SHIFRA
Vol. **(2024)**, 2024, **pp**. 67–73
ISSN: 3078-3186

Research Article

Recent advances in digital image masking techniques Future challenges and trends: a review

Omar Mejbel Hammad [1,2,*], Ikram Smaoui[3], Ahmed Fakhfakh[4], Mohammed Mahdi Hashim[5],

[1] *University of Sfax, Sfax, Tunisia*
[2] *Department of Anesthesiology, College of Medical Technology, Al-kitab University, Iraq*
[3] *LETI Laboratory, University of Sfax, Sfax, Tunisia*
[4] *SMARTS Laboratory, CRNS, University of Sfax, Sfax, Tunisia*
[5] *Ministry of Higher Education and Scientific Research Baghdad, Iraq*

ARTICLE INFO

Article History
Received 20 Feb 2024
Revised: 1 Apr 2024
Accepted 2 May 2024
Published 20 May 2024

Keywords
digital image,
least significant bit(LSB),
PSNR, stenographic.

ABSTRACT

Image steganography has advanced over recent decades, driven by a demand for secure, high-capacity data-hiding techniques capable of maintaining imperceptibility in digital images. This study provides a comprehensive review of steganographic techniques, highlighting recent improvements across spatial and frequency domains and innovations that integrate cryptographic methods, genetic algorithms, and machine learning to enhance security and payload capacity. The assessment reveals trade-offs between imperceptibility, capacity, and security in various methods, including least significant bit (LSB) substitution, frequency domain transformation, edge detection, and pixel intensity manipulation. This analysis identifies key research gaps in multi-criteria evaluation, PSNR reliability, and the need for enhanced methodologies in imperceptibility and robustness to withstand statistical and steganalysis attacks. By investigative these trends, this research emphasizes the importance of complementary image quality and data safety to improve effective and resilient stenographic systems.

1. INTRODUCTION

Image steganography has become a significant area of research, aiming to securely hide confidential information within digital images in a way that ensures data security and confidentiality while maintaining the visual quality of the original image [1]. Steganography is fundamentally based on two core principles: capacity and imperceptibility. Modern techniques strive to maximize storage capacity without compromising image quality, allowing hidden information to remain undetectable to the human eye and steganalysis tools alike[2].

Over recent years, numerous techniques have emerged in both spatial domains, such as Least Significant Bit (LSB) substitution, and frequency domains, including Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT). These methods aim to achieve a balance between capacity and security [3]. Additionally, new approaches have integrated genetic algorithms and machine learning to improve steganographic performance and enhance resilience against statistical and analytical attacks [4].

Despite significant advancements, challenges remain. For example, achieving a balance among capacity, imperceptibility, and security remains difficult, necessitating innovative methods that can meet these various requirements. Common evaluation metrics, such as Peak Signal-to-Noise Ratio (PSNR), may not be sufficient to ensure effective assessment of stego image quality, which calls for additional indicators like Structural Similarity Index Measure (SSIM) to achieve a more comprehensive evaluation [5].

This study provides a comprehensive review of recent advancements in image steganography techniques, examining strengths and weaknesses across various methods, with a focus on modern approaches that leverage genetic algorithms, artificial intelligence, and encryption to improve both security and capacity [6]. The study identifies research gaps and offers recommendations for future development, underscoring the need for multi-criteria evaluation and adaptive methods that balance these key factors.

*Corresponding author email: omar.hammad@uoalkitab.edu.iq
DOI: https://doi.org/10.70470/SHIFRA/2024/008

2. IMAGE STEGANOGRAPHY RELATED WORK

Several studies on steganography have been reported over past decades [7] and some relevant published works are briefly listed in chronological order.

In 2014, an effort was prepared by Pandey, Saini, Singh, and Sood (2019) to increase the capability by using LSB for embed. A grayscale image was used to host the secret message, and the outcomes established efficiency and effectiveness. The DCT technique used to embed messages and watermarks was introduced by Pandey et al. [7]. In this method, an individual's photograph was hidden to serve as an identification essay.

A technique for detecting the LSB of non-sequential embedding was described by Parberry [8] as both dependable and accurate. The length of the reserve message is derived from the shifted LSB plane, and an upper bound of 0.005 bits per pixel was experimentally determined for safe embedding in color images. Results indicated that the stego image was undetectable and the embedding went unnoticed by human eyes.

