STUDYING PRODUCTS AND SERVICES FOR HIDING DATA IN IMAGES

Dancho D. Talev

National Military University "Vasil Levski"
specialty "Computer Systems and Technologies", V grade, Veliko Tarnovo

ИЗСЛЕДВАНЕ НА ПРОДУКТИ И УСЛУГИ ЗА КРИЕНЕ НА ДАННИ В ИЗОБРАЖЕНИЯ

Данчо Д. Талев

Национален Военен Университет „Васил Левски"
специалност „Компютърни системи и технологии", V курс, Велико Търново

***Abstract**: From the creation of writing to modern IT, the protection of valuable data is of utmost importance. Through the ages people created many techniques and means to hide messages. The science that delves into these techniques is called steganography.*

***Keywords**: Steganography, Least Significant Bit, Mean square error, Bit error rate*

Art. 3 - Introduction

Осигуряването на „Конфиденциалност на информацията" е защитата й от разкриване от неоторизиран субект [10]. Защитата на информацията започва с определяне на ВАЖНАТА информация, тази която се нуждае от защита [1].

Един от начините за защита на информацията или осигуряването на нейната конфиденциалност е стеганографията[11]. Стеганографията осигурява сигурен трансфер на данните, поради самото скриване на факта за осъществяване на тайна комуникация. Съществуват много определения за стеганография [2],[3], [8] като общото в тях е, че тя е наука, при която с помощта на различни технически средства се извършва скриване на информация в цифрови носители, и се реализира предаването ѝ между две комуникиращи си страни, т.е. тя е науката за скриване на самото съобщение, а не на неговото съдържание.

3 Стеганографски подходи

LSB (Least Significant Bit) е често срещан и лесен подход за скриване на информация в най-младшия бит на изображения. Методът представлява замяна на най-младшия бит на някои или всички байтове на изображението с бит от конфиденциалното съобщение. Записването в последователни битове на пикселите на изображението е лесно за засичане и затова се предпочита използването на секретен ключ, спрямо който се определят отделните пиксели за промяна и четене[4].

1. SSIS (Стеганография чрез метода на разширяване на спектъра)

Стеганографията чрез разширяване на спектъра SSIS (Spread Spectrum Image Steganography) е метод, който има много предимства. Този метод е популярен още като стеганографски метод с разпръскващо се вграждане[5]. Тази система скрива и възстановява съобщения със значителна дължина в рамките на цифрови изображения, запазвайки оригиналния размер на изображението и динамичен обхват. Скритото съобщение може да бъде възстановено с помощта на подходящи ключове без никакво познаване на оригиналното изображение. Съобщението, вградено от този метод, може да бъде под формата на текст, изображения или друг цифров сигнал[3].

1.1. DCT (Дискретното косинус преобразование)

DCT (Discrete cosine transform) е едно от най-широко използваните преобразувания в стеганографията. Използването на DCT се основава на JPEG компресията. Преди началото на компресията, изображението, се представя като матрица от пиксели, която се състои от редове и колони. Всеки елемент на матрицата е пиксел от изображението. Следва преобразуване на стойността на всеки пиксел от RGB цветово пространство в YCbCr цветово пространство. С Y компонентата се обозначава интензитетът на пикселите, а компонентите Cb и Cr обозначават съответно количеството на син и червен цвят в пикселите. Следващ етап в алгоритъма е изображението да се раздели на блокове 8x8, всеки от които се подлага на дискретно косинус преобразуване [9]. Ако броят на пикселите по хоризонтала или вертикала не се дели без остатък на 8, се добавят фиктивни колони или редове в изображението. JPEG компресията осигурява най-добър резултат тогава, когато стойностите на съседни пиксели в даден блок имат сходни по големина стойности[4].

1.2. DWT (Дискретно уейвлетно преобразование)

DWT (Discrete Wavelet transform) е математическа функция, която се използва за разлагането на функции или непрекъснати във времето сигнали по честотни елементи и изучаването на всеки честотен елемент с разделителна способност, съответстваща на мащаба му. Под уейвлет преобразуване или уейвлет трансформация (wavelet transformation) се разбира представянето на функция чрез уейвлети. Уейвлетите са мащабирани и транслирани копия на уейвлет-майка, която обикновено е бързо затихващо трептене или такова с крайна дължина[4].

