Transactions on Computer Science and Intelligent Systems Research
ISSN: 2960-1800, eISSN: 2960-2238 | Volume 6
ISET 2024

Research on Key Technologies of Spatial Domain Image Steganography and Analysis of Typical Applications

Chuanyue Zhang

School of Computer Science and Engineering, Tianjin University of Technology, Tianjin, China

631501010903@mails.cqjtu.edu.cn

Abstract. In the digital age, secure storage and communication of information are crucial aspects of everyday life, drawing significant global interest. Steganography serves as a pivotal method for concealing private information within various media forms—such as images, videos, and text—enabling secure information transmission. This paper delineates the distinctions between information hiding and encryption and delves into image steganography. The focus here is on spatial-based image steganography techniques, which are broadly categorized into traditional and deep learning-based methods. Traditional methods rely on modifications to the pixel values of the host image, often resulting in minor but detectable changes if not carefully managed. On the other hand, deep learning-based methods leverage neural networks to learn how to encode data in an image in a way that is much harder to detect. A comprehensive performance analysis of these techniques is provided, complete with comparative tables to aid in clarity and reference. Additionally, this paper aims to guide researchers by charting current trends in the field and suggesting future research directions. By exploring these advanced techniques, the paper contributes to the broader discourse on enhancing the security and efficacy of steganographic practices.

Keywords: Information Hiding; Steganography; Spatial-Domain Steganography.

1. Introduction

In today's digital landscape, innovations in internet technology and the digitization of information have made online storage and exchange of data integral to our daily lives. Consequently, there is increasing emphasis on the secure transmission of private information. Confidentiality systems are crucial for protecting information security. Broadly, secure data protection systems can be categorized into two main approaches: information encryption, known as cryptography, and information hiding. Figure 1 illustrates the role of steganography within a security system. Although both information hiding and encryption aim to secure data, they differ fundamentally in their methods. Steganography conceals the existence of the information itself, making it undetectable, whereas encryption scrambles the content of the information, rendering it unreadable without the decryption key. These differences underscore diverse strategies in information security, each with its unique strengths and vulnerabilities in protecting data privacy.

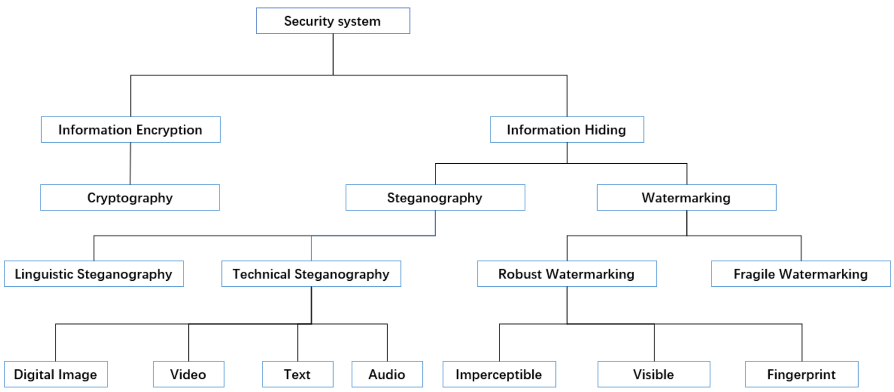

Figure 1. A general branch of security systems [1].

Content from this work may be used under the terms of CC BY-NC 4.0 licence (https://creativecommons.org/licenses/by-nc/4.0/).
Published by Warwick Evans Publishing.

Information hiding is divided into two branches, one is watermarking and the other is steganography. These two fields are used to hide confidential messages from other unauthorized users. These two fields are very similar. But their main goals are different. Steganography aims to hide the protection and communication tools associated with secret information. On the contrary, the objective of watermarking technology is to preserve the reliability and security of private data, that is, to secure the proprietary rights and entitlements of the content. Watermarking is utilized to defend the intellectual property associated with the concealed information. Table 1 describes the basic characteristics of information hiding and cryptographic systems.

Table 1. Summarized distinction between information encryption and information hiding.

