UDC 004.056.55; 004.9; 003.26.

Image steganography – classic and promising methods: a study

Vitaly Zubok[1,2], Ivan Kazmidi[1]

[1] *National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"*
[2] *G.E. Pukhov Institute for Modeling in Energy Engineering NAS of Ukraine*

Abstract

Steganography, the art and science of hiding information within digital media, remains a dynamic and increasingly vital discipline in the age of pervasive digital communication and cybersecurity threats. Images, in particular, serve as highly adaptable carriers for covert data due to their ubiquity and rich payload capacity. This paper presents a comprehensive classification of image-based steganographic techniques, surveying both time-tested methods (e.g., LSB modification, wavelet transform) and cutting-edge approaches. We highlight how artificial intelligence—through deep learning models, generative adversarial networks, and AI-driven compression/enhancement — can greatly improve embedding robustness and evasion of detection. Furthermore, we explore the nascent frontier of quantum steganography, leveraging superposition, entanglement, and quantum key distribution to achieve unprecedented levels of security. Finally, we outline promising research directions that fuse classical methods with next-generation AI and quantum technologies, setting the agenda for the next wave of advances in secure information hiding.

Keywords: cybersecurity, steganography, digital images, quantum technologies, artificial intelligence

Introduction

Along with digital technologies, methods and tools of steganography and steganoanalysis are developing. Modern technologies, such as AI and quantum computing, are developing rapidly. It is necessary to review existing and promising methods of image steganography, predict the development directions of this field in the near future and identify possible research directions

1. Methods for the literature review

The literature review is carried out with the aim of studying the current and potential problems arising in the context of image steganography by examining existing methods of this technology and relevant scientific sources. Given this aim of the article, the search for sources should be carried out accordingly.

1.1. Source material selection criteria

Authoritative scientific databases are used, in particular IEEExplore, ResearchGate, Arxiv, ScienceDirect, Scopus, Google Scholar, CrossRef, Thesai and Semantic Scholar, with preference given to publications published within the last five years, although the actual time period covers the last 15 years. The main sources are articles and conference proceedings, which ensure conciseness and accuracy of the presentation of the main ideas. When selecting materials, preference is given to English-language publications that cover both known and new, promising methods of image steganography, as well as their modifications and improvements to individual characteristics. Such selection criteria will allow us to focus specifically on the ideas of steganography methods and will provide a wider range of potential research directions.

1.2. Data extraction and classification

The analysis covers the main methods of image steganography, an assessment of their advantages and limitations, with special attention to the latest methods that use artificial intelligence and quantum computing technologies. All sources and methods of steganography are systematized according to two main criteria: the types of images in which these

methods are used, and the common methodology for embedding information in images. The analysis focuses on the practical and ideological aspects of image steganography methods, without excessive immersion in a deep theoretical analysis of individual techniques, while emphasizing general directions for further research in this area. This classification of sources clearly demonstrates the difference in approaches to steganography of different types of images, as well as the evolution of steganographic methods within the same type of images.

The use of these databases guarantees high quality and reliability of the materials obtained, and also allows quick access to the latest scientific developments. Focusing on English-language publications ensures coverage of the most relevant and innovative research, since most of the advanced scientific developments are published in English. Grouping materials by image types and information embedding methodology promotes a structured approach to analysis, which facilitates the identification of general trends and promising directions for the development of image steganography. Focusing on the practical aspects of the methods allows obtaining important conclusions for further research and development of new solutions in this area, avoiding excessive abstraction in theoretical studies.

