие (Dither Modulation) [6]. Сообщение можно закодировать перестановкой, которая встраивается в 1d или 2d массив. Встраивание в частотную область цифрового изображения специально выбранной перестановки, которая имеет циклы длиной не больше 2, ее называют инволюция, оказывается устойчивым к JPEG сжатию с потерей [7].

Встраивание цифровых водяных знаков (ЦВЗ) предусмотрено рядом приложений. К их числу относится Adobe Acrobat и редактор TEX, который может создавать выходной файл в PDF. Эти приложения позволяют встроить видимые ЦВЗ, представляющие собой полупрозрачный текст или изображения, которые затрудняют зрительное восприятие. Техника видимых ЦВЗ предполагает, что их может удалить законный пользователь за отдельную плату [8].

В отличие от рассмотренных методов мы сосредоточили внимание на защите изображений в PDF документах. Для этой цели предложен конвертор $PDF - SVG$. Он сохраняет изображения, извлеченные из PDF документа, в формате PNG или JPEG, в которые встраиваются как невидимые, так и видимые ЦВЗ. Защищенное изображение конвертор возвращает обратно в документ. Для случая видимых ЦВЗ целью является восстановление исходного изображения. В нашем методе величина PSNR (Peack Signal Noise Ratio) между оригиналом и восстановленным изображением может достигать порядка 55.8 дБ. Это значение свидетельствует о высоком качестве восстановленного изображения.

1. Встраивание с помощью конвертора

Стеганографическая схема содержит конвертор, который осуществляет преобразование между двумя форматами PDF и SVG, алгоритмы встраивания и детектирования.

1.1. Схема

Работа схемы содержит следующие шаги:

1. Конвертор извлекает изображения из PDF документа и сохраняет их в графическом формате PNG или JPEG. Эти или модифицированные изображения конвертор возвращает обратно в PDF документ.

2. Извлеченные изображения могут модифицироваться путем встраивания, детектирования или удаления ЦВЗ.

В качестве ЦВЗ используется бинарное изображение M, которое встраивается в контейнер C, полученный из графического файла PNG или JPEG. В случае невидимых ЦВЗ алгоритмы детектирования извлекают встроенные данные M'. В случае видимых ЦВЗ восстанавливается исходный контейнер CR. Из-за необратимости преобразований извлеченные данные и восстановленный контейнер будут отличаться от оригиналов. Однако в обоих случаях требуется выполнить условие неразличимости

$$M \approx M',$$
$$C \approx CR.$$

Эти условия допускают две интерпретации. С одной стороны есть два изображения, которые выглядят одинаково. С другой стороны можно говорить о недетектируемости. Для невидимых ЦВЗ это означает невозможность определить с вероятностью единица наличие встроенных данных путем статистического анализа. Для видимых ЦВЗ это означает невозможность определить был ли удален встроенный ЦВЗ из изображения нелегитимным пользователем.

1.2. Конвертор

Важным свойством нашего конвертора является обратимость, что позволяет преобразовывать данные без потерь.

В сети Интернет можно найти большое число предложений как преобразовать изображение из PDF в графический формат PNG, JPEG и обратно. Были выбраны наугад два конвертора[1] и полутоновое изображение a.png с яркостью пиксела $0, 1, \ldots, 255$. Мы рассмотрели преобразование

$$\mathsf{a.png} \to \mathsf{PDF} \to \mathsf{b.png}.$$

Было найдено, что разность яркостей пикселов у изображений a.png и b.png достигала 129 единиц, что заметно при визуальном восприятии. Для нашего конвертора разность оказалась равно нулю, что означает обратимость преобразования.

Отметим точность, с которой получается этот результат. Для кодирования в графическом формате обычно используются целые неотрицательные числа, поэтому при вычислениях или записи в графический формат все числа округляются. Чтобы исключить случайное совпадение, было протестировано 200 различных pdf-документов. В результате наш конвертор можно считать обратимым по крайней мере в случае преобразования данных, представленных целыми неотрицательными числами. Это означает, что конвертирование не будет вносить ошибок в процессы извлечения ЦВЗ и восстановления контейнера.

