9. Sheluhin O.I., Osin A.V., Smol’skij S.M. Self-Similarity and Fractals. *Telecommunication Applications*. Moscow: Fizmatlit, 2008, 368 p. (In Russ.)
10. Kartashevskiy I., Buranova M. Calculation of Packet Jitter for Correlated Traffic. *Lecture Notes in Computer Science*, 2019, vol. 11660, pp. 610–620. DOI: https://doi.org/10.1007/978-3-030-30859-9_53
11. Conolly B.W., Choo Q.H. The waiting time process for a generalized correlated queue with exponential demand and service. *SIAM Journal on Applied Mathematics*, 1979, no. 37 (2), pp. 263–275.
12. Hadidi N. Queues with partial correlation. *SIAM Journal on Applied Mathematics*, 1981, no. 40 (3), pp. 467–475.
13. Hadidi N. Further results on queues with partial correlation. *Operations Research*, 1985, no. 33, pp. 203–209.
14. Langaris C. Busy-period analysis of a correlated queue with exponential demand and service. *Journal of Applied Probability*, 1987, no. 24, pp. 476–485.
15. Langaris C. A correlated queue with innitely many servers. Journal of Applied Probability, 1986, no. 23, pp. 155–165.
16. Kartashevskij I.V. Use of copulas in statistical analysis of telecommunication traffic. *Infokommunikacionnye tehnologii*, 2016, vol. 14, no. 4, pp. 405–412. (In Russ.)
17. Fantatstsini D. Modeling multivariate distributions using copula functions. *Prikladnaja ekonometrika*, 2011, no. 3 (23), pp. 98–132. (In Russ.)
18. Farlie D.G.J. The performance of some correlation coefficients for a general bivariate distribution. *Biometrika*, 1960, no. 47, pp. 307–323.
19. Gumbel E.J. Bivariate exponential distributions. *Journal of the American Statistical Association*, 1960, no. 55, pp. 698–707.
20. Morgenstern D. Einfache Beispiele zweidimensionaler Verteilungen. *Mitteilungsblatt für Mathematische Statistik*, 1956, no. 8, pp. 234–235.
21. Penikas G.I. Copula models as applied to finance problems. *Zhurnal novoj ekonomicheskoj assotsiatsii*, 2010, no. 7 (7), pp. 24–44. (In Russ.)

Reseived 04.12.2020

ТЕХНОЛОГИИ КОМПЬЮТЕРНЫХ СИСТЕМ И СЕТЕЙ

УДК 004.056

A BRIEF OVERVIEW OF DATA HIDING METHODS IN DIGITAL IMAGES

Verdiyev S.G., Naghiyeva A.F.
Azerbaijan Technological University, Ganja, Azerbaijan Republic
E-mail: info_tel@inbox.ru

The Internet and wireless communications have created new opportunities for the mass exchange of multimedia information. This has created new challenges in terms of the security and storage of the information transmitted through global and local networks. This article is devoted to the study of steganography methods of safety, in particular, those based on LSB concealment, in the spatial area of digital images. The classification of steganography methods has given based on the works of the last 5 years. The most popular and widespread image steganography methods have been investigated, describing their merits and challenges. The most commonly used terminology was identified and various methods of data concealment are presented. The visual and statistical steganalysis methods for computing the statistical difference between the input image and the stegoimage is also considered. The article may be useful to researchers in developing new, more effective steganography methods of information hiding.

Keywords: *information security, steganography, information hiding, image steganography, steganalysis*

Introduction

Two decades of our century is characterized by increasing the number of digital cameras and devises of mobile communication and accordingly flow of information circulated over the Internet in the shape of multimedia. Recently developed and implemented worldwide, nets, software, and devices have enhanced the ability of users to access multimedia sources globally. This in turn, has increased the interest of the attackers in detecting and using the transmitted over public communication channels secret data. Thus, the growing role of scientific research aimed at ensuring the reliability of information systems, i.e. information security, is evident.

Cryptography, steganography and watermarking methods have been developed and used for this purpose. When using Cryptography, a secret message is encrypted and sends via an open communication network to the recipient of the message. In this case, the eavesdropper may detect the presence of the message but cannot read the encrypted information. When using Steganography, a secret message is hidden in a certain media domain [12]. The intruder does not know or suspects the existence of a secret message.

The watermarking technique, like steganography, is another way of concealing data and is used to protect copyrights, medical images, military purposes, and others. In contrast steganography the presence of hidden information may be known at the watermarking method [2]. Ideally, the purpose of watermarks is to make the removal/manipulate hidden information impossible.

Various multimedia media have contributed to the development of many different concealment technologies for information security. Information security means preventing an attacker from detecting the presence of hidden information. The concealment and transmission of data take place in verbatim systems.

When designing stegosystems, the most important issue is to ensure that safety criteria are properly developed. The main purpose of this article is to study these criteria for creating novel steganographic systems with higher attack resistance and payload capacity.

Steganography

Steganography is a new branch of science used to hide data [23; 27], preferable to cryptography and watermarking, because it securely hides communication, and no one can know about the presence of hidden data other than the sender and the receiver. Simply put, steganography is invisible communication. The word steganography has the Greek origin stegano (securely) and graphics (writing).

Ancient Greeks used primitive elements of steganography, but computer steganography is now used, consisting of many branches. Secret information is hidden in various multimedia media, the so-called containers. There are many unused spaces in the container that are convenient to insert a secret message.

Once the message is inserted into these spaces, the container is sent to the recipient and the data must be invisible to a third party. You can hide information in any part of the container, but some spaces are more convenient for data hiding.

There are different types of steganography dependent on the cover medium [23; 27].