2. Методите за скриване на информация

2.1. Скриване на информация в текст

Един от първите мтоди на стеганографията е скриването на информация в текст. Пример за това е скриването на конфиденциално съобщение във всяка nта буква от всяка дума в текстово съобщение. След бързото развитие на Интернет и различните цифрови файлове важността на текстовата стеганография намалява. Възможно е скриване на съобщение посредством празни интервали в края на всеки ред на текстов файл, но като цяло методът не се използва, тъй като текстовите файлове имат много малък излишък[4].

2.2. Скриване на информация в аудио/ видео файл

При скриването на информация в аудио или видео файл се използват подобни техники на тези за изображения. Технология, уникална за аудио стеганографията, е маскирането, което използва свойствата на човешкото ухо, за да скрие информацията незабележимо[4].

При скриване на информация в аудио или видео файл се използват неравномерни интервали между ехото, за да се кодира последователност от стойности. Като цяло е възможно да се създадат условия, при които тези сигнали да бъдат неуловими от човешкото възприятие. Ехо сигналът се характеризира с три параметъра: начална амплитуда, степен на затихване и забавяне. Когато се достигне определен праг между сигнала и ехото, те се смесват. В този момент човешкото ухо вече не може да различава тези два сигнала[6].

2.3. Скриване на информация в изображения.

Изображенията са едни от най- масово използваните и предаваните файлове в интернет пространството. За тях е характерно, че имат голям излишък в цифровото си представяне, което ги прави най- добри и най- популярни контейнери за целите на стеганографията. Поради

спецификата на човешкото зрение скриването в тях на конфиденциална информация става напълно незабележимо[4].

3. Изследване на продукти и услуги за криене на данни в изображения

3.1. Изследвани статистически характеристики

3.1.1. Стеганографски подходи

BER (Битрейт грешка)

Както подсказва името, битрейт грешката се определя като процент, при който възникват грешки в преносната система. Той може да бъде директно преведен на броя на грешките, които възникват в низ от един отбелязан брой битове. Определението на битрейт грешката може да бъде превърнато в проста формула:

$$BER = \frac{\text{Броят на грешките}}{\text{Общ брой предадени битове}} \qquad (1)$$

Пример:

Като пример, приемете тази предадена битова последователност:

0 1 1 0 0 0 1 0 1 1

и следната получена последователност на битовете:

0 0 1 0 1 0 1 0 0 1

Броят на битовите грешки (подчертаните битове) в този случай е 3. BER е 3 неточни бита, разделени на 10 прехвърлени бита, което води до BER от 0.3 или 30%[7].

3.1.2. *MSE (Средна квадратична грешка) и PSNR (Отношение на пиковия сигнал към шума)*

Изчисляването на средната квадратична грешка е стандартен статистически подход за обективно измерване на степента на различие между две изображения. Малка стойност на MSE означава, че средното ниво на разликата между тях е малко. В случай на две еднакви изображения, MSE има стойност, равна на нула. За разлика от MSE, по-голяма стойност на PSNR означава по-добро качество на изображението. При еднаквост на две изображения, PSNR има стойност клоняща към безкрайност. Основна цел на всички стеганографски методи е минимизиране на стойността на MSE и съответно максимизиране на стойността на PSNR[4].

3.1.3. *SSIM (Индексът за измерване на структурната прилика в изображение)*

Индексът за измерване на структурната прилика в изображение SSIM (Structural Similarity Index for measuring) е подобен на MSE и PSNR, но е създаден с цел да ги подобри. Като показател той измерва промяната в яркостта, контраста и структурата на дадено изображение. За получаването на SSIM се комбинират стойностите, получени за средната интензивност на яркостта, вариациите в контраста и структурата на взаимната корелация между оригиналното и стегоизображението[6].