[1] http://pdf-png-jpg.eu/, http://online2pdf.com/convertor-png-to-pdf

2. Частотное встраивание

Встраивание данных осуществлялось путем замены части коэффициентов дискретного вейвлет преобразования контейнера пикселами ЦВЗ.

2.1. Встраивание с помощью вейвлет преобразования

Алгоритмы встраивания и детектирования содержат следующие шаги:

1. Контейнер подвергается одноуровневому дискретному вейвлет преобразованию DWT (Discrete Wavelet Transform).
2. Часть коэффициентов из выбранного частотного блока заменяется на биты сообщение и осуществляется обратное преобразование IDWT.
3. Встроенные данные извлекаются из выбранного частотного блока.

Вейвлет преобразование извлеченного из PDF документа изображения C дает четыре блока коэффициентов

$$\mathsf{DWT}(C) = \{cA, cH, cV, cD\},$$

где cA коэффициенты аппроксимации, cH, cV и cD коэффициенты горизонтальных, вертикальных и диагональных деталей. В литературе их также называют LL, LH, HL, HH частотными полосами от Low и High, высокий и низкий. Пусть сообщение M встраивается, например, в блок cD. Для этого M масштабируется путем изменения размера и яркости

$$M \to M_u \to aM_u,$$

где aM_u - изображение с новыми размерами и яркостью, которые определяются коэффициентами u и a. Эти коэффициенты играют важную роль, они подбираются экспериментально, исходя из поставленной задачи. Изменяя u или a, можно полностью или частично заполнить контейнер или сделать встроенные данные как видимыми, так и невидимыми. В результате часть коэффициентов cD заменяется на aM_u и блок со встроенными данными cD^* используется далее для формирования стегоконтейнера

$$S = \mathsf{IDWT}\{cA, cH, cV, cD^*\}.$$

Данные извлекаются из стегоконтейнера S', который получается из S путем некоторого преобразования T:

$$\mathsf{T} : S \to S'.$$

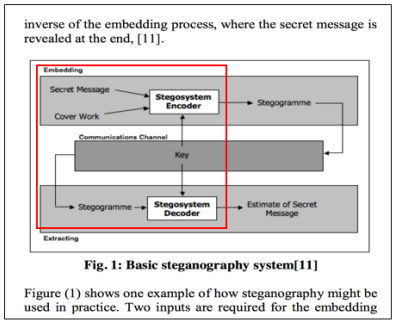
С помощью T описывается ряд процессов, в число которых входит запись изображения в графический формат, считывание, конвертирование, передача данных конвертору и др.

2.2. Эксперимент

Результат встраивания невидимого ЦВЗ приведен на рис. 1. Слева фрагмент PDF документа[2], он содер-

[2] Фрагмент из работы Y-C Lai, W-H Tsai, Covert communication via PDF files by new data hiding techniques, NSC project No, 97-2631-H-009-001

жит изображение *Fig. 1: Basic steganographic system*, которое расположено в тексте. Изображение защищено невидимым ЦВЗ, встроенным в область, отмеченную красным. Справа приведен ЦВЗ, представленный бинарным изображением. Для DWT был взят ортогональный вейвлет *db6* из семейства Добеши.



ЦВЗ,
бинарное изображение

Контейнер с ЦВЗ, a=20, u=0.5, вейвлет db2

Рис. 1. Фрагмент PDF документа с защищенным изображением.

Выбранные величины a=20 и u=0.5 означают, что яркость бинарного ЦВЗ увеличена в 20 раз и заменено 50% коэффициентов блока cD.

Мы рассмотрели встраивание с несколькими вейвлетами из семейства Добеши db1, db2, db6, db26, db41 для a=20 и u=0.5. При детектировании возникали ошибки, когда в извлеченных ЦВЗ от 2% до 15% пикселов воспроизводится неправильно. Было установлено, что основной причиной ошибки является потеря точности при округлении, которая возникает при записи цифрового изображения с ЦВЗ в графический формат.

3. Пространственное встраивание

Используя побитовое сложение, можно встроить бинарное изображение в битовую плоскость полутонового контейнера. Тогда ошибки округления при записи изображения в графический формат будут исключены.

