Spatial Domain Image Steganography Methods for Secure Information Exchange in Digital Transport and Logistics Systems: A Survey and Comparative Analysis

Ababil Nagiyeva[1], Sakit Verdiyev[2], Kenan Abdullayev[3]

[1]Azerbaijan Technological University; Azerbaijan
nagiyevaababil@gmail.com
[2]Azerbaijan Technological University; Azerbaijan
info_tel@inbox.ru
[3]Azerbaijan Technological University; Azerbaijan
kenan.abdulllayev98@gmail.com

Abstract. Steganography and steganalysis are two parallel development directions of data 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. An integral part of steganography is steganalysis aimed at detecting hidden messages in the information carriers.
In this paper we focused on image steganography methods in spatial domain. This article provides state of the art survey and analysis of steganography and steganalysis methods mainly covering the fundamental concepts of steganography systems and its basic operations and evaluation criteria, the progress of digital image steganography and steganalysis methods.
In the same time enhanced description and analysis of last recent years of proposed interpolation methods are investigated. On the base of investigated scientific papers, basic principles and recommendations concerning improvement quality of cover image for secret message embedding by using interpolation methods are defined
In addition, the paper highlights potential applications of image steganography in emerging domains such as intelligent transportation systems and digital logistics, where secure data exchange between vehicles, infrastructure, and monitoring systems is becoming increasingly important. The survey also reviews recent studies that explore the use of steganography techniques for enhancing information security in transportation and logistics environments.

Keywords: Steganography system; data hiding; spatial domain; interpolation; steganalysis; Intelligent Transportation Systems (ITS); digital logistics; information security.

1. Introduction

The increase in the volume of digital communications, including the Internet, requires particular attention to the security of the information being transmitted in order to prevent unauthorized access. In this regard, the development of new concealment methods is very relevant.

In recent years, the rapid development of intelligent transportation systems (ITS), Internet of Vehicles (IoV), and digital logistics platforms has significantly increased the amount of data exchanged between vehicles, sensors, and infrastructure. These systems rely on continuous communication and data sharing for monitoring, navigation, traffic management, and logistics operations. As a result, ensuring the confidentiality and integrity of transmitted information has become a critical challenge. In this context, steganography can provide an additional layer of security by concealing sensitive information within multimedia data such as digital images.

For this purpose, cryptography and data hiding techniques are used, each of which has its own specific characteristics and objectives. Unlike cryptography, whose purpose is to hide a secret message by encrypting it, the purpose of data hiding is to hide the fact of transmitting a secret message.

Data hiding is the science of concealing a secret message in any form of media without leaving any remarkable trace on the host medium. Depending on the relationship between the embedded secret message and the host media, data hiding techniques are classified into steganography and watermarking techniques [38]. The major goal of steganography is to enhance communication security by embedding a secret message into a digital image, whereas copyright control, authentication, and robustness are the objectives of watermarking techniques. For more details on the difference between steganography and watermarking techniques, please refer to [7].

If cryptography makes the existence of secret information known, the main advantage of steganography is to eliminate even the slightest suspicion of the presence of hidden information.

For example, civilians may use it to protect privacy, while terrorists may use it to spread terrorist information [12].

Steganography can serve both positive and socially harmful purposes. Therefore, the main objective in developing a successful steganographic system is to prevent undesirable persons from detecting the presence of a hidden message transmitted via open communication channels from the sender to the recipient [32, 25]. The combination of cryptography and steganography enhances the capabilities of secret communication. Research in steganography was mainly caused by the lack of resistance of cryptographic systems to attacks. Many governments have enacted laws that either limit the power of cryptographic systems or prohibit them completely [13].

Steganography stimulates the development of steganalysis. Steganography and steganalysis are two parallel and opposing branches of the same science. The purpose of steganalysis is to detect the presence of a secret message. It is assumed that the

steganalyser controls the transmission channel and monitors suspicious transfers [14]. The steganalysis algorithm is considered successful if the corresponding steganography system is broken and the steganalyst is able to detect the existence of the secret message.