1. Text steganography. Under this approach, hidden data are embedded in a text document.

2. Image Steganography. Classified information is hidden in an image because it has a large amount of information space to hide a secret message.

3. Audio steganography. This type of steganography hides a secret message in a sound document.

4. Video steganography. In implementing this method, M4, MPEG, AVI video documents are used to hide data.

5. Network or protocol steganography: In this case, the secret message is hidden by adopting a network protocol such as TCP, UDP, ICMR, IP, etc.

Sufficiently noteworthy scientific works from different countries devoted to digital steganography and its part of the image steganography is performed [1]. Abbas Cheddad et al. published in 2009 a review of steganographic methods developed by that time, their features, and their effectiveness. This was a serious analytic work that attracted the attention of experts in the field of information hiding. Steganographic methods developed up to 2009 have been analyzed and systematized. Based on this systematization, some recommendations were made regarding the object-oriented embedding mechanism. The innovative secret communication technologies developed over decades have become an independent scientific field and, according to the authors' classification [1], looks like Figure 1.

Cheddad. A., et al [1] are made comparison of methods of steganography, watermarking, and cryptography, including modern and popular methods of data hiding, such as spatial and frequency domain, adaptive steganography, and others. All these considerations are accompanied by comprehensive illustrative material and their explanations.

All aspects and drawbacks of the methods discussed were also considered. In general, this work of the authors can be estimated as a very successful survey of concealment techniques.

Another equally appealing and comprehensive review by Mehdi Hussein et al. was devoted to steganography [13]. According to their critical opinion, Cheddad et al. published their article in 2009, and therefore it does not contain the achievements of the last six years. At the same time, Cheddad A. et al. classification of image steganography is limited by spatial and transform domain, adaptive technics. They, therefore, presented new, more comprehensive observations on the spatial domain method, which differs from the Cheddada article and others a new classification concerning the embedding of the domain, the types of encryption of the classified information, the format of the images. Each of the methods proposed in the literature has its weaknesses and strengths, as well as its scope of application. If in the earliest publications [3; 4; 9–11; 14–16; 21; 24] Special attention was paid to increasing of payload hidden information, the recent work shows a tendency to develop algorithms with a higher level of security. It follows from the literature that there is no one-size-fits-all method of steganography for all cases of concealment. Each method used has its peculiarities. For example, using the LSB-based spatial domain method makes it possible to hide a large amount of information, is characterized by the ease of implementation, and the possibility of combining with different methods. But at the same time, the higher the payload capacity, the more distorted the image is. While PVD is characterized by more degree of security.

Application of steganography:

– Covert communication and secret data concealing;

– Digital watermarking;

– E-commerce;

– Protection of stored data alteration;

– Media;

– Database system [20].

The terms most commonly used in steganography:

1. Stegosystem – the set of necessary software and devices to implement the secret communication.

2. Embedding – the operation of inserting a secret message into a container.

3. Cover Image – Input Image for Data Embedding.

4. Capacity is the amount of information that can be inserted into cover image without much distortion.

5. Stego image – Input Image with embedded data.

6. Secret message or payload – message to be transmitted via an open channel of communication.

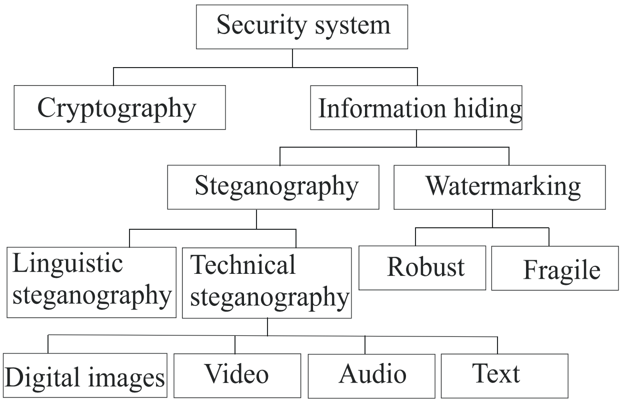

Figure 1. Classification of information security systems

7. Embedding distortion – is a distortion that appears in a stegoimage as a result of data hiding.

8. Robustness – the ability of the stegosystem to protect the contents of stegoimage.

9. Extraction is an operation to extract an embedded secret message from stegoimage.

Image investigation using MATLAB

At the time of researching and designing steganographic algorithms, the most convenient and effective tool is MATLAB [23; 14] which allows focusing on the data hiding algorithm itself. At this time, you don't have to waste time opening a file, recognizing its format, putting an image on the screen. MATLAB allows you to visualize an image directly in the form of a matrix, perform bit operations (AND, OR, XOR, …, etc.), and much more. Using these conveniences and the capabilities of MATLAB, it is possible to perform all kinds of manipulations with digital images.

Image steganography

The last decades have been characterized by the wide implementation of digital cameras and high-speed internet transmissions and connected with that world wide circulated huge flows of data on the shape of an image.

A big part of the global population is connected over e-mail and social sets and their applications as a messenger, Whats App, Instagram. Most of those connections are accompanied by images. That's the reason why image steganography has so rapid development and implementation accordingly.