3.1. Встраивание в битовые плоскости

В основе алгоритма лежит идея удвоения битовых плоскостей [9]. Благодаря избыточности, можно построить полутоновое изображение с двумя одинаковыми битовыми плоскостями, причем визуально оно не будет отличаться от исходного. Тогда одна из плоскостей может быть использована для встраивания данных, а вторая для слепого детектирования ЦВЗ или восстановления контейнера.

Любое полутоновое изображение с битовой глубиной k можно представить с помощью набора битовых плоскостей. Для $k = 8$

$$C = B_8 2^7 + \cdots + B_1 2^0, \qquad (1)$$

где $B_V = bitget(C, V)$ битовая плоскость, для вычисления которой введена функция `bitget`, $V = 1, 2, \ldots, 8$. Плоскость B_1 называют LSB (Least Significant Bit) плоскостью, она не содержит семантической информации. Используя (1), можно получить изображение с двумя битовыми плоскостями. Пусть B_V и B_U, где $V > U$ две битовые плоскости C. Тогда изображение C_D с двумя битовыми плоскостями B_V имеет вид

$$C_D = C - B_U 2^{U-1} + B_V 2^{U-1}. \qquad (2)$$

Алгоритм встраивания, использующий (2), содержит следующие шаги.

1. Для выбранных V и U строится контейнер C_D с двумя битовыми плоскостями .
2. В плоскость V встраивается бинарное изображение путем побитового сложения

$$C \to S = C_D - B_V 2^{V-1} + (B_V \oplus M) 2^{V-1}. \qquad (3)$$

Встроенное изображение будет видимым или невидимым в зависимости от выбора V. Мы рассмотрим случай видимых ЦВЗ, для которого в качестве V следует взять старшие битовые плоскости. Чтобы восстановить контейнер, старшая плоскость V, содержащая ЦВЗ, удаляется, а на ее место ставится U

$$S \to CR = S - bitget(S, V) 2^{V-1}$$
$$+ bitget(S, U) 2^{V-1} - bitget(S, U) 2^{U-1}.$$

Отличие контейнеров определяется младшей битовой плоскостью

$$C - CR = B_U 2^U. \qquad (4)$$

Пример работы показан на рис. 2.

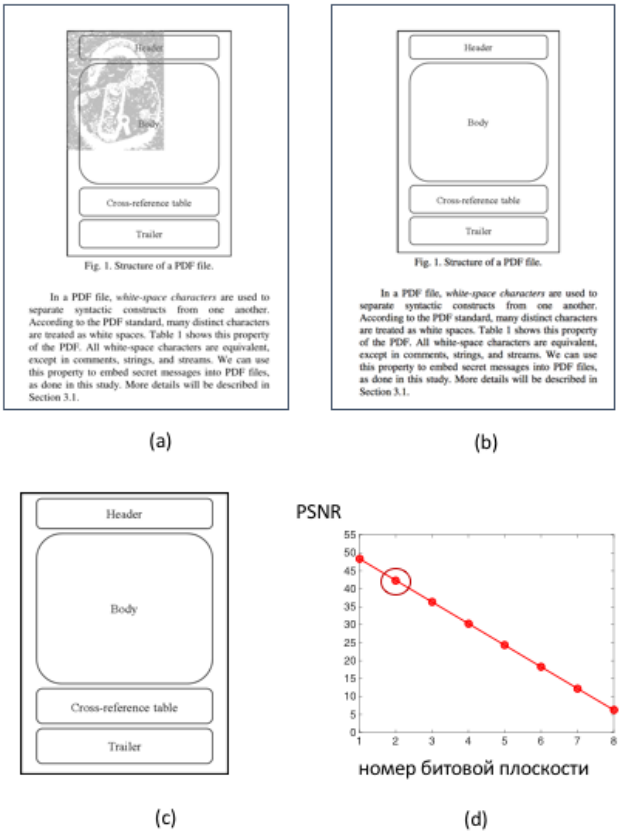


Рис. 2. Видимые и устранимые ЦВЗ.

