УДК 004 **Информационные технологии**

Нагиева Абабил Фахраддин гызы, *старший преподаватель,*

Кафедра компьютерной инженерии и телекоммуникаций, Азербайджанский Технологический Университет, Гянджа, Азербайджан

НАБЛЮДЕНИЕ ЗА МЕТОДАМИ СОКРЫТИЯ ДАННЫХ, ИСПОЛЬЗУЕМЫМИ В СТЕГАНОГРАФИИ ИЗОБРАЖЕНИЙ
OBSERVE OF DATA HIDING TECHNIQUES USED IN IMAGE STEGANOGRAPHY

Аннотация: Стеганография – это искусство передачи секретного сообщения в электронный носитель информации, не вызывая подозрений относительно наличия скрытой информации третьей стороны. В этой статье мы сосредоточились на методах стеганографии изображений, основанных на интерполяции изображений. На основе обзора литературы по тематике статьи предпринята попытка обеспечить теоретическую основу исследования для разработки новых, более эффективных алгоритмов обратимой стеганографии на основе интерполяции изображений, оценить уровень развития темы, обосновать выбор направления дальнейших исследований.

Ключевые слова: Обзор литературы, Стеганографическая система, концепция стеганографических систем, сокрытие данных, интерполяция изображений, оценка критериев, сравнение эффективности алгоритмов.

Abstract: Steganography is the art of transmitting a secret message in an electronic carrier of information without causing suspicion concerning the presence of hidden information of a third party. In this paper, we focused on image steganography methods based in image interpolation. Based on a survey of the literature on the subject of the article, an attempt is made to provide a theoretical basis for research to develop new, more efficient reversible steganography algorithms on image-based interpolation, assess the level of development of the topic, justify the choice of the direction of further research.

Keywords: Literature review, Steganography system, concept of steganography systems, data hiding, image interpolation, criteria evaluation, algorithms efficiency comparison.

Introduction

The increased flow of digital communications, via the Internet and other networks, requires special attention to the security of the transmitted information to avoid unauthorized access to the communication channels. In this regard, the development of new methods of concealment is very relevant.

For this purpose, cryptography and data hiding techniques are used. So that each of them has self-specific characteristics and objectives. Unlike cryptography, the purpose of which is to conceal a secret message by encryption, steganography is to disguise the very fact of transmitting a secret message. Steganography is the science of concealing a secret message in any form, leaving no visible traces on the medium. Depending on the relationship between embedded secret messages and the host media, data hiding techniques are classified into steganography and watermark techniques [8; 21; 35]. The major goal of steganography is to enhance communication security by embedding a secret message into the digital image vs. copyright control, authentication and robustness are objectives of watermark techniques. For more details on the difference between steganography and watermark techniques please refer to [7].

Concept of steganography system

As a scientific direction, digital steganography has been formed recently, so its terminology has not been fully established. The most important concepts of steganography were identified in the spring of 1996 at the first International Concealment Conference - Information Seminar on Concealment of Information, Cambridge [45] and in April 1998, in Portland, US.

The steganography system (stego-system) is a set of methods and tools that ensure the transmission of private information through open communication channels. The main purpose of the steganography process is not to encrypt data, but to ensure that embedded data transmits unnoticed, intact and recoverable. The scheme of the steganography system and its basic operations are shown in Figure 1.

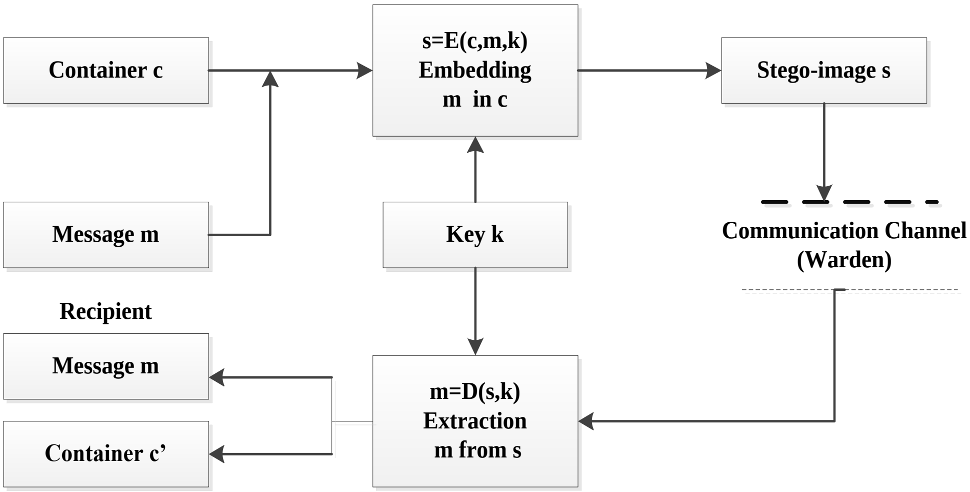

Fig. 1. Basic operations in the steganography system

-The term Container (Cover Image) denotes any digital media that is used to hide a secret message.