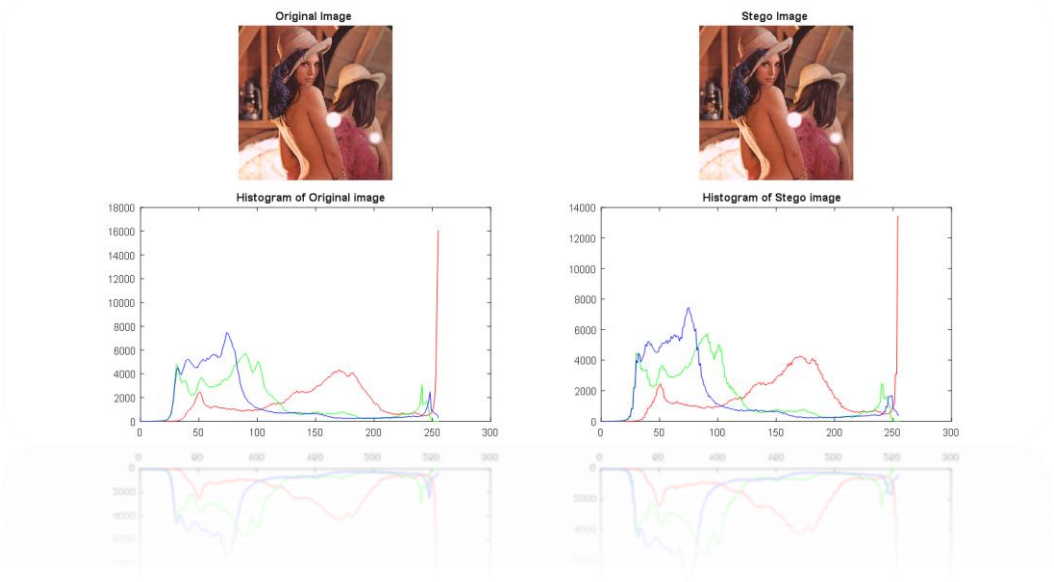
4Експериментални изследвания.

В таблици 1 е представени резултати от вграждането с различни програмни програмни системи.

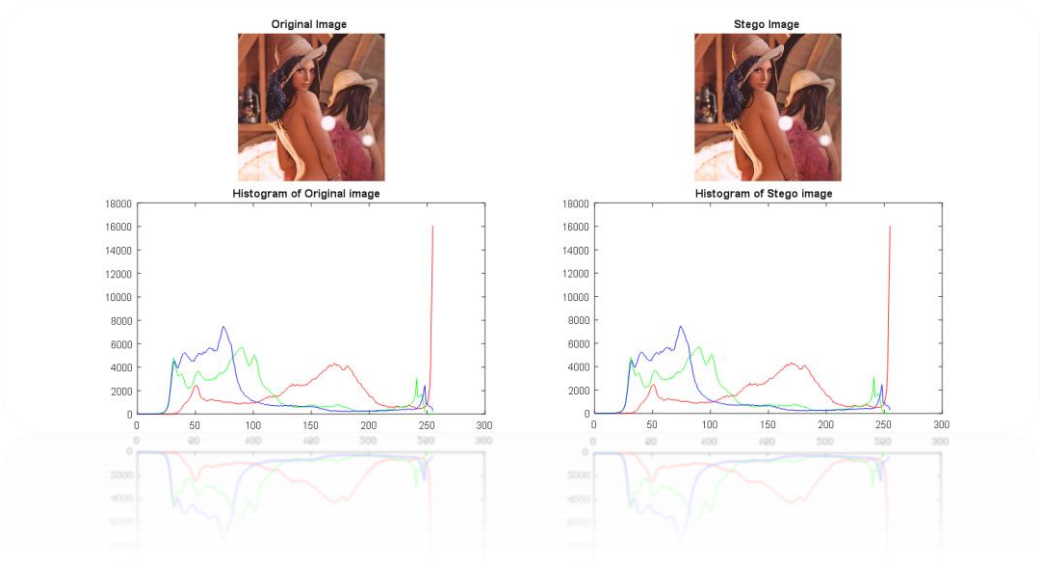
Таблица 1. Статистически характеристики на стегоизображение „Lena“

Програмна реализация	Размер на вградени данни	Изображение	BER	MSE	Peak-SNR	SNR	SSIM
Invisible Secrets 4	10B	lena_10b_AES.bmp	0.4996	0.4996	51.1444	45.1390	0.9994
	100B	lena_100b_AES.bmp	0.5003	0.5003	51.1388	45.1334	0.9994
	1кB	lena_1kb_AES.bmp	0.5003	0.5003	51.1389	45.1335	0.9994
	10kB	lena_10kb_AES.bmp	0.5006	0.5006	51.1361	45.1307	0.9994
	100kB	lena_100kb_AES.bmp	0.5000	0.5000	51.1411	45.1357	0.9994
Master Stego	10B	lena_10b_master stego.bmp	6.6732e-05	0.0001	89.8875	83.8824	1.0000
	100B	lena_100b_master stego.bmp	7.1533e-04	0.0007	79.5857	73.5806	1.0000
	1kb	lena_1kb_master stego.bmp	0.0074	0.0074	69.4673	63.4620	1.0000
	10kB	lena_10kb_master stego.bmp	0.0679	0.0679	59.8148	53.8074	0.9999
	31kB	lena_31kb_master stego.bmp	0.2074	0.2074	54.9629	48.9505	0.9998
Hide’n’send	10B	lena_10b_hide.jpg	0.8512	16.2716	36.0165	30.0056	0.9878
	100B	lena_100b_hide.jpg	0.8516	16.3348	35.9997	29.9888	0.9877
	1kB	lena_1kb_hide.jpg	0.8536	16.8900	35.8545	29.8438	0.9873
	6,1kB	lena_6,1kb_hide.jpg	0.8641	19.9235	35.1371	29.1275	0.9852
Stegano	100B	Lena_100b_rgb_1младши бит.bmp	3.2471e-04	0.0003	83.0159	77.0108	1.0000
	100B	Lena_100b_rgb_2младши бита.bmp	2.6042e-04	0.0009	78.7644	72.7593	1.0000
	100B	Lena_100b_rgb_3младши бита.bmp	1.9938e-04	0.0026	74.0619	68.0568	1.0000
	100B	Lena_100b_r_3младши бита.bmp	2.0182e-04	0.0024	74.3599	68.3548	1.0000
	100B	Lena_100b_rg_3младши бита.bmp	2.0426e-04	0.0022	74.6212	68.6162	1.0000