The most popular and well-known steganography techniques are the new directions of steganography. Image Steganography is the science and art of concealing data in digital images to ensure secret communication [1; 13; 15] Due to its advantages, image steganography became more popular than other methods The digital image in a image steganography is called a container and plays the role of a hidden

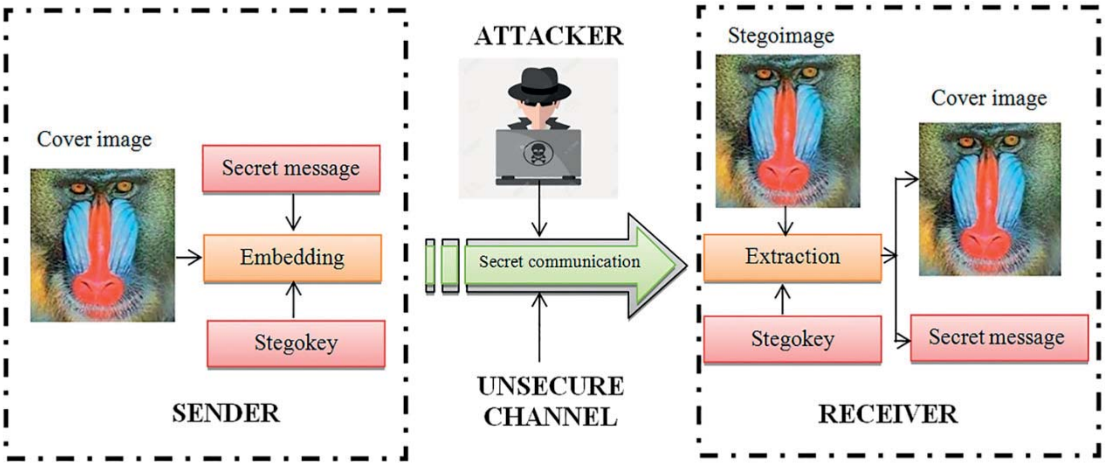

Figure 2. The principal scheme of the reversible steganography system

Table. Image embedding algorithms assessment

Measures	Advantage	Disadvantage
High Capacity	High	Low
Perceptual transparency	High	Low
Robustness	High	Low
Temper resistance	High	Low
Computation Complexity	Low	High

information carrier. The container must be selected correctly since the reliability of the stegosystem depends on the characteristics of the image [8; 11]. Therefore, steganographic methods for the selection of digital images were develop [9; 10; 24].

For this purpose, the statistical characteristics of the different images are compared and the those samples that provide a higher quality of stegoimage, the larger payload, a better indicators of imperceptibility, high security are selected. Various preliminary container improvement technologies are available. One of them is image interpolation technic [4; 6; 17].

Image steganography techniques

Image steganography is a way of hiding information in a digital image so that it becomes a steganographic image. The image is then transmitted through an open channel of public communication to the recipient of the information. If the third party (the attacker) interested in the information transmitted does not know and does not suspect the presence of the hidden information, the communication system is considered to be of high quality [20; 5; 18]. The algorithms for hiding data are reversible and irreversible. In the first case, depending on the type of algorithm used, the recipient of the secret message can retrieve the message with or without a stegokey. During the use of irreversible algorithms, it is not possible to extract a secret message.

The principal scheme of the reversible steganography system is shown in Figure 2.

Steganography image algorithms differ from each other in their characteristics given in Table. For example, after the embedding of a large amount of secret information into the cover image, the visual quality of the stegoimage deteriorates compared to the container. The amount of distorting between of the stegoimage and the container determines the quality of the secret information embedding algorithm used. Similarly assessed other characteristics of steganography algorithms in the process of which verbal terms of type High or Low are used. An example of this evaluation is given in Table [11].

In [20; 18] authors gave an overview of the most popular steganography methods in the field of digital images and discussed important techniques concerning exploiting image formats into the two categories, Figure 3. Image steganography techniques can be divided into two subdivision:

1. Image (spatial) domain.
2. Transform (frequency) domain.

Following the classification of Mehdi Hussain et al. [13] spatial domain techniques are looking as listed below:

1. List Significant Bits (LSB).
2. Pixel Value Difference (PVD).
3. Exploiting Modification Direction (EMD).
4. Multi-Base Notation System (MBNS).
5. Pixel Pair Matching (PPM).

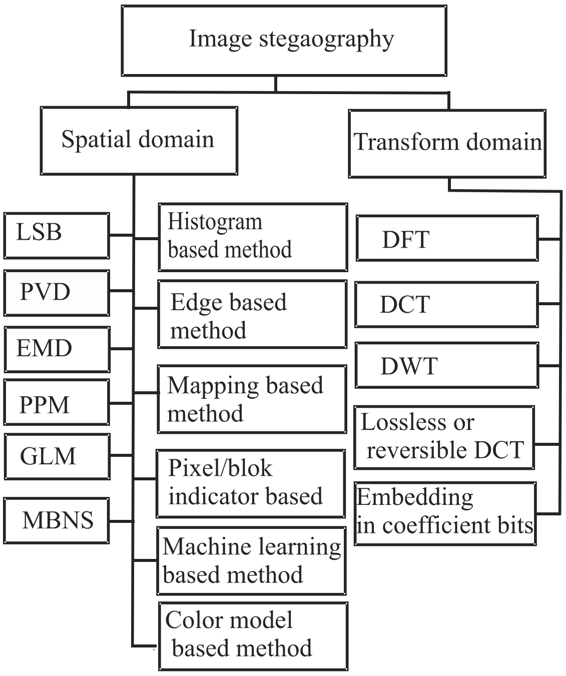

Figure 3. Scheme of image steganography classification

6. Gray Level Modification (GLM).
7. Pixel Value Prediction (PVD).
8. Histogram based methods.
9. Edge-based methods.
10. Mapping based methods.
11. Pixel/block indicator base methods.
12. Color model-based methods.
13. Machine learning-based methods.

The methods of a spatial domain are characterized by the simplicity of the embedding of secret information into the cover image while it is possible to insert a greater amount of information. At the same time, a significant disadvantage is low robustness to stego attacks. Transform Domain techniques are classified [7; 25] as:

1. Discrete Fourier Transform Technique (DFT).
2. Discrete Cosine Transform Techniques (DCT).
3. Discrete Wavelet Transform Method (DWT).
4. Lossless or reversible method (DCT).
5. Embedding in coefficient bits.