На рис. 2 (a) приведен фрагмент PDF документа с изображением *Fig.1 Structure of PDF file*[3], в которое встроен видимый ЦВЗ. Использованы плоскости $V = 7$ и $U = 2$. Фрагмент PDF и изображение с удаленным ЦВЗ представлены на рис. 2 (b) и (c). После удаления ЦВЗ восстановленный документ визуально неотличим от исходного. На рис. 2 (d) приведена зависимость пикового отношения сигнал шум PSNR от номера удаленной битовой плоскости. Для рассматриваемого случая $U = 2$ величина PSNR=42.3417 Дб. Это значение совпадает с рассчитанным из эксперимента, который включает цепочку преобразований с конвертированием. Найденное совпадение подтверждает обратимость этих преобразований. Полученное значение PSNR свидетельствует о высоком качестве восстановленного изображения и совпадает с визуальной оценкой. В этом примере для дублирования использована вторая битовая плоскость $U = 2$. Если взять LSB плоскость $U = 1$, то можно получить более высокое PSNR: порядка 55.8 дБ, как это следует из графика на рис. 2 (d). Заметим, наши результаты получены для пространственного встраивания. В случае частотной техники, развитой в [10] для видимых ЦВЗ на основе DWT, значение PSNR оказываются несколько хуже: 37-40 дБ.

4. Выводы

1. Изображения, входящие в состав PDF документов, могут быть скопированы нелегитимным пользователем и потому нуждаются в своей собственной защите.
2. В стеганографической схеме может быть использован конвертор, который преобразует изображения из PDF в графический формат и обратно. Поэтому можно использовать разные методы защиты цифровых изображений, включающие пространственную и частотную технику.
3. Для встраивания в частотной области возникает характерная ошибка, обусловленная потерей точности из-за сохранения изображения в графическом формате. При использовании битовых плоскостей эта ошибка может быть исключена.

5. Литература

[1] Ndoundam R., Ekodeck S. G. PDF Steganography based on Chinese Remainder Theorem // arXiv:1506.01256v1 [cs.CR] 3 Jun 2015.

[2] Meral H.M., Sankur B., Ozsoy A. S., Gungor T.,Sevinc E. Natural language watermarking via morphosyntactic alterations, // Computer Speech & Language Journal, 2009. - Vol. 23, No 1, pp 107-125.

[3] Wang J.T., Tsai W.H. Data hiding in PDF files and applications by imperceptible modifications of PDF object parameters. // Proc. of 2008 Conf. on Computer Vision, Graphics & Image Proc., Yilan, Taiwan, Aug. 2008, pp. 24-26.

[4] Zhong S., Cheng X., Chen T. Data hiding in a kind of pdf texts for secret communicationl. International // Journal of Network Security, 2007. - Vol. 4(1), pp. 17–26.

[5] Alizadeh-Fahimeh, F., Canceill-Nicolas, N., Dabkiewicz-Sebastian, S., Vandevenne-Diederik, D. Using Steganography to hide messages inside PDF files, // 2012, SSN Project Report.

[6] Bitar A.W., Darazi R., Couchot J-F., Couturier R. Blind digital watermarking in PDF documents using Spread Transform Dither Modulation, // Multimes Tools Appl, DOI 10 1007 s11042-015-3034-2,

[7] Chroni M, A. Fylakis A., Nikolopoulos S.D. Watermarking PDF Documents using Various Representations of Self-inverting Permutations. // arXiv:1501.02686 [cs.MM], 2015.

[8] Mintzer F.C., Lotspiech J., Morimoto N. IBM, 1997. Safeguarding digital library contents and users: Digital watermarking. // D-Lib Magazin [Online]. Avalable: http//www.dlib.org/dlib/december97/ ibm/12lotspiech.html.

[9] Горбачев В.Н., Кайнарова Е.М., Денисов Л.А. Встраивание бинарного изображения в плоскости Грея. // Компьютерная оптика, 2013. - Т. 37, № 3, - С. 385-390.

[10] Hu Y, S., Huang S.K.J An algorithm for removable Visible Watermarking.// IEEE. Transactions on circuits and systems video technology. 2006. - Vol. 16, No 1, pp.129-133.

[3] Фрагмент страницы из [2]