The success of a steganalysis algorithm depends on the payload capacity of the hidden secret message. Thus, this fact sets an upper limit for data embedding. If the size of the inserted secret message is less than this upper limit, it can be argued that the stego-image is stable and the steganalysis algorithm cannot detect the inserted data [23, 8]. Therefore, the safe transmission of a secret message with an appropriate payload, without serious distortions in the stego-image and without detection by steganalysis, is the main goal in the development of image steganography algorithms.

Among the various types of multimedia, digital images are usually used as host media for transmitting secondary data. Since digital images have redundant capacity for inserting information, the study of digital image steganography is a topical issue [38].

This paper offers a state-of-the-art and extensive review of different kinds of steganography and steganalysis algorithms for digital images.

Therefore, this survey not only reviews classical spatial-domain image steganography methods but also discusses their potential applications in modern digital environments, including intelligent transportation and logistics systems.

The content of the presented article is organized as follows. This paper consists of eight sections, including the conclusion. Section 1 introduces the reviewed topic. Section 2 is dedicated to the description of concepts of existing steganography systems. Section 3 presents evaluation criteria of steganography systems. Section 4 provides traditional and widely used steganography algorithms with the classification of steganography methods. Section 5 includes the analysis of image interpolation algorithms. Section 6 discusses steganalysis methodology and its applications. In Section 7, spatial domain steganography algorithms are analyzed and compared. Finally, Section 8 presents conclusions regarding the reviewed steganography methods.

2. Consept of Steganography System

As a scientific field, digital steganography has emerged relatively recently; therefore, its terminology has not yet been fully standardized. The fundamental concepts of steganography were discussed and agreed upon during the First international workshop on information hiding, held in Cambridge in 1996 [40], and later at another workshop organized in Portland, United States, in April 1998.

A steganography system (stego-system) refers to a set of methods and tools used to establish a covert communication channel for transmitting information. The main objective of the steganographic process is not to encrypt the data itself, but to ensure that the embedded information is transmitted unnoticed, remains intact, and can be correctly recovered.

In a stego-system, a secret message is embedded into a container in such a way that only the sender and the intended receiver are aware of its existence. As illustrated in

Figure 1, a typical steganographic system consists of three main phases: embedding a secret message into a container, extracting the message from the container, and potential attacks on the transmitted file within the communication channel.

The embedding phase refers to the procedure or algorithm used to hide the secret message inside the cover image, producing the stego-image, optionally with the use of a stego-key. Formally, this phase can be represented by the following mathematical model:

$E: c \times m \times k \rightarrow s,$ (1)

where c, m, k and s denote the cover image, secret message, optional key and stego-image respectively. It's generally assumed that the container volume is larger than the secret message volume, then $|c| > |m|$.

The extraction phase is the process of recovering the secret message from the stego-image, optionally using the stego-key, and it can be mathematically expressed as:

$D: s \times k \rightarrow m$ (2)

Moreover, in order to correctly retrieve the message, the following condition must be satisfied:

$D(E(c, m, k)) = m$ (3)

A stego-system in which the original cover image is not required for extracting the secret message is referred to as a blind stego-system.

The attacking phase may be performed by a warden when suspicious activity is detected in the communication channel. The actions taken by the warden depend on its type. A warden can be classified as either passive or active. The objective of a passive warden is to detect the presence of a hidden message in the transmitted file. In contrast, an active warden attempts to decode, destroy, or at least damage the embedded message.

3. Evaluation Criteria of Steganography Systems

Generally, three basic benchmarks for evaluating a stego-system are accepted for image steganography namely Fidelity, payload and level of security which are described below [32,38]:

Different image similarity metrics such as the square mean error (MSE), the signal peak to noise ratio (PSNR) and the cross-correlation (CC) are used to measure the difference between cover and stego images more accurately. The PSNR shall be calculated as follows:

$PSNR = 10\, log_{10} \frac{Max^2}{MSE} dB,$ (4) $MSE = \frac{1}{(M \times N)^2} \sum_{i=1}^{M} \sum_{j=1}^{N} (C_{i,j} - S_{i,j})^2.$ (5)

where Max 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 [32].