	Information Steganography		Information Encryption
	Steganography	Watermarking	Cryptography
key objective	Hiding secret information and communication processes	Protecting Intellectual Property	Protecting confidential information
Sense of security	Difficult to identify	Depends on the method of attachment	Very easy (channel visible)
Security of communication	Depends on the confidentiality of the embedding method	Depends on the confidentiality of the embedding method	Depends on the confidentiality of the key
Keying Demands	Depends on embedding method	Depends on the embedding method	Urgent
Types of outputs	Text	Image/Text/Video	Image/Text/Video
Erosion of security	When confidential data is detected	When confidentiality confidence loses integrity	When the translation is deciphered
Detection and Extraction complexity	Both are complex	Both are complex	Simple to detect but complex to extract
challenges	Robustness	Imperceptibility, Security, Payload capacity and Robustness	Key management and encryption algorithm complexity

This paper aims to introduce some key technologies and their application scenarios in spatial-based image steganography. The subsequent material in this pap is divided into 4 parts: In section 2, an overview of steganography, including its origin, general process and application scenarios are described. In section 3, some key techniques of spatial image steganography are introduced and their performance is analyzed. In section 4, a summary of the whole paper is provided, and future research directions and recommendations are outlined.

2. Steganography: Overview

2.1. Background on Steganography

Steganography as a concept has its linguistic foundations in the ancient Greek words "stegano" and "graphy", which together mean " concealed messaging"错误!未找到引用源。 [2]. From ancient times to the present, people have never given up the study of how to hide information from unauthorized users. According to The Histories of Herodotus, in the 5th century AD, the ancient historian Herodotus concealed a secret missive by having it written on the shaved head of his most loyal retainer, dispatched the servant to Aristagoras once the hair had grown back, and directed Aristagoras to have the servant's head shaved again upon reaching his destination. Coincidentally, Demaratus sent a warning to Greece about an impending attack by writing a secret message directly on the wooden back of a wax tablet before applying the wax surface [3].

The majority of contemporary steganographic techniques leverage a variety of multimedia formats, including pictures, videos, and audio files. Image steganography is one of the most prolific areas of steganography., providing a variety of techniques for different image formats [4].

2.2. Generalized Architecture for Image Steganographic Systems

Figure 2 shows the relevant structure of the fundamental steganographic workflow. Assume that "M" is the confidential information to be transmitted, "K1" represents the optional cryptographic key, "K2" is the corresponding decryption key, "E_{em}" is the key set by the embedding method, "E_{ex}" is the extraction method, "C" represents the stego medium, and "S" signifies the modified image containing the embedded confidential information. In addition, it is assumed that the secret P_{em} represents the embedding process, whereP_{ex} represents the extraction process. The procedures for embedding and extracting private data are explicated in accordance with the ensuing algebraic representation:

$$P_{em} = E_{em}(M, K1, C) \rightarrow S \tag{1}$$

$$P_{ex} = E_{ex}(K2, S) \rightarrow M \tag{2}$$

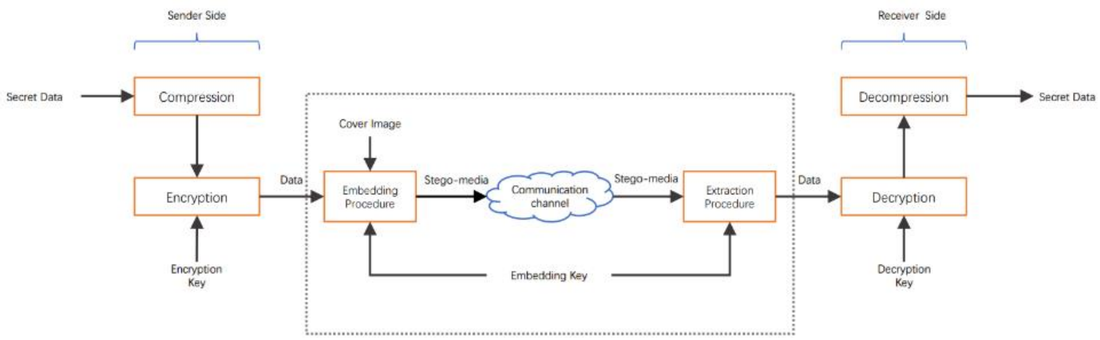

Figure 2. Standard Conceptual Model of Steganography Utilizing Images (Photo credit: Original).