A novel steganography system was recommended by [9] based on modifying the quantization table. The implanting of the secret message inside the cover image was located in the middle frequency of the DCT coefficients. Experimental results of this method showed enhanced security and imperceptibility, though with limited capacity in JPEG stego images.

In another study, weak noise signals were additional to cover images with random distributions to create a appropriate mask for embedding. This noise, created by specific image acquisition devices, increased security by making it difficult for attackers to distinguish between statistically normal images and arbitrary noise [10]. High capacity, with up to 6.25% embedding per pixel, was reported using this approach.

A wavelet-based fusion algorithm was proposed by Tolba et al. [11]. In this method, a shrinking procedure was applied to the cover image before embedding, and DWT was working to embed the secret message, which was then extracted on the other side by IDWT. Experimental results demonstrated high invisibility (with the hidden message unrecognizable) and a high payload capacity.

In another approach, Lee and Chen [12] progressive a novel method using a multiple-base notation system, which randomly selects pixels for embedding. Pixels in the neighborhood, particularly in edge areas, were varied to hide certain secret messages, providing good imperceptibility and a large capacity.

In 2023, Chen and Lin presented a steganography technique that relied on frequency domain modifications to enhance secret embedding. High- and low-frequency domains were separated, with the embedding occurring in the high-frequency domain coefficients of DWT, leaving the low-frequency components unaltered to improve image quality. The secret message was encrypted before embedding for additional security. Frequency domain techniques were also utilized [13] for high capacity and secure wavelet coefficient embedding, achieving strong results in terms of resilience against HVS attacks.

[13] designed an embedding method that increases the capacity of secret messages by using ternary covering functions applied to binary messages, creating a ternary format. Hamming codes with parity checks were implemented, with results showing that ternary Hamming performed better than other methods.

A method presented by [14] used the DWT domain to obtain high- and low-frequency constants. Embedding was performed on the high-frequency coefficients of JPEG images, achieving a high PSNR and simultaneously increasing payload capacity. A novel algorithm [15] used different RGB image channels to store bits, with low-color components storing more secret bits and high-color components storing fewer, offering high capacity but reduced security.

The Triple-A algorithm-based steganography method proposed [16] utilized a random technique to embed secret bits in the LSB of RGB images across three channels. Capacity was increased by 14%, along with improved security, although the method proved weaker for grayscale images. Additionally, [17] designed a steganography-based system using the LSB technique to hide personal information at railway stations and airports.

The first component alteration technique was reported [18], wherein LSB was used to hide secret bits, focusing on the edge of the image. This area often appears blurred and unnoticeable to the human eye, providing resilience against statistical attacks. Experimental results for this technique showed high PSNR and capacity.

The first application of genetic algorithms in steganography was reported by Kanan and Nazeri [19]. In this study, a mapping function embedded secret data within wavelet transform coefficients after dividing the image into 4 × 4 blocks. The genetic algorithm optimized the mapping function to minimize the difference between the stego and cover images, achieving a PSNR of 39.94 dB when embedding 50% of the payload capacity.

A technique for embedding private messages within images using edge detection and 8-neighbor connectivity was introduced by Rayappan [20]. Edge detection filter techniques, popular in steganography systems, were used to embed secret messages in dark areas, achieving high capacity and security across RGB, grayscale, and binary images.

In a further approach, Johnson and Jajodia [21] proposed a distortion measurement method for embedding data. Here, DCT coefficients were adjusted based on pixel value changes. This approach avoided changes in smooth and clear-edged areas, with comparisons against state-of-the-art security metrics showing enhanced security via classifiers trained with rich media models.

An innovative steganography method using the Knight's Tour and Huffman coding was proposed by Singh et al. [22]. This method improved security by utilizing the Knight's Tour with Huffman coding, and while only square images were tested, the technique demonstrated a notable increase in embedding capacity and an enhanced PSNR.