-Message is secret data transmitted, which may be text or image.

-Stego-image is an Image with embedded secret message.

- is a phase of insertion secret message into a cover image.

- is a phase of extraction secret message m from stego image.

- digital key to encrypt the secret message before it can be inserted into the Cover Image.

-The Communication channel is the channel through which the Stego container is transmitted, which is monitored by the warden (attacker).

-Container is a Stego Image after extraction of secret message.

A stego-system in which, cover image is not required to extract a secret message is called a blind stego-system. Attacking phases that may be performed by a warden, when he feels something unusual in the communication channel. The tasks performed by the warden depend on the type of warden. A warden can be passive or active. The goal of a passive warden is to reveal the existence of a hidden message in the transmitted file. The goal of an active warden is to decrypt, destroy, or at least damage a hidden message. 3. Evaluation criteria of steganography system

Steganography systems are assessed against the three main criteria described below: image fidelity, payload and security level [35]. At all stages of the development of stenographic algorithms, it is necessary to evaluate the efficiency of different phases of algorithms functioning. In the scientific literature, there are different types ofimage similarity metrics for measuring the visual quality of images such as the Square Mean Error (MSE), the Signal Peak to Noise Ratio (PSNR), and the Cross-Correlation (CC), Structural Similarity Index Metric (SSIM) and others are used to measure the difference between cover and stego images more accurately. A detailed description of the existing methods with their formula is given in [26]. The PSNR shall be calculated as follows:

$$PSNR = 10\log_2 \frac{Max^2}{MSE} dB \tag{4}$$

$$MSE = \frac{1}{(M \times N)^2} \sum_{i=1}^{M} \sum_{j=1}^{N} \left(C_{ij} - S_{ij}\right)^2 \tag{5}$$

where denotes the maximum pixel value of the image. A higher value indicates the better quality of steganography algorithm. HVS is unable to distinguish the images with PSNR more than 36 dB [35].

SSİM calculated by formula

$$SSIM = \left(\frac{(2 \times C \times S + K1)(2 \times M_{CS} + K2)}{\left(M^2{}_C - M^2{}_S + K2\right)^2 \times (C)^2 + (S)^2 + K1} \right) \tag{6}$$

Where C and S are the mean of pixel in image C and S and Ms are the computed variance of all pixel in both C and S images, Ms is the co-variance between both C and S and K1 and K2 are the constants.

SSIM is usually used to determine the similarity of two compared images. It varies between 0 and 1. The closer this value is to 1, the better the visual quality of the stego image, and both images look similar. A comparison of PSNR and SSIM methods with the same capacity values is presented in [33].The data was embedded into medical images.(Table 1.) .As can be seen from Tab.1, both methods exhibit the same degree of similarity.

Table 1. Images identity evaluation metrics

Image	Capacity (bits)	PSNR (dB)	SSIM
Med 1	641,252	34.3521	0.9628
Med2	640,126	35.2874	0.9745
Med 3	643,204	34.0269	0.9662
Med 4	642,262	36.5412	0.9788
Med 5	641,076	35.0145	0.9721
Med 6	643,196	34.1721	0.9601

This means that there is no contradiction between the two methods and they can be used with equal success in each case. At the same time, the coincidence of the results of the two metrics increases the reliability of the obtained experimental data. All these techniques have some distinctive features and can be used in all kinds of specific cases.

Classification of steganography methods.

Steganography methods can be classified mainly into the following categories

Steganography by cover selection

The possibility of choosing cover images is an indisputable advantage of the steganography method of concealment of information.

In these methods, the sender must select a suitable cover image from the image base and then insert a secret message into it. Because choosing a suitable cover image has a significant impact on the reliability of the steganography system and the ability of the algorithm to detect the presence of hidden messages. The size of the container directly affects the bandwidth of the steganography data channel [38].

Hansi S. Subhedar [21] claimed that embedding of secret message in chosen cover image will enhance system performance and as a result more secured steganography.

Kermani [15] was first introduced the cover selection technique for hiding a secret message in cover image. This algorithm uses the image texture similarity effect where some blocks of the cover image are rearranged by similar blocks of the secret image The results of the comparison of the secret image's and the cover image's blocks allow to select of the most suitable image to be used as a container for the embedding of the secret message. They have also proposed algorithms by using statistical features of image blocks and their neighborhoods to improve Kermani algorithms. The emergence of virtual edges and corners in the rearranged blocks is eliminated by the use of the block's neighborhood information.

Sadkhan [34] proposed a system of agents allowing the sender to select the most appropriate cover image from the image base, which is based on the statistical characteristics of the selected image. After picking up an image from the database of the image, the agent system computes some specific image parameters as histogram, mean, standard deviation, and entropy and makes a decision or a choice. Using a system of steganography agents, the images that have the largest dispersion, high entropy, and greatest contrast are detected.