2. Results of literature review

2.1. Image types overview

Typically, when describing steganographic methods, researchers use criteria such as the amount of information that can be embedded, the speed of embedding and extracting information [2], and artifacts in the image using the signal-to-noise ratio [3]. However, such criteria are not classificatory, but only assessments of individual methods. When classifying steganographic methods in digital images, it is first necessary to distinguish between two main types of digital image representation. These types include raster and vector images. Each of them has its own characteristics, advantages and disadvantages. Raster images are made up of pixels, the smallest elements that have a specific color. They have a fixed resolution, which affects the quality when scaled. Such images are good at conveying color gradients and complex textures, so they are widely used in photography, digital painting, and web design. The main disadvantages are the loss of quality when enlarged, which leads to pixelation, as well as the large file size in the case of high resolution. Vector images are built using mathematical formulas that define lines, curves, and shapes. They are resolution-independent, so they scale without loss of quality. Such images are easy to edit, which makes them ideal for logos, fonts, and illustrations. In addition, they usually have a smaller file size compared to high-quality raster images. The main disadvantage is that vector images cannot convey complex color transitions and textures. Fractal images are created using mathematical algorithms that build self-similar structures. They can have any resolution, since they are generated dynamically. Such images are used in scientific visualization and art. The disadvantage is that their creation requires significant computing resources, as well as their limited use in standard graphics.

2.2. Known steganographical methods

Information is hidden in the properties of image components. Within each type of image, there can be a large number of different steganography methods, which can complement each other, or be a combination of several methods. With this in mind, the study focuses on the "basic" steganography methods, which describe not so much the technical features and mathematical differences between the methods, but their main idea, for example, a parameter or part of the image that serves as a steganographic container. Each method considered, despite its mathematical validity and efficiency, may encounter problems when used in real conditions. Let us consider the existing steganography methods for each type of image.

2.2.1. Raster image steganography

The following classification of raster image steganography methods is proposed:

- Classification by selecting a part of the image that will serve as a container for hidden information
- Classification by transforming the image before embedding information

The color of each pixel of a raster image is represented in the form of bits, by changing which information can be embedded in the image. One of the most common methods is to

change the least significant bit [1]. In this method, the authors use the last bit of the pixel color in which the information is hidden. If you change the smallest bit in each of the components, the color will remain almost unchanged, but the data will be hidden. The main advantage of this method is the simplicity of implementation and the high density of hidden information. However, it is vulnerable to compression attacks and image changes, since any editing can destroy the hidden data.

The method of using the alpha channel [4] consists in embedding information in the alpha mask of the image, which determines the presence of transparent areas. This is possible for formats that support transparency, such as PNG. The authors take advantage of the fact that the alpha mask is, in fact, an independent image that is added to the original image. However, the main limitation is that not all images contain transparent areas, so its application is limited.

The container image can not only be selected from certain possible options, but also generated from scratch. This approach is used in the Julian set method [13]. The mentioned sets, when converting the parameters of the points of the sets to an image, create a fractal image. Fractal images, with the exception of special software tools, are displayed as raster images with predefined dimensions. Information is recorded in the color parameters of pixels. To extract information, it is necessary to distinguish the difference between the original image and the container image. In this case, the parameters of the Julian set can act as a kind of secret key for generating the original image and extracting hidden information, although studies of the reliability of such a key have not been presented.

A more complex approach to steganography of raster images consists in preliminary transformations of the container image. A good example is steganography based on discrete transformations. The discrete cosine transform [2] or the discrete wavelet transform [3] are used. In this case, the hidden data is embedded in the frequency components of the image obtained by means of appropriate transformations over the binary representations of the container image. The raster image is divided into parts, after which the image is embedded in some of these parts by another method, for example, the last bit method. After embedding, the information components are assembled back into a complete image. Due to the mathematical features of the resulting discrete transformations, this method is more resistant to attacks, since the hidden data remains unchanged even after compression. The disadvantage is the complexity of implementation and the smaller amount of data that can be hidden compared to the last bit method.

It is worth noting that the previous methods can be combined with each other. This provides an additional level of security, since without knowledge of the combination algorithm, data recovery is impossible. In this case, pixels in which information will be embedded are randomly selected, using already known steganographic methods. The main disadvantage of this approach is the need for synchronization between the sender and receiver of the random pixel generator and its initial data. In addition, this method does not relieve the hidden data of the shortcomings of the methods of hiding it, but only complicates the search for the fact of hiding data.

2.2.2. Vector image steganography

Steganographic methods for embedding information in vector images can generally be divided into two groups [5]:

- Spatial methods
- Frequency methods.