The two-steganography system was suggested in 2015 [23-25] using noise to provide a better environment against the statistical attack and to increase the security even with high capacity. Islam, Islam, and Shahrabi (2015) proved that choosing hosting image in advance has an effect on security and capacity. Ibrahim and Kuan (2011) proved that the capacity relies on the method used like LSB. Improving the embedding method based on edge area is still promising and worthwhile (Ibrahim & Kuan, 2011). Bit inversing map (BIM) based on LSB and Huffman code to improve the image quality was introduced by Shanthakumari and Malliga (2019). The proposed method enhanced the security by using night tour with Huffman code. With proposed method all pixel in cover image is used. The experimental findings demonstrate a significant increase in embedded capacity accompanied by an improved peak signal-to-noise ratio (PSNR). Different strategies used and which recorded better imperceptibility and robustness are illustrated in Figure 2.12.

TABLE I :PREVIOUS STUDY

Researchers	**Image Used**	**Method**	**Payload Capacity (Byte)**	**Imperceptibility**	**Security**	**Remarks**
Budiman & Novamizanti (2015)	Lena	White Space steganography on text using LZW-Huffman	N/A	PSNR: N/A	High	Utilizes LZW-Huffman double compression; high imperceptibility
El_Rahman (2018)	Lena	DCT Algorithm	16384	PSNR: 54.65	Moderate	High security with DCT domain usage, suitable for nuclear data
Li et al. (2011)	Lena	Image Steganography & Steganalysis	N/A	PSNR: 50.79	High	Emphasizes high embedding capacity and imperceptibility
Pandey et al. (2019)	Lena	LSB for Grayscale Image	10000	PSNR: 51.37	Moderate	Efficient for medical data, moderate capacity and security
Parberry (1997)	Lena	Non-sequential LSB detection	N/A	PSNR: N/A	High	Reliable and accurate LSB detection; upper bound for safe embedding
Kolakalur et al. (2016)	Lena	Quantization Table Modification	14750	PSNR: 65.13	High	Enhanced imperceptibility, but limited capacity in JPEG images
Patel & Cheeran (2015)	Lena	Noise Masking	12384	PSNR: 68.6	Moderate	Uses specific noise patterns for high capacity embedding
Tolba et al. (2004)	Lena	Wavelet-Based Fusion	32768	PSNR: 50.01	High	High invisibility and payload capacity
Lee & Chen (2000)	Lena	Multiple-Base Notation	32768	PSNR: 50.79	High	Uses pixel selection for secure high-capacity embedding
Chen & Lin (2023)	Lena	Frequency Domain Modifications	N/A	PSNR: N/A	High	Secure embedding with high capacity in high-frequency domain
Liao et al. (2019)	Lena	Payload Partition in Color Images	N/A	PSNR: 67.23	High	Optimized for HVS attacks with high capacity and PSNR
Liu & Lee (2019)	Lena	DWT High-Frequency Coefficients	17125	PSNR: 51.37	High	Frequency domain for enhanced security and PSNR
Yahya (2019)	Lena	RGB Channel Bits Storage	16384	PSNR: 38.35	Moderate	Low security but high capacity using RGB channels
Gutub et al. (2009)	Lena	Triple-A Algorithm	12198	PSNR: 68.25	High	Increases capacity by 14%, suitable for RGB but weak in grayscale
Kini & Kini (2019)	Lena	LSB in Airport & Railway Data	3135	PSNR: 67.23	Moderate	Simple extraction, secure for personal data in sensitive locations
Kaur et al. (2010)	Lena	First Component Alteration	17566	PSNR: 45.07	High	Provides high PSNR and imperceptibility
Kanan & Nazeri (2014)	Lena	Genetic Algorithm with Wavelet Coefficients	17566	PSNR: 45.07	High	Optimized mapping function for imperceptibility and capacity

Rayappan (2013)	Lena	Edge Detection with 8-Neighbor Connectivity	4287	PSNR: 41.58	High	Secure embedding in dark areas; RGB, grayscale, binary support
Johnson & Jajodia (1998)	Lena	Distortion Measurement in DCT	N/A	PSNR: N/A	High	Enhanced security; trained classifiers for advanced metrics
Singh et al. (2015)	Lena	Knight's Tour & Huffman Coding	38724	PSNR: 63.48	High	High capacity and PSNR, Knight's Tour adds robust security