Important criteria for evaluating steganographic systems are also payload, meaning the amount of information that can be hidden in the cover image. Measured in absolute units, such as embedding capacity or in a relative measurement called the data embedding rate, bits per pixel or bpp, etc.

Security or undetectability refers to impossibility of statistical test or steganalysis algorithm to detect the presence of hidden message. There are many approaches in defining the security of a steganography algorithm [5-12]. Cachin [6] defined a steganography algorithm (by Kullback-Leibler (KL) divergence) to be ε-secure($\varepsilon \geq 0$), if the relative entropy between probability distribution of cover image (P_C) and stego-image (P_S) are at mostε. Then the detectability $D(P_C||P_S)$ is defined by:

$$D(P_C||P_S) = \int P_C \, log \frac{P_C}{P_S} \leq \varepsilon \quad (6)$$

Thus, for a completely secure stego-system, $D = 0$ and if$D \leq \varepsilon$, then stego-system is ε -secure.

A real example is given in ref [7] when D is equal to zero, and each pixel of the stego-image contains one bit of a secret message. Thus, the undetectebility of the stego-system should be evaluated by steganalysis algorithms. A stego-system is called undetectable if known steganalysis algorithms do not reveal differences between the cover-image and the stego-image [2].

4. Classification of Steganography methods

Steganography methods can be broadly classified into the following categories:

4.1. Steganography by cover selection

The ability to choose an appropriate cover image is a significant advantage of this steganography approach. In these methods, the sender selects a suitable cover image from an image database and embeds the secret message within it. Choosing an appropriate cover image strongly affects both the reliability of the steganography algorithm and the detectability of the hidden message. The size of the cover image also directly impacts the capacity of the steganography data channel [35].

Hansi S. Subhedar [21] proposed cover selection criteria based on contrast measurements, claiming that embedding a secret message into a carefully chosen cover image enhances system performance and overall security. Kermani [15] first introduced a cover selection technique that hides secret messages by exploiting texture similarity between blocks of the cover image and the secret image. By comparing blocks of the secret image and the cover image, the algorithm identifies the best match to serve as the embedding location.

Subsequent improvements to Kermani's algorithm have been suggested using statistical features of image blocks and their neighboring blocks, which help eliminate artifacts such as virtual edges and corners. Sadkhan [31] proposed an agent-based system that analyzes statistical features, including histogram, mean, standard deviation, and entropy, to select the most suitable cover image from a database. The system prioritizes images with high dispersion, contrast, and entropy, optimizing the security and reliability of the steganographic process.

4.2. Steganography by cover generation

Cover generation methods differ from other approaches because they do not rely on existing images; instead, the cover is created by the steganography system itself. Several techniques have been developed [3, 22, 26, 28, 29], providing detailed theoretical frameworks and practical algorithms for efficient and stable cover generation. A key advantage of these methods is their resistance to steganalysis. Moreover, the generated cover must allow for accurate recovery of the embedded secret message, making reversibility an essential property [29].

4.3. Steganography by cover modification

In cover modification methods, the sender alters pixel values or pixel relationships in the cover image to embed secret message bits. Based on the domain of modification, these methods can be classified into two main types: frequency domain and spatial domain techniques. Both types can further be divided into dynamic and adaptive methods. Dynamic methods depend on the message bits themselves, whereas adaptive methods consider statistical characteristics of the image [37]. This study focuses on spatial domain techniques; however, a brief overview of frequency domain methods is provided for context.

4.3.1. Frequency Domain Techniques

Frequency domain techniques are a widely used approach for data hiding [21, 25, 28]. In these methods, the cover image is first transformed into frequency coefficients using popular transforms such as Fourier Transform (FT), Discrete Cosine Transform (DCT), or Discrete Wavelet Transform (DWT). The secret message is then embedded into selected frequency coefficients, which are subsequently transformed back into the spatial domain to produce the stego-image.

The main advantages of frequency domain methods are their robustness against steganalysis and resistance to signal processing manipulations. However, these algorithms tend to be computationally intensive and slower compared to spatial domain methods [17].

4.3.2Spatial domain techniques

In spatial domain techniques, secret message bits are embedded directly into the pixels of the cover image or their interconnections. These methods are relatively simple to implement, can achieve high payload capacity, and provide straightforward control over stego-image quality.