The merit of methods of embedding information into the frequency domain is the most greater resistance to stego attacks. The disadvantage is the complexity of the algorithms and the lower payload capacity compared to the spatial domain methods.

List of significant bits (LSB)

There are many methods for concealing information in an image. Secret information can be hidden in sequential or randomly selected image pixels. Typically, noisy image space is ideal for data hiding because most pixels on the noisy parts of the image have different colors during embedding.

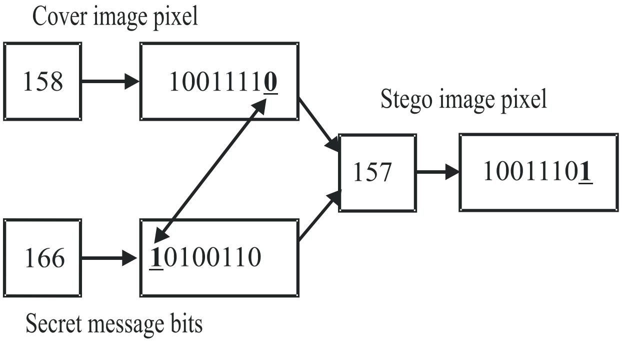

Figure 4. A model of cover image pixel value calculation (replaced secret message bit value is 1)

Therefore, the probable small distortions do not hurt the image and are invisible to the human eye. The LSB method implementation is based on the replacement of LSB bits of the image with secret information bits.

Implementation of the LSB method using different algorithms it is possible to identify the bits to be modified [23; 13]. The container capacity and the visual quality of the stegoimage depend on the format of the digital image [8; 22]. The following image formats are used to select the containers:

1. BMP – Point Map.
2 .GIF – Graphical Data Interchange Format.
3. TİFF – Tagged Image File Format.
4. PNG – Portable Network Graphics.
5. JPEG – Joint Photographic Experts Group.

The basic concept of LSB substitution is shown in Figure 4. According to this concept, the last bits in a sequence of bits can be evaluated as less significant. If these bits are replaced by bits of secret information, the distortions in the stego image are very small. It is possible to replace all pixels in the sequence of bits of the stegoimage, but usually, two pixels [23; 5] are used for hiding.

If the value of the bit of the hidden image in the cover image is 1, then the value of this pixel increases or decreases (+/-1). If the value of the hidden secret message bit is 0, no change will occur.

Suppose pixel value of the cover image is 158, and in the binary system it is 10011110 (Figure 4.) and the bit value of the hidden secret message is 1 and during the embedding fixed as (+/–1) then the pixel value of the cover image increases to + 1 and becomes 159 (originally 158) or value is equal to –1, this number becomes 157. In the other case, the cover image value is 175, and in the binary system it is 10101101. If the hidden secret message bit is 0, the cover image pixel value is unchanged see Figure 5.

LSB based steganography is an art of data hiding and in the same time fundamental direction of IT science which can hide an big amount of secret

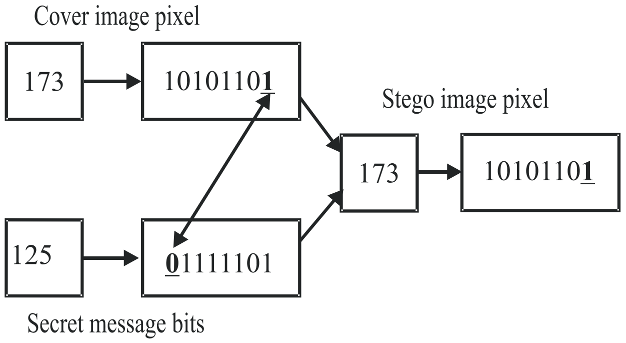

Figure 5.A model of cover image pixel value calculation (replaced secret message bit value is 0)

information. The selection for modification pixels of container image or sequence of their replacement is determined by stego key [23; 25].

Steganalysis

To study the efficiency of the developed steganographic algorithms, there exist specially developed and widely used methods of steganalysis which, as part of steganography, are steganographic attacks, i.e. a countermeasure against concealment methods [13; 4].

Steganalitic methods are divided into visual and statistical methods. In the first case, the presence of hidden information in the container is visually assessed by the expert. Although this method is simple but based on subjective data limited by human perception, the result is not very precise. Statistical methods of steganalis are based on more precise mathematical methods, and the results based on quantitative descriptions of statistical indicators are much more accurate [1; 4; 19].

To detect the presence of concealed information in a stegoimage, it is compared to the cover image. This comparison is made based on several objective indicators of the image. The several most popular indicators of interference assessment are known [7]. These are MSE, RMSE, PSNR, and NCC.

1. MSE (Mean Square Error) σ^2:

$$\sigma^2 = \frac{1}{M \times N} \sum_{i=1}^{M \times N} \left(P(i,j) - S(i,j) \right)^2, \qquad (1)$$

where $S(i,j)$ is cover pixel value; $P(i,j)$ – is stego image pixel value; $M \times N$ the height and width dimension of the cover image. If MSE value is estimated low it means the difference between cover and stego image very slightly.