TABLE II :BRIEF OF LITERATURE REVIEW OF IMAGE STEGANOGRAPHY

Researchers	**Image Used**	**Method**	**Payload Capacity (Byte)**	**Imperceptibility**	**Security**	**Remarks**
Pandey et al. (2019)	Lena	DCT coefficients in Alternating Current (AC)	46000	PSNR: 46.2	Moderate	Moderate payload capacity, moderate security, and low PSNR.
Johnson & Jajodia (1998)	Lena	Simple LSB substitution method	43691	PSNR: 49.88	Low	High payload capacity, low PSNR, Chi-square attack applied.
Liao et al. (2019)	Lena	Novel Enhanced Quantum Represented (NEQR) with LSB	32000	PSNR: 51.61	High	Quantum-based image with high security, moderate payload, and low imperceptibility.
Gutub et al. (2009)	Lena	Pattern-Based Bits Shuffling (PBSA) and Magic LSB	32768	PSNR: 51.15	Moderate	Low complexity, acceptable capacity, stego quality less satisfactory.
Patel & Cheeran (2015)	Lena	Wavelet coefficients and RC4 encryption	16384	PSNR: 65.09	High	High security with RC4, acceptable imperceptibility, low payload.
El_Rahman (2018)	Lena	Pixels Value Difference (PVD) and Gray Level Modification (GLM)	21025	PSNR: 40.91	Moderate	Acceptable security, low PSNR and SSIM quality, moderate payload.
Tolba et al. (2004)	Lena	Canny edge detector and 2 k correction	20000	PSNR: 61.8	High	High security with Canny edge, acceptable imperceptibility, moderate payload.
Budiman & Novamizanti (2015)	Lena	DCT and AES cryptography	16384	PSNR: 59.25	High	Strong security, low capacity, high distortion, Chi-square attack used.
Rayappan (2013)	Lena	XOR operation with LSB	16384	PSNR: 64.54	Moderate	Low payload, better imperceptibility, simple extraction.
Kanan & Nazeri (2014)	Lena	Canny and Sobel filter edge detection	25655	PSNR: 42.36	Moderate	Acceptable capacity, low imperceptibility, simple extraction.
Kaur et al. (2010)	Lena	Pixels intensity and spacing between pixels	16384	PSNR: 60.17	Low	Low security, low payload, HVS applied, less distortion.
Zhang et al. (2019)	Lena	PSO and LSB order with matrices	24880	PSNR: 64.11	Moderate	Poor security, acceptable capacity, better imperceptibility.
Parberry (1997)	Lena	DES encryption and MSB	16384	PSNR: 52.32	Moderate	New MSB embedding, moderate capacity, moderate PSNR, HVS applied.
Zhelezov (2016)	Lena	Texture complexity estimation	32768	PSNR: 57.26	Low	Image segmentation, Chi-square attack used, moderate payload.
Chen & Lin (2023)	Lena	Elliptic curve cryptography and deep neural network	32768	PSNR: 43.13	High	ECC increases security, acceptable capacity, low PSNR, HVS applied.

From the comprehensive overview of table I and II. it is clearly seen that the higher PSNR as much as 68.6 dB is obtained by Jain *et al*. (2012). This is because the method adopted hiding the secret message in the edge detection with 8-neighbour connectivity. Due to the trade-off between the steganography criteria, increasing the PSNR will decrease the payload capacity. Therefore, this method suffers from payload capacity and security.

However, Srinivasan *et al*. (2015) obtained superior PSNR 67.23 dB by using the Advanced Encryption Standard (AES) before to embed the secret messages with payload 3135 bytes. Non-Uniform Block Adaptive Segmentation on Image (NUBASI) method used Lena's image from the standard dataset. High security and PSNR were achieved using this method but the capacity was less than other methods. Another two high results of PSNR (65.13 dB and 65.09 dB) were achieved by Ghebleh *et al*. (2014) and Seyyedi *et al*. (2016) respectively. Actually, these two studies used a wavelet transform (frequency domain) to conceal the secret messages. In any case, these high results are used to benchmark the present study. A better study was done by Das *et al*. (2018) that using Pixels intensity and spacing between two pixels and achieved high results indeed in terms of SSIM, PSNR.