Spatial methods use the parameters of graphic objects as information containers.

The Haowen-Lee method [6] uses the distance between points as a container for information. For this, the image is divided into zones according to a certain defined mask. After division, changes are made to the position of the points in each zone according to the mask and the data to be embedded. This method also has a modification [7], in which each zone is additionally divided into two parts by a diagonal and has its own separate mask. The embedding of information in this case occurs by transferring points from one half of the zone to the other symmetrically with respect to the diagonal.

The line splitting method [8] divides lines into strips, each of which has two lines, one of which denotes the bit value 0, and the other - 1. Information is hidden by moving points from one straight line to another. The authors of both methods, first of all, developed them for applying watermarks to electronic maps depicted using vector graphics. In this case, the information is mostly recorded in the parameters of the road layout, the shift from the real position

is imperceptible. It should be noted that for this direction of steganography use, the speed of embedding and extracting information from the steganographic container can be critically important. This is primarily due to the size of the maps and the potential need to watermark each copy of the map. The disadvantage of spatial methods is low protection against active countermeasures, for example, affine stretching or shifting operations performed on a vector image, which with a high percentage of success will destroy the hidden message. Another disadvantage is that embedding information using spatial methods more often than other methods leads to changes in the image that can be noticed by the human eye. Unlike spatial methods, frequency methods, before embedding information, perform certain manipulations with the parameters of objects in order to reduce them to the desired form, after which mathematical transformations are applied. The results of these transformations can serve as containers for hidden information.

The discrete Fourier transform method [9] uses an appropriate discrete transform to hide data. The information is stored in the broken lines that are on the image. The coordinates of each point of the broken line are converted to a complex number, forming a sequence of complex numbers over which the discrete Fourier transform is performed. The coefficients obtained after the Fourier transform are changed in accordance with the message that needs to be hidden. This method is primarily used for watermarking. In this case, the values of the coefficients will be calculated for the processed image and compared with the desired ones. It can also be used for information transmission, however, to extract the hidden information, you need to have the original image.

The previous method can be modified [10]. After forming a similar sequence of complex numbers from the coordinates of points in the image, a three-level wavelet transform [11] is used, which results in four groups of wavelet coefficients. Depending on the permissible deviation from the original image, information, which most often represents a watermark, can be added to several or all four groups of wavelet coefficients. The authors of both previous methods used the dependence of image integrity on the coefficients of certain mathematical transformations to embed and verify watermarks. Frequency methods are more resistant to active attacks and are more likely to preserve the hidden message after image operations. However, such methods can lead to a decrease in image quality, which may give away the fact of interference with the image structure.

2.2.3. Fractal image steganography

Fractals, as a rule, do not exist independently, but are images of certain mathematical formulas, functions or sets. One of such sets is the Julian set [13]. Although, first of all, these sets are a group of points with certain characteristics, some of their mathematical values, for example, the distance of points from the neighborhood of the Julian set to the set itself, when transferred to an image will form a fractal. In this method, the Julian set forms an image of a fractal, which is divided into three layers by the RGB color values. Message bits are written in each of the three layers, which are then combined and form an image with hidden information. To extract information, it is necessary to find the input data from which the Julian set and the corresponding primary fractal were formed, and then compare the two images. The author notes that in this method, the parameters of the Julian set can act as a security key for building information.

2.3. Promising research directions

2.3.1. Artificial intelligence

One of the promising areas of research is the use of artificial intelligence capabilities in steganography. This area is quite promising, given the constant improvement of the quality of artificial intelligence when working with images. Artificial intelligence can be used as a means of detecting embedded information in images, as a means of destroying hidden information, and as a means of embedding information. To detect embedded information, machine learning algorithms can be used to detect certain patterns in the properties of images that potentially indicate the presence of hidden information [14,15]. This method is especially relevant for vector images, since information is hidden in the properties of mathematical functions that describe the objects of a vector image. With the advent of artificial intelligence, a new way of expanding an image has appeared, that is, improving its quality by artificially increasing the number of pixels. Unlike previous methods of image enhancement, such as the Lanchos filtering method [18], where there are specific