2. PSNR (Peak Signal to Noise) measures the similarity of two images, i.e. how the matched images differ from each other

$$PSNR(dB) = 10 \log_{10} \frac{x_{peak}^2}{\sigma^2}, \qquad (2)$$

where $x_{peak} = 255$ here x is the max value of pixel vary on the range [0..255],

3. RMSE – measures the difference between these two images. Because the computation of these two metrics (PSNR and RMSE) is very simple and fast, they are widely used.

$$RMSE = \frac{1}{\left[M \times N \right]^R} \times$$
$$\times \sum_{i=1}^{M} \sum_{j=1}^{N} \left(X_{ij} - Y_{ij} \right)^2 \sum_{j=1}^{n} \left(X_i - \overline{X} \right)^2 \qquad (3)$$

where: N – is the number of lines in the cover image; M – is the number of columns in the cove image; $X_{i,j}$ – is the intensity of i,j pixels in the cover image; $Y_{i,j}$ – is the intensity of i,j pixels in the stego image.

4. NCC, Normalized cross-correlation is used to calculate the degree of similarity (or distinctiveness) between two analyzed images:

$$NNC = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} \left(x_{ij} \times y_{ij} \right)}{\sum_{i=1}^{M} \sum_{j=1}^{N} \left(x_{ij} \right)^2}. \qquad (4)$$

A more comprehensive listing and critical analysis of steganalysis methods are given by Dr. Rajkumar L. Biradar and Ambikea Umashetty [25] and Mehdi Hussaina et al [13].

In turn, statistic steganalysis methods are divided into dependent (specific) algorithms for embedding a secret message and independent (universal) methods that can be used for a wider range of embedding techniques discussed in this review. Steqanalytic techniques are used to detect the presence of a secret message in a stego container or to eliminate traces of the introduction of a secret message. In [13; 18; 26] is described in each method used to detect the transmission of a secret message. A comparative analysis of various steganalysis methods was made and their effectiveness was described. For example, Pallete image steganalysis, Raw image steganalysis, YPEQ image steganalysis.

Specific methods include Pairs of Values, RS, Chi-square analysis, and others which are focused on List Significant Bits methods. However, all these steganalysis methods are not very popular, cause the attacker does not know in advance which method of embedding was used to hide information. Binary Similarity Measures (BSM), Wavelet-Based Steganalysis, Feature-Based Steganalysis, etc. refer to the number of universal algorithms that detect hidden information [13; 26].

Let consider an example of calculating the difference between a container and a stego image.

Figure 6. Cover image Lena

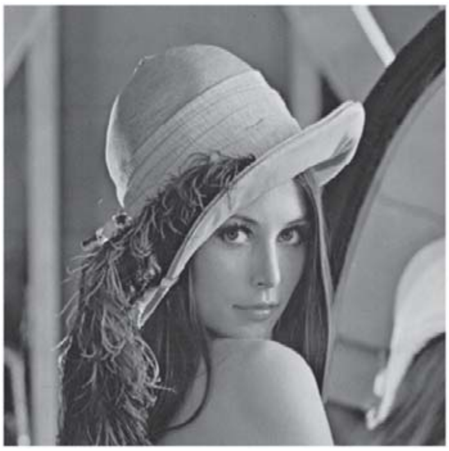

Figure 7. Stego image Lena

Figure 8. Cover image pepper

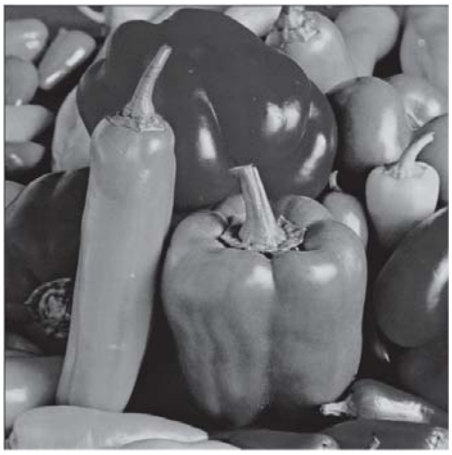

Figure 9. Stego image pepper

For this purpose PSNR method has used. Depending on the type of implemented embedding algorithm, the PSNR values may vary considerably. The result is also vary depending on the types of images. The quality of the used algorithm is determined by the value of the PSNR. The standard Lena image Figure 6 with the size 512x512, taken from the image database of Granada University (USA) has used. A secret message with a size 1x2097152 was embedded into the container. The PSNR was calculate by equation

$$PSNR\left(dB\right)=10\log_{10}\frac{255^2}{1.5229}=46.3041;$$

$$\sigma^2=\frac{1}{512\times512}\sum_{i=1}^{512\times512}\left(P\left(i,j\right)-S\left(i,j\right)\right)^2.$$

Calculations are carried out according to the corresponding program in the MATLAB. The initial image and the stego image are entered consecutively. Based on data from the stego image $P\left(i,j\right)$ and container $S\left(i,j\right)$ under formula (4), σ^2 is calculated. $M\times N$ is equally 512×512 the size of the images.

The result is very high, it means that the images being compared are almost the same Figure 6, Figure 7, Figure 6, shows the image of Lena on the cover image and Figure 7, shows the stegoimage. As can be seen from the visual comparison of the images there is no visible distortions or difference between them.

In the same way, was calculated PSNR for another standard pepper image Figure 8, Figure 9, the result is 47.36431

That shows that PSNR differs for each concrete image. In [10], a serious study was conducted of the algorithms developed by the authors for message embedding aimed at ensuring high reliability and invisibility while introducing as much secret information as possible. The methodology of the experiments carried out when 30 different digital images are used as a container is described. At that time, the maximum payload capacity of each of them was determined, which ensured that the system was sufficiently reliable, which ensured the high reliability of the stegosystem in terms of image quality and invisibility. Invisibility was measured against criteria such as MSE, PSNR, etc. The PSNR values for containers with different capacities were compared.

Conclusion

Based on many scientific publications, a literary review of steganographic methods of embedding secret information into digital images has been made with the priority work of recent years. During the review of these works, it became clear that most of them were published in 2009–2013 years and are mostly devoted to methods of embedding in the spatial domain, based on LSB. The weaknesses and strengths of the proposed methods have been examined.