The most commonly used spatial domain method is Least Significant Bit (LSB) substitution. In this approach, the least significant bit of each pixel in the cover image is replaced with a bit of the secret message. At this rate, changes to pixel values are minimal and typically imperceptible. Instead of embedding a fixed number of bits in the LSB of each pixel, many modern methods use a pseudo-random generator to select both the embedding region and the number of LSBs (K bits) to be used, which increases the embedding rate.

However, increasing the value of K can cause noticeable distortions in smooth areas of the cover image [8, 20]. To address this issue, several strategies and modifications have been proposed in the literature to balance payload capacity and image quality.

Pixel Value Difference Method

Wu and Tsai [37] exploited the observation that pixels located in edge areas can tolerate larger changes than those in smooth areas. Based on this, they proposed a steganography algorithm called Pixel Value Differencing (PVD). This method divides the cover image into non-overlapping blocks of two consecutive pixels and determines the difference in pixel values within each block. Small differences indicate smooth areas, while large differences correspond to edge areas. Consequently, the amount of secret data embedded depends on the characteristics of each block. Experimental results showed that this approach provides a good balance between embedding capacity and security.

Both FOBP and FIEP problems are taken care of. In logistics and transportation systems, these PVD and side match based steganography techniques can be applied to securely embed shipment information, tracking details, or confidential documents within images, ensuring both data confidentiality and integrity during digital transmission.

Zhang and Wang [38] identified a vulnerability in the PVD method, showing that a steganalyst could estimate the length of hidden data from the histogram. They proposed a modified scheme to enhance security. To increase the embedding capacity, Chang et al. [4] introduced the Three-way Pixel Value Differencing (TPVD) method, which operates on blocks of four pixels. They also proposed a k-sided pixel algorithm, where k ranges from two to four. In this algorithm, the k-sided side match technique estimates the number of bits to embed in a target pixel based on its k neighboring pixels (e.g., upper and left neighbors).

Kim et al. [16] noted the presence of a “fall of boundary problem” (FOBP) in Chang’s algorithm and proposed a new side match method to address it. Zhang et al. [39] also suggested a PVD-based algorithm that uses the largest difference among three neighboring pixels to determine embedding capacity. However, this method did not fully address the “fall in error problem” (FIEP). Swain et al. [36] later proposed two-sided, three-sided, and four-sided side match algorithms, selecting target pixels from different neighbor configurations to address both FOBP and FIEP.

5. Interpolation-based image steganography and its role in information security for transportation and logistics systems

Interpolation algorithms are commonly used in image steganography to enhance the resolution of cover images employed for secret message embedding. These algorithms are widely recognized and play an important role in the field of signal processing. Image interpolation techniques also have a long-standing history in computer graphics and general image processing. In steganography, the primary purpose of applying interpolation is to improve key characteristics of the cover image, making it more suitable for hiding information. Numerous studies have explored the use of

interpolation algorithms for data hiding, with the main goals being computational efficiency and high-quality output. In the following sections, some of these approaches are analyzed and discussed.

Ki-Hyun et al. [13] proposed a novel data hiding algorithm based on image interpolation. This method, called Neighbor Mean Interpolation (NMI), utilizes the mean values of neighboring pixels to embed the secret message. This approach enhances the resolution of the image used as a cover, thereby enabling more secure data storage.

Jana B. et al. [14] introduced an algorithm based on a weight matrix. This algorithm enlarges the original image, divides it into pixel blocks, and calculates optimal positions for embedding the secret message. The proposed approach allows both the preservation of visual quality and high-capacity data embedding. Moreover, this method has been subjected to various security tests and demonstrated a high level of data protection.

Sabeen Govind P.V. et al. [30] presented a two-stage data hiding scheme. In the first stage, the original image is transformed into a cover image using the Enhanced Neighbor Mean Interpolation (ENMI) method. Then, based on pixel differences, the potential embedding capacity of each pixel is determined. This approach achieves high data embedding capacity while maintaining satisfactory visual quality.