2.3. Application

Steganography is used in many different applicable applications, including organizations or institutions to securely transmit secret data, embed personal information into photos on smart ID cards to control copyright, and embed patient details in medical images to protect information and speed up transmission. In summary, steganography can be used to protect and transmit sensitive information in a covert manner.

3. Image Steganography

Image-based steganography can be generally classified into approximately three distinct approaches: transform domain steganography, spatial-based image steganography, and adaptive embedding technology. Spatial-based image steganography can be predominantly differentiated into two primary strains one is based on traditional methods, and the other is based on deep learning methods. Spatial-based image steganography is generally represented by LSB steganography, which is simple to implement but has relatively weak hiding capacity and robustness. Table 2 provides a comprehensive assessment contrasting transform-based and spatial-based approaches and adaptive embedding methods.

Table 2. Comparative analysis of spatial domain and transform domain techniques with adaptive embedding methods.

Features	Spatial Domain	Transform Domain	Adaptive Embedding
Payload Capacity	High	Low	Depends on the specific steganographic technique
Insertion Point	Direct manipulating of pixel values	Transform coefficients	Depends on the specific steganographic technique
Adaptability to Cover Object Format	Format dependent	Format dependent	Depends on the specific steganographic technique
Complexity	Low	High	Depends on the specific steganographic technique
Robustness to Various Image Manipulations	Not robustness	Less susceptible to discovery	Depends on the specific steganographic technique
Visual undetectability	High	Low	Low
Geometrical distortion attacks	Not robustness	Less vulnerable	Less vulnerable

This section delves into some key spatial-based image steganography schemes. In addition, Table 3 offers a comprehensive examination of the traditional methods and Table 4 offers a comprehensive examination of the deep learning-based methods.

3.1. Based on Traditional Steganography Methods

3.1.1. Least significant bit (LSB) based method.

Traditionally, the least significant bit (LSB) replacement method represents a common spatial image steganography technique [5]. The working principle of the LSB method is to modify the lowest bits of some pixel values in the image without being discovered, and the secret information is transmitted in binary form. The slight modification of these bits is undetectable by the human eye.

To attain the same level of efficacy as the Least Significant Bit (LSB) method, numerous alternative techniques have been devised; Jagan et al. proposed a stego-space domain enhanced least significant bit replacement algorithm based on character sequence. optimization, which achieved higher embedding rate and security by encoding the secret message in two stages [6].

3.1.2. Pixel value differencing (PVD) based method.

Another traditional spatial domain method is the pixel value difference (PVD) method proposed by Wu et al.. This method is a steganographic technique based on pixel difference. Specifically, when working, this method divides the image into non-overlapping pixel blocks, calculates the difference of pixel values in each block, and then determines the number of bits to embed based on the difference range. The greater the difference between two pixels, the more payload can be embedded. The merits of this algorithm are that it can embed a large amount of secret information without causing obvious visual distortion, and can extract secret information without the original image. The challenges are that it may be detected by statistical analysis attacks, is not suitable for low-quality images.

3.1.3. Exploiting Modification Direction(EMD) based method.

Another common traditional spatial domain method is to use the modified direction (EMD) method. This method achieves the purpose of steganography by making full use of the pixel modification direction. Specifically, when this method works, the hidden number is carried by n pixels, and at most only one pixel is increased or decreased by 1. And because there are 2n different modification methods plus the case of no modification, there are a total of (2n+1) possibilities. The greatest extent of pixel value alteration is confined within a range of only (±1). In general, this method applies a specific basis to select local changes aligned with the pixel intensity in the carrier medium. Therefore, this method has a relatively higher payload. Not only that, compared with the PVD and LSB methods, this method also preserves seamless visual integration. At the same time, when the selected pixels increase, the embedded payload is fundamentally reduced. The algorithm proposed by Kuo et al. effectively enhances the embedded payload. The merits of this algorithm are high steganographic efficiency, full utilization of modification direction, improved steganographic security. The challenges are high computational complexity.