Methods of estimating statistical characteristics of steganographic algorithms by steganalysis have been studied. From the large number of publications reviewed in this work, it can be seen that every year new and new steganographic methods are offered and this process is endless. And even though there's been a lot of success in concealing information in an image, there's still a lot of problems to solve.

Despite the obvious progress in image steganography, there are many problems in developing novel steganographic algorithms with a higher level of robustness by selecting more suitable stego containers and taking into account the features of the embedded information. A reasonable compromise must be found between the maximum possible payload capacity and the quality of the stego image. Here we have chosen and described those methods, which have interest in our further research on the development of a new method of embedding the message in the spatial domain using the LSB methodology, which must be characterized by a more accurate information embedding technique and a high level of safety.

References

1. Abbas C. et al. Digital image steganography: Survey and analysis of current methods. *Signal Processing*, 2010, vol. 90, no. 3, pp. 727–752.
2. Asifullah K., Sana A.M., Ayesha S. A recent survey of reversible watermarking techniques. *International Journal of Information Sciences*, 2014, pp. 251–272. DOI: https://doi.org/10.1016/j.ins.2014.03.118
3. Ahmad A.M., Ali A.H., Mahmoud F. An improved capacity data hiding technique based on image interpolation. *Multimedia Tools and Applications*, 2019, vol. 78, no. 6, pp. 7181–7205.
4. Li B. et al. A survey on image steganography and steqanalysis. *Journal of Information Hiding and Multimedia Signal Processing*, 2011, vol. 2, no. 2, pp. 142–172.
5. Chin N.Y., Shen C.H., Cheonshik K. Improving stego image quality in image interpolation based data hiding. *Computer Standards & Interfaces*, 2017, pp. 209–215. DOI: https://doi.org/10.1016/j.csi.2016.10.005
6. Rajkumar L.B., Ambika U. A survey paper on steganography techniques. *International Journal of Innovative Research in Computerand Communication Engineering*, 2016, vol. 4, no. 1, pp. 721–730. DOI: https://doi.org/10.15680/IJIRCCE.2016.0401158
7. Eltyeb E., Elgabar A. Comparison of LSB steganography in BMP and JPEG images. *International Journal of Soft Computing and Engineering*, 2013, vol. 3, no. 5, pp. 91–95.
8. Hedieh S., Mansour J. Evolutionary rule generation for signature-based cover selection steganography. *Computer and Information Technology Workshops: Proc. IEEE 8th International Conference on 2008*, 2008, pp. 379–384. DOI: https://doi.org/10.1109/CIT.2008
9. Jung K.H., Yoo K.Y. Data hiding method using image interpolation. *Comput Stand Interfaces*, 2009, vol. 31, no. 2, pp. 465–470.
10. Junying Y., Haishan C. Embedding suitability adaptive cover selection for image steganography. *International Conference on e Education, e-Business and Information Management (ICEEIM)*, 2014, pp. 36–39.
11. Kefa R. Steganography the art of hiding data. *Information Technology*, 2004, vol. 3, no. 3, pp. 245–269. DOI: https://doi.org/10.3923/itj.2004.245.269
12. Mehdi H. et al. Image steganography in spatial domain: A survey. *Signal Processing: Image Communication*, 2018, vol. 65, no. 3, pp. 46–66. DOI: https://doi.org/10.1016/j.image.2018.03.012
13. Manju N., Monika M. Steganography: The art of hiding text in image using Matlab. *International Journal of Advanced Research in Computer science*, 2013, vol. 4, no. 8, pp. 206–210. DOI: https://doi.org/10.26483/ijarcs.v4i8.1788
14. Mansi S.S., Vijay H.M. Current status and key issues in image steganography: A survey. *Computer Science Review*, 2014, vol. 13,

no. 14, pp. 95–113. DOI: https://doi.org/10.1016/j.cosrev.2014.09.001

15. Mansi S.S., Vijay H.M. Performance evaluation of image steganography based on cover selection and contourlet transform. *International Conference on Cloud & Ubiquitous Computing & Emerging Technologies*, India, Pune, 2014, pp. 231–236. DOI: https://doi.org/10.1109/CUBE.2013.39
16. Manasi J., Arpita M., Kankana D. A secure Image steganography using efficient map based LSB technique. *International Journal of Advanced Research in Computer Science and Software Engineering*, 2016, vol. 6, no. 3, pp. 657–660.
17. Mamta Y., Amita D. Image steganography techniques: A review. *International Journal for Innovative Research in Science & Technology*, 2015, vol. 2, no. 2, pp. 243–248.
18. Mehdi K., Husrev T.S., Nasir D.M. Performance study of common image steganography and steganalysis techniques. *Journal of Electronic Imaging*, 2006, vol. 15, no. 4, DOI: https://doi.org/10.1117/1.2400672
19. Nazinder K., Amanjot K. Art of steganography. *International Journal of Advanced Trends in Computer Applications*, 2017, vol. 4, no. 2, pp. 30–33. DOI: https://doi.org/10.1016/j.sigpro.2009.08.010
20. Johnson N.F., Jajodia S. Exploring steganography: Seeing the unseen. *IEEE Computer*, 1998, vol. 31, no. 2, pp. 26–34.
21. Nissar A., Mir A. Classification of steganalysis techniques: A study. *Digital Signal Processing*, 2010, vol. 20, no. 6, pp. 1758–1770. DOI: https://doi.org/10.1016/j.dsp.2010.02.003
22. Sheluhin O.I., Kanaev S.D. *Steganography. Algorithms and Software Implementation*. Moscow: Gorjachaja linija – Telekom, 2017, 592 p. (In Russ.)
23. Seyyedi S.A., Ivanov N. A novel secure steqanography method based on zero tree method. *International Journal of Advanced Studies in Computer Science and Engineering*, 2014, vol. 3, no. 3, pp. 1–9.
24. Shamsul K. et al. A steganographic technique for highly compressed JPG images. *Computer Science Review*, 2013, vol. 10, no. 5, pp. 107–118.
25. Sakit V. et al. An overview of steqanalysis methods. *Actual Multi-Disciplinary Scientific-Practical Problems of Information Security: Proceedings of the V Republican Conference*, Baku, 2019, pp. 204–206. (In Azerbaijani). DOI: https://doi.org/10.25045/NCInfoSec.2019.50
26. Verdiyev S.Q., Nagiyeva A.F. Experimental analysis of steganography. *Actual Multi-Disciplinary Scientific-Practical Problems of Information Security: Proceedings of the III Republican Conference*, Baku, 2017, pp. 51–55. (In Azerbaijani). DOI: https://doi.org/10.25045/NCInfoSec.2017.10