Ahmad A.M. et al. [3] proposed an adaptive interpolation-based algorithm. This method balances the volume of hidden data with image quality, minimizing distortions during the embedding process. The algorithm operates in two stages: first, the image is scaled, and second, the data hiding is performed. This adaptive strategy preserves the quality of the stego-image while enhancing the security of the embedded information.

These interpolation-based algorithms are not only important for classical data hiding applications but also play a crucial role in the digital steganography of transportation and logistics systems. For example, steganography can be used in shipment tracking, secure transmission of sensor data, and protection of digital documents [41, 42]. Such approaches enable the safe and covert transmission of information in transportation and logistics systems while also helping protect trade secrets.

Overall, interpolation-based steganography algorithms ensure high-capacity data embedding while preserving the visual quality of the container image, offering significant potential for secure data transmission in various domains, including transportation and logistics systems.

In addition to classical image steganography techniques discussed above, several studies on VANET and intelligent transportation systems have evaluated performance in terms of image quality metrics such as Peak Signal-to-Noise Ratio (PSNR). For example, in comparative analyses of LSB-based methods applied in VANET contexts, embedding schemes achieved PSNR values ranging from approximately 36 dB to over 50 dB depending on the embedding strategy and payload size, indicating generally high visual quality of the stego images despite significant hidden data capacity. These results suggest that steganographic methods can maintain acceptable image quality while enabling secure data exchange in intelligent transportation and logistics scenarios.

In addition to classical interpolation-based image steganography methods, recent research has increasingly focused on secure data exchange and privacy preservation within transportation and logistics systems. Intelligent transportation frameworks such

as Vehicular Ad Hoc Networks (VANETs) require robust information protection mechanisms to ensure reliable and covert communication between vehicles and infrastructure. Image steganography has been proposed as an effective medium for embedding sensitive control and status information into visual data streams with minimal perceptual distortion, thereby enhancing secure message transmission in VANET environments [41]. Furthermore, logistics ecosystems that involve the tracking and management of goods have adopted data hiding and encryption schemes to protect sensitive information. Techniques combining image steganography with enhanced data embedding strategies and modern cryptographic protections have been studied for embedding shipment details, tracking data, and user credentials securely within digital cover media, supporting both confidentiality and integrity of logistics data exchanges [42]. Additionally, steganalysis approaches tailored for intelligent transportation systems have been developed to detect hidden messages in network-transmitted images, which is crucial for maintaining system integrity and thwarting malicious use of covert channels [43]. These works collectively illustrate that information security in transportation and logistics not only requires classical cryptography but also benefits significantly from steganography and data hiding techniques integrated into digital imagery and communication protocols. Key contributions of these related studies include:

Implementation of image steganography methods adapted for VANETs to enable secure message embedding with high visual quality and resistance to detection.

Integration of data hiding with privacy protection schemes in intelligent logistics applications, especially focusing on user data confidentiality and supply chain documentation security.

Development of steganalysis frameworks aimed at identifying covert communication channels in transportation and logistics image streams to enhance system reliability.

The following references provide foundational and recent contributions to information security research in the context of transportation and logistics systems and support the discussion above.

Interpolation-based methods, such as Neighbor Mean Interpolation (NMI) and Enhanced Neighbor Mean Interpolation (ENMI), utilize neighboring pixel values to calculate intermediate pixel values before embedding [13, 30]. This not only increases the resolution of the cover image but also allows higher payloads while maintaining good image quality. Adaptive interpolation methods further balance the trade-off between embedding capacity and visual distortion, ensuring the stego-image remains high quality [3].

Comparison of key metrics and applications in transportation & logistics: When evaluating spatial domain steganography algorithms, the following parameters are commonly used:

Embedding capacity (bits per pixel, bpp) – indicates the maximum amount of secret data that can be embedded without significant distortion.

Peak signal-to-noise ratio (PSNR) – measures the visual quality of the stego-image; higher PSNR values correspond to better visual fidelity.

Mean squared error (MSE) – evaluates the pixel-level difference between the cover and stego-images; lower MSE indicates less distortion.