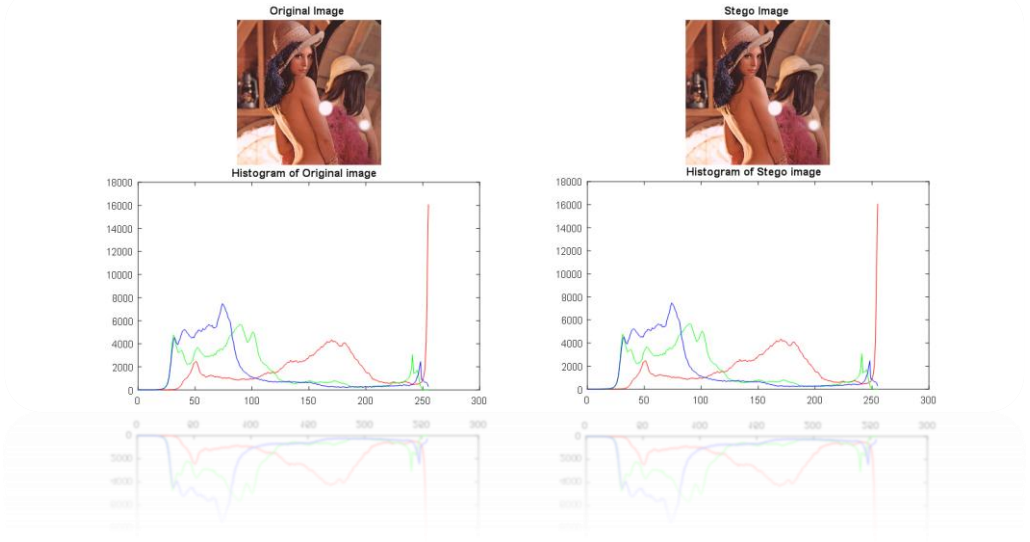
4.1. Хистограмни анализи.



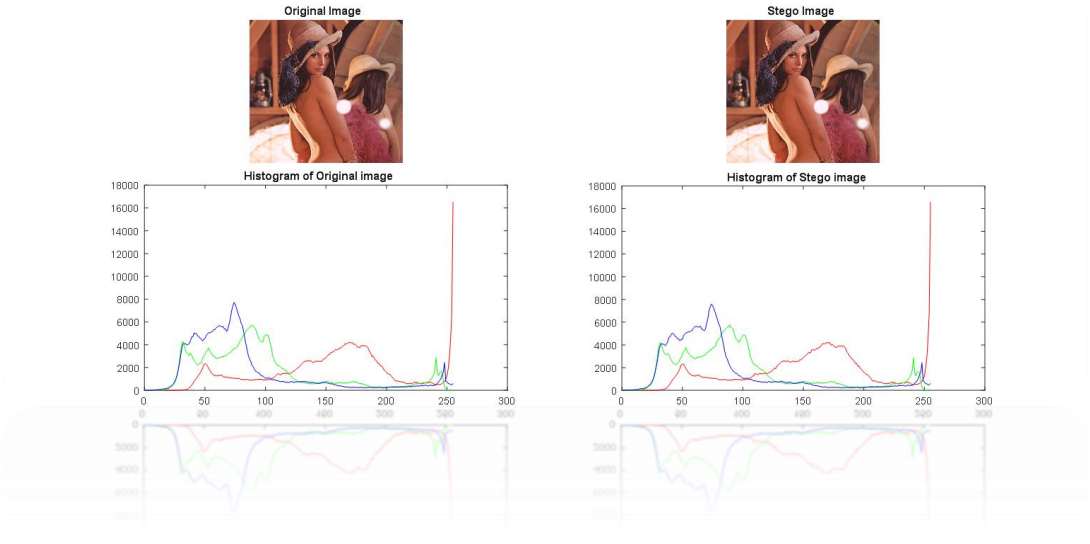
Фиг.*1 Хистограмен анализ (Lena.bmp,100b , Invisible secrets 4)*