Received 20.11.2020

Sakit Gambai oglu Verdiyev, Azerbaijan Technological University, 103, Khatai Avenu, Ganja, AZ2011, Azerbaijan Republic; Professor, Head of Computer Engineering and Telecommunication Department, Doctor of Technical Science. Tel. +994 50 378-73-37. E-mail: info_tel@inbox.ru

Ababil Faxraddin gizi Nagiyeva, Azerbaijan Technological University, 103, Khatai Avenu, Ganja, AZ2011, Azerbaijan Republic; Doctoral Student of Computer Engineering and Telecommunication Department. Tel. +994 22 254-49-82. E-mail: nagiyevaababil@gmail.com

СОКРЫТИЕ ДАННЫХ В ЦИФРОВЫХ ИЗОБРАЖЕНИЯХ

Вердиев С.Г., Нагиева А.Ф.
Азербайджанский технологический университет, Гянджа, Республика Азербайджан
E-mail: info_tel@inbox.ru

Интернет и беспроводная коммуникация создают новые возможности для массового обмена мультимедийной информацией. Все это создает новые проблемы для хранения и передачи через глобальные и локальные сети информации. Настоящая статья посвящена изучению стеганографических методов безопасности, в частности основанной на методологии наименее существенных бит в пространственной области цифровых изображений. Приводится классификация стеганографических методов по данным публикаций последних 5 лет. Изучены наиболее широко распространенные и используемые методы стеганографии изображений с описанием их достоинств и недостатков. Дано определение наиболее используемых терминологий и рассмотрены различные методы сокрытия данных. Рассмотрены также стеганалитические методы расчета статистических разниц между входными изображениями и стегоизображениями.

Ключевые слова: *информационная безопасность, стеганография, сокрытие информации, стеганография изображений, стегоанализ*

DOI: 10.18469/ikt.2020.18.4.06

Вердиев Сакит Гамбай оглу, д.т.н., профессор, заведующий кафедрой компьютерной инженерии и телекоммуникаций (КИТ) Азербайджанского технологического университета (АзТИ). AZ2011, Республика Азербайджан, г. Гянджа, проспект Хатаи, 103. Тел. +994 50 378-73-37. E-mail: Info_tel@inbox

Нагиева Абабил Фахраддин гызы, докторант кафедры КИТ АзТИ. AZ2011, Республика Азербайджан, г. Гянджа, проспект Хатаи, 103. Тел. +994 22 254-49-82. E-mail: nagiyevaababil@gmail.com

Литература

1. Digital image steganography: Survey and analysis of current methods / C. Abbas [et al.] // Signal Processing. 2010. Vol. 90, no. 3. P. 727–752.
2. Asifullah K., Sana A.M., Ayesha S. A recent survey of reversible watermarking techniques // International Journal of Information Sciences. 2014. P. 251–272. DOI: https://doi.org/10.1016/j.ins.2014.03.118
3. Ahmad A.M., Ali A.H., Mahmoud F. An improved capacity data hiding technique based on image interpolation // Multimedia Tools and Applications. 2019. Vol. 78, no. 6. P. 7181–7205.
4. A survey on image steganography and steqanalysis / B. Li [et al.] // Journal of Information Hiding and Multimedia Signal Processing. 2011. Vol. 2, no. 2. P. 142–172.
5. Chin N.Y., Shen C.H., Cheonshik K. Improving stego image quality in image interpolation based data hiding // Computer Standards & Interfaces. 2017. P. 209–215. DOI: https://doi.org/10.1016/j.csi.2016.10.005
6. Rajkumar L.B., Ambika U. A survey paper on steganography techniques // International Journal of Innovative Research in Computerand Communication Engineering. 2016. Vol. 4, no. 1. P. 721–730. DOI: https://doi.org/10.15680/IJIRCCE.2016.0401158
7. Eltyeb E., Elgabar A. Comparison of LSB steganography in BMP and JPEG images // International Journal of Soft Computing and Engineering. 2013. Vol. 3, no. 5. P. 91–95.
8. Hedieh S., Mansour J. Evolutionary rule generation for signature-based cover selection steganography // Computer and Information Technology Workshops: Proc. IEEE 8th International Conference on 2008. 2008. P. 379–384. DOI: https://doi.org/10.1109/CIT.2008
9. Jung K.H., Yoo K.Y. Data hiding method using image interpolation // Comput Stand Interfaces. 2009. Vol. 31, no. 2. P. 465–470.
10. Junying Y., Haishan C. Embedding suitability adaptive cover selection for image steganography // International Conference on e Education, e-Business and Information Management (ICEEIM). 2014. P. 36–39.
11. Kefa R. Steganography the art of hiding data // Information Technology. 2004. Vol. 3, no. 3. P. 245–269. DOI: https://doi.org/10.3923/itj.2004.245.269
12. Image steganography in spatial domain: A survey / H. Mehdi [et al.] // Signal Processing: Image Communication. 2018. Vol. 65, no. 3. P. 46–66. DOI: https://doi.org/10.1016/j.image.2018.03.012
13. Manju N., Monika M. Steganography: The art of hiding text in image using Matlab // International Journal of Advanced Research in Computer science. 2013. Vol. 4, no. 8. P. 206–210. DOI: https://doi.org/10.26483/ijarcs.v4i8.1788
14. Mansi S.S., Vijay H.M. Current status and key issues in image steganography: A survey // Computer Science Review. 2014. Vol. 13, no. 14. P. 95–113. DOI: https://doi.org/10.1016/j.cosrev.2014.09.001
15. Mansi S.S., Vijay H.M. Performance evaluation of image steganography based on cover selection and contourlet transform // International Conference on Cloud & Ubiquitous Computing & Emerging Technologies, India, Pune. 2014. P. 231–236. DOI: https://doi.org/10.1109/CUBE.2013.39