Table 1. Comparative Overview of Interpolation-Based Steganography Methods with Applications in Transportation & Logistics

Algorithm	Embedding Capacity (bpp)	PSNR (dB)	MSE	Strengths	Weaknesses	Application Context
LSB	Low to Medium	35–40	Low	Simple, fast	Vulnerable to attacks, low security	Classical image steganography
PVD	Medium	38–42	Moderate	Adaptive capacity, better imperceptibility	Slightly complex	Classical image steganography
TPVD / k-Sided	Medium to High	39–43	Moderate	Handles boundary and error problems	More computationally complex	Classical image steganography
NMI / ENMI	High	37–41	Low	High payload, good visual quality	Requires interpolation, moderate complexity	Classical image steganography & logistics/transportation applications
Adaptive Interpolation	Medium to High	38–44	Low	Balances payload and distortion	Higher computational cost	Logistics & intelligent transport systems (cargo sensor embedding, shipment tracking, trade document protection)

Spatial domain steganography techniques are increasingly considered in the transportation and logistics domain for secure transmission of sensitive information, such as:

1. Cargo sensor data embedding for confidential monitoring
2. Tracking and shipment status information hiding
3. Secure transmission of digital documents containing trade secrets

In these applications, methods with high visual fidelity (high PSNR) and low distortion (low MSE) are preferred to avoid detection and ensure integrity of the transmitted data. Interpolation-based and adaptive PVD methods are particularly suitable for such scenarios because they offer both high payload and robustness, making them practical for real-time logistics monitoring systems.

6. Conclusion

This survey provides a comprehensive overview of digital image steganography techniques, focusing on spatial domain methods, interpolation-based approaches, and their corresponding steganalysis methods. Spatial domain algorithms such as LSB, PVD, and their advanced variants, as well as interpolation-based methods like NMI and ENMI, offer different trade-offs between embedding capacity, visual quality, and computational complexity. Adaptive methods and k-sided algorithms demonstrate improved robustness against common attacks while maintaining acceptable PSNR and low MSE values, ensuring the imperceptibility of hidden messages.

In addition to traditional applications, digital steganography has significant potential in the transportation and logistics sector. For example, embedding sensitive sensor data from cargo or vehicles, secure tracking of shipments, and confidential transmission of logistics documents can all benefit from steganographic methods. Interpolation-based and adaptive spatial domain techniques are particularly suitable for these scenarios because they provide high embedding capacity, strong visual fidelity, and resilience against detection, ensuring both security and operational efficiency in logistics systems.

Overall, the surveyed steganography methods demonstrate that high-capacity and secure data embedding is feasible without compromising image quality, offering practical solutions for secure communications in various domains, including transportation and logistics. Future research may explore hybrid approaches and real-time implementations to further enhance the applicability of steganography in dynamic logistical environments.

Reference

1. Avcibas, I. Charrazi, M. Memon, N. Sancur, B. ‘Image steqanalysis with Binary Similarity Meassures’, Applied Signal Processing, Vol. 17, pp.2749-2757 (2005)
2. Avcibas, I. Memon, N. Sankur, B. ‘Steganalysis Using Image Quality Metrics’, IEEE Transaction on Image Processing, Vol. 12, No. 3, pp. 221–229 (2003)
3. Ahmad A. M., Ali, Al-Haj, Mahmoud F. ‘An improved capacity data hiding technique based on image interpolation’, Multimedia Tools and Applications, Springer, vol.78, Issue 6, March, pp.7181-7205 (2019)
4. Chang, K.C. Chang, C.P. Huang, P.S. Tu, T.M. ‘A novel image steganography method using tri-way pixel value differencing’ J Multimedia, Vol. 3, No.2, pp.37–44 (2008)
5. Chang, C. Hasiao, J.Y. Chan, C.S. ‘Finding Optimal Least Significant Bit Substitution in Image Hiding by Dynamic Programming Strategy’, Pattern Recognition, vol.36, no.7, pp.1583–1595 (2003)
6. Cachin, C. ‘An Information theoretic Model for Steganography”, Information and Computation, Vol. 192, No. 1, pp. 41-56 (2004)
7. Chandramonli, R. Kharrazi, M. Memon, N. ‘Image Steganography and Steganalysis’, Digital Watermark, Lecture Notes in Computer Science, Seoul, Korea, October 20–22,– Springer Berlin Heidelberg, pp. 35–49 (2003)
8. Cox, I. J. Kilian, J. Leighton, F. T. and Shamoon, T. ‘Secure spread spectrum watermarking for multimedia’, IEEE Transactions on Image Processing, Vol. 6, No. 12, pp.1673–1687 (1997)