mathematical formulas that calculate the addition of new pixels, artificial intelligence models use a large amount of diverse data on which they were trained. Formalizing the logic of a specific artificial intelligence model is a much more difficult task than calculating the image enhancement using well-known mathematical methods. Additionally, this method is enhanced by the ability to constantly retrain the corresponding artificial intelligence model, thereby making changes to the image enhancement process, which further complicates the protection of hidden information from destruction. Similarly, it is possible to use image compression using AI instead of known methods. A combination of these methods, i.e., a primary reduction in image quality, followed by an increase in quality to the initial level, will hide the changes introduced into the image by the destruction of hidden information. Generative adversarial networks have the potential to be used as generators of container images [16,17] that can store information using other modern steganographic techniques while remaining resistant to steganoanalysis. There are already descriptions of models of so-called steganographic generative adversarial networks [4] (SGANs). Although such networks were developed exclusively for generating images with hidden data, there is potential for using related technologies to embed information into predefined images.

2.3.2. Quantum technology

Another direction of development of steganography is its combination with quantum technologies [19]. At present, the main directions of quantum steganography are: • Use of the property of superposition • Use of the property of quantum entanglement • Use of quantum key exchange protocols Superposition is the property of a unit of quantum information, a qubit, to be in several different states simultaneously. By changing the states of qubits, it is possible to hide the necessary information in a quantum message. At the same time, to read the hidden information, it is necessary to read the qubits in a certain way, thereby forcing them to take the desired state in which the secret message will be. Information at this time can be hidden by using quantum operations on qubits, for example, quantum logic gates or qubit phase shifts. Quantum entanglement connects qubits with each other. Attempts to read or intercept a qubit of information will lead to changes in the qubits associated with it. In this case, the corresponding states of entangled qubits can be calculated without even being able to measure their state. This property allows you to create a communication channel between the sender and the recipient and securely transmit hidden data in interconnected qubits. Quantum key exchange protocols are key exchange protocols in which the properties of the quantum world act as a guarantor of the secure exchange of a common secret key, providing protection against data interception of the key exchange process. These protocols can ensure a secure connection establishment process, thereby simplifying the transmission of information using steganographic methods. Although the above information refers to the smallest unit of quantum information, a qubit, it will also be relevant for the transmission of more complex data objects through quantum channels, including images. Depending on the image format, the information can be hidden in the binary version of the image, and then translated into qubits, or directly in qubits. Moreover, both options for embedding secret information will equally benefit from the aforementioned quantum technologies.

Discussion

This study reaffirms that image steganography is not merely an applied art but a vibrant scientific field, continually driven forward by technological innovation. While classical methods provide a solid foundation, they face challenges in capacity limits, vulnerability to signal processing, and operational efficiency. By integrating artificial intelligence—enabling smarter embedding, adaptive detection evasion, and AI-generated carrier images—and by harnessing quantum phenomena—such as superposition for multi-state encoding, entanglement for tamper-evident channels, and quantum key exchange for secure parameter sharing—researchers can substantially elevate both the stealth and resilience of steganographic systems. As digital communication landscapes evolve, interdisciplinary collaboration at the intersection of steganography, AI, and quantum computing will be essential to meet emerging security requirements and to pioneer the next generation of covert communication techniques.

References

[1] Aslam, Muhammad & Rashid, Muhammad & Azam, Farooque & Abbas, Muhammad & Rasheed, Yawar & Alotaibi, Saud & Anwar, Muhammad. (2022). Image Steganography using Least Significant Bit (LSB) - A Systematic Literature Review. 32-38. 10.1109/ICCIT52419.2022.9711628.

[2] Khalaf, Ashraf A. M. & Fouad, Osama & Hussein, Aziza & Hamed, Hesham & Kelash, Hamdy & Ali, Hanafy. (2019). Hiding data in images using DCT steganography techniques with compression algorithms. TELKOMNIKA (Telecommunication Computing Electronics and Control).17.10.12928/telkomnika.v17i3.