16. Manasi J., Arpita M., Kankana D. A secure Image steganography using efficient map based LSB technique // International Journal of Advanced Research in Computer Science and Software Engineering. 2016. Vol. 6, no. 3. P. 657–660.
17. Mamta Y., Amita D. Image steganography techniques: A review // International Journal for Innovative Research in Science & Technology. 2015. Vol. 2, no. 2. P. 243–248.
18. Mehdi K., Husrev T.S., Nasir D.M. Performance study of common image steganography and steganalysis techniques // Journal of Electronic Imaging. 2006. Vol. 15, no. 4. DOI: https://doi.org/10.1117/1.2400672
19. Nazinder K., Amanjot K. Art of steganography // International Journal of Advanced Trends in Computer Applications. 2017. Vol. 4, no. 2. P. 30–33. DOI: https://doi.org/10.1016/j.sigpro.2009.08.010
20. Johnson N.F., Jajodia S. Exploring steganography: Seeing the unseen // IEEE Computer. 1998. Vol. 31, no. 2. P. 26–34.
21. Nissar A., Mir A. Classification of steganalysis techniques: A study // Digital Signal Processing. 2010. Vol. 20, no. 6. P. 1758–1770. DOI: https://doi.org/10.1016/j.dsp.2010.02.003
22. Шелухин О.И., Канаев С.Д. Стеганография. Алгоритмы и программная реализация. М.: Горячая линия – Телеком, 2017. 592 с.
23. Seyyedi S.A., Ivanov N. A novel secure steqanography method based on zero tree method // International Journal of Advanced Studies in Computer Science and Engineering. 2014. Vol. 3, no. 3. P. 1–9.
24. A steganographic technique for highly compressed JPG images / K. Shamsul [et al.] // Computer Science Review. 2013. Vol. 10, no. 5. P. 107–118.
25. An overview of steqanalysis methods / V. Sakit [et al.] // Actual Multi-Disciplinary Scientific-Practical Problems of Information Security: Proceedings of The V Republican Conference, Baku. 2019. P. 204–206. DOI: https://doi.org/10.25045/NCInfoSec.2019.50
26. Verdiyev S.Q., Nagiyeva A.F. Experimental analysis of steganography // Actual Multi-Disciplinary Scientific-Practical Problems of Information Security: Proceedings of The III Republican Conference, Baku. 2017. P. 51–55. DOI: https://doi.org/10.25045/NCInfoSec.2017.10

Получено 20.11.2020

УДК 621.396.01

ОБ ОПТИМАЛЬНОЙ МОДИФИКАЦИИ ПРОЕКЦИЙ ИЗОБРАЖЕНИЙ НА БАЗИСНЫЕ ВЕКТОРЫ ПРИ СКРЫТНОМ ВНЕДРЕНИИ ИНФОРМАЦИИ

Черноморец А.А., Болгова Е.В., Коваленко А.Н.
Белгородский государственный национальный исследовательский университет, Белгород, РФ
E-mail: chernomorets@bsu.edu.ru, bolgova_e@bsu.edu.ru, kovalenko_a@bsu.edu.ru

Статья посвящена проблеме разработки методов скрытного контроля за использованием и распространением цифровых изображений на основе модификации коэффициентов разложения (проекций) изображений в различных системах базисных векторов, определяемых используемым двумерным преобразованием. В работе предложено для оценивания искажений изображений-контейнеров при скрытном внедрении информации на основе субполосного анализа в рамках двумерного косинус-преобразования применять оценки искажения значений проекций изображений на собственные векторы субполосных матриц данного преобразования. Сформулирована и аналитически решена задача поиска оптимальных модифицированных значений проекций изображения-контейнера с позиции минимизации его искажения, задаваемого как квадрат евклидовой нормы разности исходного и модифицированного изображений. Для иллюстрации преимуществ разработанного метода оптимальной модификации значений проекций были проведены вычислительные эксперименты. Показано, что применение разработанного метода позволяет получить меньшие искажения анализируемых изображений-контейнеров по сравнению с известными методами скрытного внедрения данных в изображения.

Ключевые слова: *скрытное внедрение, изображение-контейнер, субполосный анализ, косинус-преобразование, субполосные матрицы, собственные векторы, проекции изображения*

Введение

В настоящее время для контроля за использованием изображений, содержащих важные данные, достаточно широко применяются методы скрытного внедрения контрольной информации в изображения [1–3].

Во многих методах для скрытного внедрения в изображения одного бита информации применяется относительная замена (модификация) значе-