Steganography by cover generation

The method of cover generation differs from other steganography methods in that it does not require the use of a real existing cover image, and the cover image is generated by the stegosystem itself. Many cover generation techniques [31; 28; 30] are developed, where has introduced detailed and systematized description of the theory and algorithms of cover generation, proposed efficient and stable generation methods. Ritchie, Philip Carson, [31] presented a wide overview of container generation methods. The methods of container generation are highly resistant to steganalytic attacks. The generated cover must be being able to recover the hidden bits of information in other words it can be reversible.

Steganography by cover modification

In these methods, the sender is modified the pixels of the cover image embedded secret bits of messages. Methods of steganography by modifying the cover image are divided into methods of embedding in the spatial and frequency domain. In each of these classifications can be dynamics and adaptive methods. Dynamic methods are message bit dependent whereas adaptive methods are based on image statistical features [9]. This study devoted to spatial domain issues; therefore, it is necessary to high mention relevant methods in this domain.

Spatial domain techniques

In spatial domain techniques, the secret message bits are embedded directly into pixels of the cover image or their interconnection. This method is very simple and is convenient in utilization, provides a large amount of payload, and allows control of the quality of the stego-image. The Least Significant Bits (LSB) method is often used to hide a message in a spatial domain. In this method, the 8th bit of every pixel of the cover image is substituted by one bit of a secret message, at this rate, the pixel value may change hardly by one bit of secret message, at this rate, the pixel value may change hardly by. Instead of embedding a fixed volume of secret messages in the LSBs of each pixel, most existing approaches use pseudo-random generator to select embedding domain and K bits of LSB. At this time the embedding rate increases.Based on spatial domain-oriented data hiding methods many algorithms [4; 16; 39] have been developed and successfully used in different areas of steganography, among which the method PVD (Pixel Value Difference) can be highlighted. Wu and Cai [41] discovered that pixels that are located in the areas of the edges can withstand more changes than those which are in the smooth areas therefore, proposed a steganography algorithm based on pixel value differencing The cover image is divided into non-overlapping blocks consisting of two consecutive pixels. . This method takes into account the difference in values of the blocks used. Zhang and Wang [43] demonstrated that a loophole exists in the PVD method and steganalyst can even estimate the length of hidden bits from the histogram the use of this method in image-based interpolation algorithms yields good results.

Conclusion

This paper has presented an universal survey of steganography methods in the spatial domain. The basic difference between the objective of cryptography, steganography, and watermarking was discussed.

The steganography system with its methods and tools was presented and special attention was given to image steganography in the spatial domain. In addition to the above mentioned the most commonly used performance for evaluating steganography and steganaysis algorithms were discussed.

Библиографический список:

1. Cox, I. J. Kilian, J. Leighton, F. T. and T. Shamoon. - Secure spread spectrum watermarking for multimedia IEEE Transactions on Image Processing, Vol. 6, 1997, No. 12, pp.1673–1687.

2. Lisa, M., Charles, B. and R. Charles. Spread spectrum image steganography. - IEEE Transactions on Image Processing, Vol. 8, 1999, No. 8, pp. 1075–1083.

3. Seyyedi, S.A., R.K. Sadykhov. Digital Image Steganography Concept and Evaluation. - International Journal of Computer Applications, vol. 66, 2013, No. 5, pp.17–23.

4. Chandramonli, R., Kharrazi, M., N. Memon. Image Steganography and Steganalysis Digital Watermark. - Lecture notes in Computer Science. Vol. 2939, 2003. pp. 35-49.

5. Zaker, N., A. Hamzeh. A novel steganalysis for TPVD steganography method based on differences of pixel difference histogram. - Multimedia Tools and Applications, Vol. 58, 2012, No 4. pp. 147-166.

6. Seyyedi, S.A., Sadau, V., N. Ivanov. A Secure Steganography Method Based on Integer Lifting Wavelet Transform. - International Journal of Network Security, vol.18, 2016, No 1, pp.124-132.

7. Li, B. He, J. Jiwu, H., Y. Q. Shi. A Survey on Image Steganography and steqanalysis. - Journal of Information Hiding and Multimedia Signal Processing, Vol. 2, 2011, No. 2, pp.142-172.

8. Lee, C-F., Huang, Y-L.-An efficient image interpolation increasing payload in reversible data hiding. - Expert System Application, vol. 39, 2012, No 8, pp. 6712-6721.

9. Sabeen, G.P.V., Judy, M.V. A secure framework for remote diagnosis in health care: A high capacity reversible data hiding technique for medical images.- Computers and Electrical Engineering, Elsevier, Vol. 89, 2021, No 4, pp. 2303-2317.ue University, 2015, pp.549/

10. Sadkhan, S.B. Al-Barky, A.M. and N.N. Muhammad. An Agent based Image Steganography using Information Theoretic Parameters. - MASAUM Journal of Computing, Vol. 1, 2009 No. 2, pp. 258-264.