Table 3. Effectiveness evaluation of steganographic methods based on spatial domain tradition.

method	reference	algorithm	merit	challenge	payload (bpp)	PSNR	anti-steganalysis
LSB based	Sarreshtedari et al. [7]	±1 LSB	· High concealment · Simple implementation	· Lower payload · Depends on the key	1 bpp	~53 dB	HCF-COM
	Jajan et al. [8]	eLSB	· High capacity embedment rate · High security	· High algorithm complexity · Limited file types · Easy to detect	NA	NA	NA
PVD based	Balasubra manian et al. [9]	OctonaryPVD	·Adaptive embedding ·Resistant to various statistical steganalysis	· Lack of modern steganalysis evaluation	~ 3.6 bpp (gray image)	~40 dB	PVD analysis & RS analysis
EMD based	Kuo et al. [10]	GEMD	· Leverage adaptive modulus mapping to determine the optimal weight of the extraction function	· Modify all pixels to embed secret data · Limited payload	1.5 bpp	~50.2 dB	NA

3.2. Based on Deep Learning Methods

The incorporation of deep learning techniques into the field of steganography in recent years has demonstrated a significant enhancement regarding the potency of steganographic methods. Steganographic techniques employing deep learning methodologies are founded upon the fundamental principles of machine learning. Deep learning-based steganography can be categorized into two main types: adversarial network-based methods and convolutional neural network-based methods.

3.2.1. Convolutional Neural Networks(CNN) based method.

Baluja's approach involved the creation of a convolutional neural network that was structured around an encoder-decoder paradigm as its fundamental design principle. This approach employs a deep neural network architecture to facilitate the simultaneous training of the hidden image and the recovered image, thereby establishing a cohesive, paired framework. The encoder embeds the secret image seamlessly into a cover image of identical dimensions, while the decoder is able to fully recover the hidden secret image. The key benefit of this model is its capability to conceal a full-sized color image within another image of equal dimensions, going beyond just text-based information, while also making detection more challenging. However, the drawback is that excessive distortion may arise when the hidden data is too extensive.

3.2.2. Generative Adversarial Networks(GAN) based method.

Zhu et al. developed a deep learning-based data hiding approach reliant on generative adversarial networks (GANs), which they named HiDDeN. The method consists of three components: encoder network, decoder network and adversarial network. The encoder network encodes the input mask image and hidden information into a visually indistinguishable hidden image. The decoder network can accurately restore the original hidden information from the hidden image. The decoder network can accurately restore the original hidden information from the hidden image. The merit of this algorithm is that it does not require the design of complex heuristic algorithms. Models trained under different random initializations will produce diverse hiding strategies, which will make it difficult for the adversary. The challenge is that the robustness of the algorithm to noise needs to be further improved.

Table 4. Effectiveness evaluation of steganographic methods based on spatial domain deep learning.

method	reference	algorithm	merit	challenge	payload(bpp)	PSNR	anti-steganalysis
GAN based	Zhu et al. [11]	GAN	· Highly precise secret data extraction	· Restricted hiding capacity · Demands excessive memory resources	0.203 bpp	<40 dB for Combined model	ATS analysis
CNN based	Baluja [12]	CNN	· Enhanced embedding capacity		1:1 ratio	NA	NA

Most spatial-based information hiding methods can accommodate large data capacities, but they are less robust and are easily affected by different image processing, image filters, and lossy compression. In summary, Table 5 briefly compares and summarizes the advantages and disadvantages of the key spatial-based image steganography techniques mentioned above.