[3] Della Baby, Jitha Thomas, Gisny Augustine, Elsa George, Neenu Rosia Michael, A Novel DWT Based Image Securing Method Using Steganography, Procedia Computer Science, Volume 46,2015,Pages 612-618,ISSN 1877-0509, https://doi.org/10.1016/j.procs.2015.02.105.

[4] Nichal, Arjun & Jadhav, Mr.Aniket & Pingale, Mr & Mohite, Mr.Chaitanya & Ponde, Mr. (2015). A Novel Steganography Scheme via the use of Alpha channel. IJIREEICE. 3. 18-21. 10.17148/IJIREEICE.2015.3404.

[5] O. Kinzeryavyy (2015), Steganographic methods for hide data in vector images resistant to active attacks based on affinian transformations [Doctoral dissertation, National University "Kyiv Aviation Institute"], erNAU - Electronic Institutional Repository of the National Aviation University of Ukraine.

[6] Yan, Haowen & Li, Jonathan. (2011). A Blind Watermarking Approach to Protecting Geospatial Data from Piracy. International Journal of Information and Education Technology. 94-98. 10.7763/IJIET.2011.V1.16.

[7] Kang H. A vector watermarking using the generalized square mask / H. Kang // Proc. of the International Conference on Information Technology : Coding and Computing. — Las Vegas (USA), 2001. — pp. 234-236.

[8] Sonnet, Henry & Isenberg, T. & Dittmann, J. & Strothotte, Thomas. (2003). Illustration watermarks for vector graphics. 73- 82. 10.1109/PCCGA.2003.1238249.

[9] V. Solachidis, N. Nikolaidis and I. Pitas, "Fourier descriptors watermarking of vector graphics images," *Proceedings 2000 International Conference on Image Processing (Cat. No.00CH37101)*, Vancouver, BC, Canada, 2000, pp. 9-12 vol.3, doi: 10.1109/ICIP.2000.899265.

[10] Y. Li and L. Xu, "A Blind Watermarking of Vector Graphics Images," in Computational Intelligence and Multimedia Applications, International Conference on, Xi?an, China, 2003, pp. 424, doi: 10.1109/ICCIMA.2003.1238163.

[11] Debnath, Lokenath & Antoine, Jean-Pierre. (2003). Wavelet Transforms and Their Applications. Physics Today - PHYS TODAY. 56. 68-68. 10.1063/1.1580056.

[12] Al-Rammahi, Hassanein. (2014). Steganography Using Fractal Images Technique. IOSR Journal of Engineering (IOSRJEN).

[13] Nori, Ahmad & Alqassab, Asmaa. (2014). STEGANOGRAPHIC TECHNIQUE USING FRACTAL IMAGE By.

[14] Al-Obaidi SAR, Lighvan MZ, Asadpour M. Enhanced image steganalysis through reinforcement learning and generative adversarial networks. Intelligent Decision Technologies. 2024;18(2):1077-1100. doi:10.3233/IDT-240075

[15] Al-Iedane, Hussein Ali and Mahameed, Ans Ibrahim (2023), Applying and Evaluating Machine Learning Models for the Detection of Digital Image Steganography, Doi: 10.2139/ssrn.4427951

[16] D. Hu, L. Wang, W. Jiang, S. Zheng and B. Li, "A Novel Image Steganography Method via Deep Convolutional Generative Adversarial Networks," in *IEEE Access*, vol. 6, pp. 38303-38314, 2018, doi: 10.1109/ACCESS.2018.2852771.

[17] Volkhonskiy, D., Nazarov, I., & Burnaev, E. (2020, January). Steganographic generative adversarial networks. In Twelfth international conference on machine vision (ICMV 2019) (Vol. 11433, pp. 991-1005). SPIE.

[18] Burger, W., & Burge, M. (2009). Principles of digital image processing: core algorithms. Springer. https://doi.org/10.1007/978-1-84800-195-4.

[19] Mayer, J. (Ed.). (2024). Steganography - The Art of Hiding Information. IntechOpen. doi: 10.5772/intechopen.1001493