***Фиг.**2 Хистограмен анализ (Lena.bmp,100b , Master Stego)*



***Фиг.**3 Хистограмен анализ (Lena.bmp,100b , Stegano)*



***Фиг.**4 Хистограмен анализ (Lena.bmp,100b , Hide’N’Send)*

Art. 4 - Acknowledgments

В заключение може да се каже, че дори безплатно разпространяваните стеганографски приложения за предаване на конфиденциални данни са достатъчно надеждни и сигурни, за да може да се обменя важна информация, без да се буди подозрение в страничния наблюдател. Препоръчително е те да бъдат сменяни периодично, с цел избягване на стеганализиращите програми. Благодарение на направените изследвания могат да се направят следните изводи за работата на стеганографските системи и да се определят препоръчителни характеристики на използваните прикриващи обекти и конфиденциалните съобщения.

• При вграждане на еднакви по дължина съобщения на латиница в едно и също изображение получените стегоизображения в различните стеганографски системи имат сравнително малка разлика в стойностите на изследваните параметри. Тази закономерност е в полза на изображенията създадени, с помощта на българските стеганографските системи. Но при вграждане на големи по дължина съобщения показанията са в полза на Invisible secrets 4;

• Установено е, че с повишаване на размера на вгражданите данни статистическите характеристики на изображенията се влошават, макар че визуалното качество, се запазва отлично. Това може да доведе до препоръка да се крият и предават данни в малки обеми;

• Хистограмният анализ позволява с просто око да се забележат съществения различия в червената цветова компонента при RGB цветовия модел на изследваните двойки изображения, както и в зелената и синята компонента.

References:

[1] Държавна комисия по сигурността на информацията първоначално обучение сборник лекции (второ допълнено издание) софия, 2015.
[2] Tasheva A., Zh. Tasheva, and Pl. Nakov. 2017. Image Based Steganography Using Modified LSB Insertion Method with Contrast Stretching. In Proceedings of the 18th International Conference on Computer Systems and Technologies (CompSysTech'17ACM, New York, NY, USA, 233-240.
[3] P. Mohan Kumar and K. L. Shanmuganathan,” Developing a Secure Image Steganographic System Using TPVD Adaptive LSB Matching Revisited Algorithm for Maximizing the Embedding Rate”, Journal of Telecommunications and Information Technology, 2/2011
[4] В. Стоянова, „Скриване на информация в изображения “, Монография, Шумен 2017г.
[5] „Spread Spectrum Image Steganography “Lisa M. Marvel, Member, IEEE, Charles G. Boncelet, Jr., Member, IEEE, and Charles T. Retter, Member, IEEE, VOL. 8, NO. 8, AUGUST 1999
[6] Павлова, Ст., Ст. Чанев, Сигурност на данните чрез използване на LSB стеганография и шифърът на Виженер в Андроид устройства, II International Scientific Conference CONFSEC, Borovec, 2018, year 2, issue 2(4), issn print 2603-2945, issn online 2603-2953
[7] Jit Lim (14 December 2010). "Is BER the bit error ratio or the bit error rate?". EDN. Retrieved 2015-02-16
[8] Stoyanova, V., Steganography System that uses the LSB method of embedding information in images, International Scientific Conference, Defense Technology forum 2015, Shumen, pp.186-193, ISSN 2367-7902, http://www.aadcf.nvu.bg/scientific_events/papers/NS_2015.
[9] Stoyanova V., Possibilities of steganography methods for hiding data based on Discrete Cosinus Transformation, international Scientific Conference Science. Education. Innovation, May 2014, Shumen. T. 1-2.Shumen: “Konstantin Preslavsky ”Univ. Press, 2014, ISBN 978-954-577-969-5.
[10] Камарашев, Г., С.Димитрова, Aspects of defence and security resource allocattion, Sibiu 2007
[11] Атанасов, А., Щ. Стоянова, Анализ на мрежовата стеганография, II International Scientific Conference CONFSEC, Borovec, 2018, YEAR 2, ISSUE 2(4), ISSN Print 2603-2945