Table 5. The merits and challenges of key spatial-based image steganography.

	method	merit	challenge
based on tradition	LSB	Suitable data capacity and straightforward application	Vulnerable to statistical analysis and environmental interference
	PVD	Expansive data hiding capability coupled with tolerable visual distortion	Vulnerable to statistical detection techniques
	EMD	Enhanced visual undetectability surpassing traditional LSB and PVD techniques	Limited payload
based on deep learning	GAN	Enhanced steganographic cover and heightened protective measures	Limited payload Overfitting risk and detectability
	CNN	Expansive embedding potential, robust, self-operating, versatile	Limited payload Overfitting risk and detectability

4. Conclusion

This paper explores key methodologies in image and spatial image steganography, elucidates the distinctions between information hiding and encryption, and assesses the merits and challenges of these technologies through comparative tables. The principal challenges in spatial image steganography are high embedding loads, security, and minimal detectability.

To fortify the robustness of the steganographic system, several recommendations are proposed:

a) Advanced Embedding Algorithms: Adoption of embedding algorithms that can withstand various attacks is suggested. For instance, encryption based on chaotic mapping or more sophisticated algorithms may be employed to obscure and secure embedded information, making it more resilient to detection and corruption.

b) Enhanced Preprocessing Operations: Prior to transmitting secret information, it is advisable to conduct preprocessing operations such as scrambling and compression encoding. These steps not only reduce the size of the original secret data but also bolster its security. Incorporating error correction coding technology can further enhance robustness by introducing redundant information, thus enabling recovery and identification even when data is partially compromised.

c) Suitable Steganalysis System Design: In designing a steganalysis system, a comprehensive consideration of the actual demand environment is crucial to determine appropriate robustness and self-recovery capabilities. It is important to avoid excessively robust systems that may complicate the algorithm unnecessarily, hinder the speed of secret information extraction, or prevent the extraction of secret information under attack conditions.

Supported by referenced literature, this analysis suggests that future research in steganography might benefit from increased integration of deep learning techniques to advance this field..

References

[1] S. Atawneh, A. Almomani, P. Sumari, Steganography in digital images: Common approaches and tools, IETE Technical Review. 30 (2013) 344-358.

[2] C. Balasubramanian, S. Selvakumar, S. Geetha, High payload image steganography with reduced distortion using octonary pixel pairing scheme, Multimedia Tools and Applications. 73 (2014) 2223-2245.

[3] S. Baluja, Hiding images in plain sight: Deep steganography, Advances in Neural Information Processing Systems. 30 (2017).

[4] A. Cheddad, J. Condell, K. Curran, P. Mc Kevitt, Biometric inspired digital image steganography, In: 15th Annual IEEE International Conference and Workshop on the Engineering of Computer Based Systems (ECBS 2008), IEEE, 2008, pp. 159-168.

[5] A. Cheddad, J. Condell, K. Curran, P. Mc Kevitt, Digital image steganography: Survey and analysis of current methods, Signal Processing. 90 (2010) 727-752.

[6] X. Zhu, Y. Huang, X. Wang, R. Wang, Emotion recognition based on brain-like multimodal hierarchical perception, Multimedia Tools and Applications (2023) 1-19..

[7] I.J. Kadhim, P. Premaratne, P.J. Vial, B. Halloran, Comprehensive survey of image steganography: Techniques, evaluations, and trends in future research, Neurocomputing. 335 (2019) 299-326.

[8] W.C. Kuo, S.H. Kuo, Y.C. Huang, Data hiding schemes based on the formal improved exploiting modification direction method, Applied Mathematics & Information Sciences Letters. 1 (2013) 1-8.

[9] S. Sarreshtedari, M.A. Akhaee, One-third probability embedding: a new ±1 histogram compensating image least significant bit steganography scheme, IET Image Processing. 8 (2014) 78-89.

[10] S. Wang, D. Zheng, J. Zhao, W.J. Tam, F. Speranza, An image quality evaluation method based on digital watermarking, IEEE Transactions on Circuits and Systems for Video Technology. 17 (2006) 98-105.

[11] X. Zhu, C. Guo, H. Feng, Y. Huang, Y. Feng, X. Wang, R. Wang, A Review of Key Technologies for Emotion Analysis Using Multimodal Information, Cognitive Computation (2024) 1-27.

[12] J. Zhu, R. Kaplan, J. Johnson, L. Fei-Fei, Hidden: Hiding data with deep networks, In: Proceedings of the European Conference on Computer Vision (ECCV), 2018, pp. 657-672.