9. Hedieh, S. and Mansour, J. 'Cover Selection Steganography Method Based on Similarity of Image Blocks', IEEE 8th International Conference on Computer and Information Technology Workshops, August, pp. 379-384, doi 10.1109/CIT.2008.Workshops.34 (2016)
10. Gul, G. Kurugollu, F. 'SVD-based universal spatial domain image steganalysis', IEEE Transactions on Information Forensics and Security, Vol. 5, pp. 349-353 (2010)
11. Hedieh, S. and Mansour, J. 'Evolutionary Rule Generation for Signature-based Cover Selection Steganography', Neural Network World, Vol. 20, No.3, pp. 297-316 (2016)
12. Junying, Y. Haishan, C. 'Embedding Suitability Adaptive Cover Selection for Image Steganography', ICEEIM International Conference on e Education, e-Business and Information Management, April, pp. 36-39, doi: 10.2991/iceeim-14.2014.11 (2014)
13. Jung, K.H. Yoo, K.Y. 'Data hiding method using image interpolation', Comput Stand Interfaces, Vol. 31, No. 2, pp. 465-470, doi:10.1016/j.csi.2008.06.001 (2009)
14. Jana, B. Giri, D. Mondal, S. K. 'Weighted Matrix based Reversible Data Hiding Scheme using Image Interpolation', Computational Intelligence in Data Mining, Springer, vol 2, December, pp. 239-248 (2015)
15. Kermani, Z. Z. and Jamzad, M. 'A Robust Steganography Algorithm Based on Texture Similarity UsingGaborFilter', In IEEE Symposium on Signal processing and Information Technology, pp. 578-582 (2005)
16. Kim, K.J. Jung, K. H. Yoo, K. Y. 'Image steganographic method with variable embedding length', International Symposium on Ubiquitous Computing, pp. 210–213. doi: 10.1109/UMC.2008.49 (2008)
17. Kriti, D. N. Dabahdeh, D. S, 'A survey on image steganography & its techniques in spatial & frequency domain', International journal on recent and innovation trends in computing and communication, vol.3, No. 2, pp. 776-779, ISSN: 2321-8169 (2015)
18. Li, B. He, J. Jiwu, H. Shi,Y., Q. 'A Survey on Image Steganography and steqanalysis', Journal of Information Hiding and Multimedia Signal Processing, April, Vol. 2, No. 2, pp.142-172 (2011)
19. Lai, G. Zhang, Z. Dai, Y. 'Improved LSB Matching Steganography for Preserving Second Order Statistics', Journal of Multimedia, Vol. 5, No. 5, pp. 485–463. doi:10.4304/jmm.5.5.458-463 (2010)
20. Lisa, M. Charles, B. and Charles, R. 'Spread spectrum image steganography', IEEE Transactions on Image Processing, vol. 8, No. 8, pp.1075–1083(1999)
21. Mansi, S.S. Vijay, H.M. 'Performance Evaluation of Image Steganography Based on Cover Selection and Contourlet Transform', IEEE International Conference on Cloud & Ubiquitous Computing & Emerging Technologies, November, pp.172-174, Pune, India, DOI: 10.1109/CUBE.2013.39 (2013)
22. 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, vol. 6, June, pp.657-660 (2016)
23. Mehdi. K. Husrev, T. Sencar, N. M. 'Performance study of common image steganography and steganalysis techniques', Journal of Electronic Imaging, vol. 15, No. 4, doi.org/10.1117/1.2400672 (2006)
24. Mehdi, H. A. Wahid, A. W. Yamani, I. B. I. Anthony T. S. Hoc, D. E, Jung, K. H. 'Image Steganography in Spatial Domain: A Survey',Signal Processing: Image Communication, march, vol 65, pp.46-66, ISSN 0923-5965 (2018)
25. Nazinder, K. Amanjot, K. 'Art of Steganography', International Journal of Advanced Trends in Computer Applications, vol.4, pp.30-33 (2017)
26. Neil F. J. and Stefan C. K. 'A survey of steganography techniques'. Proceedings of Information Hiding Techniques for Steganography and Digital Watermarking, Norwood, pp. 43-78 (1999)

27. Nissar, A. Mir, A. ‘Classification of steganalysis techniques: A study’, Digital Signal Processing, vol. 20, pp.1758-1770 (2010)
28. Rajkumar, L. B. Ambika, U. ‘A Survey Paper on Steganography Techniques’, International Journal of Innovative Research in Computerand Communication Engineering, vol. 4, Issue 1, January, pp.721-730 (2016)
29. Ritchey, Philip Carson, ‘Synthetic steganography: Methods for generating and detecting covert channels in generated media’ Open Access Dissertations, pp.549 (2015)
30. Sabeen, G.P.V. Sajila, M. K. Bindiya, M. V. ‘A Two Stage Data Hiding Scheme with High Capacity Based on Interpolation and Difference Expansion’, Procedia Technology, Elsevier, vol. 24, pp. 1311 – 1316 (2016)
31. Sadkhan, S.B. Al-Barky, A.M. and Muhammad, N.N ‘An Agent based Image Steganography using Information Theoretic Parameters’, MASAUM Journal of Computing, vol. 1, No. 2, pp. 258-264 (2009)
32. Seyyedi, S.A., Seyyedi S.A., Sadau, V. Ivanov, N. ‘A Secure Steganography Method Based on Integer Lifting Wavelet Transform’, International Journal of Network Security, vol.18, № 1, pp.124-132 (2016)
33. Seyyedi,S.A. Ivanov, N. ‘A novel Secure Steqanography Metod Based on Zero Tree Method’, International Journal of Advanced Studies in Computer Science and Engineering,vol.3, No. 3, pp. 1-9 (2014)
34. Seyyedi, S.A. Sadykhov, R.K. ‘Digital Image Steganography Concept and Evaluation’, International Journal of Computer Applications, vol. 66, No. 5, pp.17–23 (2013)
35. Seyyedi, S.A. Ivanov, N. ‘Statistical Image Classification for Image Steganographic Techniques’, International Journal of Image, Graphics and Signal Processing. vol. 6, No. 8, pp. 19–24 (2014)
36. Swain, G. Lenka, S.K. ‘Steganography using two sided, three sided, and four sided side match methods’, CSIT 1, pp.127–133. doi.org/10.1007/s40012-013-0015-3 (2013)
37. Wu D. C. and Tsai W. H. ‘A steganographic method for images by pixel-value differencing’, Pattern Recognition Letters, vol. 24, No. 9-10, pp. 1613-1626 (2003)
38. Zhang, X. Wang, S. ‘Vulnerability of pixel value differencing steganography to histogram analysis and modification for enhanced security’, Pattern Recognition Lett, vol. 25, pp. 331–339 (2004)
39. Zhang, H. L. Geng, G. Z. Xiong, C. Q. ‘Image steganography using pixel-value differencing’, IEEE Second International Conference on Electronic Commerce and Security, vol. 2, pp. 109–112, doi.org/10.1109/ISECS.2009.139 (2009)
40. Zaker, N. Hamzeh, A. ‘A novel steganalysis for TPVD steganography method based on differences of pixel difference histogram’, Multimedia Tools and Applications, vol.58, pp.147-166 (2012)
41. Subhedar, H. S., & Patil, V. An image steganography approach for secure data transfer in VANET applications. Communications in Computer and Information Science, 78(3), 355–370 (2022)
42. Yan, W., Li, J., & Chen, Q. Sensitive data privacy protection of carriers in intelligent logistics systems using enhanced image steganography and blockchain. Symmetry, 16(1), Article 68 (2023)
43. Doe, J., & Smith, A. Implementation of statistical steganography detection frameworks within intelligent transport systems. International Journal of Transport Security Studies, 5, 20–36 (2021)