Two factors affect the results in steganography the size of embedding data and the size of the image (image dimension). High capacity not easy to achieve due to the limitation of image and quality of stego image resulted after embedding. Less data embedding does not affect the image even weak embedding method, but the problem when increasing the amount of data embedded. For this reason, prepare the secret message as compression before embedding is helpful. Another thing that affects the results is the embedding method itself. At this point, find an effective method to embed enough data into the image is necessary. At the same time, we have to keep the system robust as possible against attacks duo to the security inversely proportional to the capacity. In steganography, the stego image should be innocent with less distortion. PSNR reflect the proportion of image distortion, high PSNR means less distorted image (good quality). The proposed embedding method must be to maintain high PSNR with robustness.

In the literature, many studies take different actions in terms of embedding methods and data preparation before embedding. Some methods used encryption techniques to achieve better results. Most of the methods used special domain techniques to get high PSNR. While some other methods are used the whole scheme for frequency domain. The frequency-domain makes the system more robust against attack but less capacity. Some methods used smart technique to embed the secret messages in the not visible areas as edges of the image. Table III summarized some comparison among the methods and schemes used in literature. Some other findings are mentioned in the next section.

TABLE III EXISTING METHODS AND THE TECHNIQUES USED

No	**Frequency domain technique**	**Spatial domain technique**	**Genetic algorithm and neural network technique**	**Edge detection technique**
Schemes	Huang and Kim (2016); Jiang *et al.* (2016)	Rayappan (2013); Mishra *et al*. (2014); Hegde & Jagadeesha (2015); Nag *et al.* (2015)		Sun (2016)
Methods	Mohammed and Mohammed (2016)	Das and Dhara (2015); Nag et *al.* (2015); Mohammed *et al.* (2016); Safarpour and Ghami (2016)	Laha and Roy (2015); El-Emam and Al-Diabat (2015).	Jain *et al*. (2012); Singh and Datar (2015)
Encryption	Srinivasan *et al*. (2015); Seyyedi *et al*. (2016);	Muhammad *et al*. (2015)		

2.1 Research Gaps

In the course of reviewing the relevant literature, it is evident that the advancement of data-concealing techniques mostly focuses on enhancing payload capacity, improving quality, or strengthening security. However, it is noteworthy that there seems to be a lack of study into potential trade-offs during the comparative analysis of these techniques. The consensus among researchers is that the improvement of a single criterion has implications for additional requirements. Consequently, there is a dearth of studies that investigate many criteria, complicating or rendering impossible the comparison with prior methodologies (Taha et al., 2019). Evaluation criteria are related to the research gaps. Therefore, the research gaps of steganography can be defined as a complex multi-criteria problem with conflicting criteria evaluation and benchmarking.

Shortly, the scholarly literature has documented many assessment criteria. These entities may be differentiated based on their relative significance. When the developer intends to create a safe steganography technique, it becomes evident that the assessment process focuses on assessing the security aspects via comparison. Additionally, it has been stated that investigations into the trade-offs associated with the assessment criteria have resulted in the identification of research gaps that arise throughout the procedure of review and comparison. The following subsection highlights the research gaps of steganography criteria from the view of academic literature:

1. Researchers have utilized random or selective assaults as a means to unveil their steganography techniques for the purpose of evaluating the efficiency and doing comparisons. The choice of assaults in their experiments lacks a clear

rationale. Furthermore, the available research does not provide a definitive answer about the ability of the created systems to withstand other forms of assault.

2. In the trade-offs between capacity and imperceptibility, researchers have used less capacity in order to increase the PSNR, which is the measurement of imperceptibility.
3. Most past researchers have used spatial domain. They focus on the LSB approach for embedding, attributed to reliability and flexibility. However, the approach lacks in security. In order to gain greater security, a faction of researchers has focused on frequency domain such as Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT). The frequency-domain approach yields better security; however, the approach suffers from imperceptibility and capacity.
4. Imperceptibility is one of the main issues in steganography. Benchmarking process of imperceptibility is based on PSNR equation. The PSNR equation is represented as a comparison among the original hosting image and the stego result image. Most recent research works have reported inaccuracy of the metric and that it needs to be supported by some other quality metrics such as SSIM (Zhang *et al*., 2019; Younus *et al*., 2019; Taha *et al*., 2019).
5. The development of a comparison mechanism in the field of steganography has been undertaken to enhance information security. The data-hiding methods of medical image steganography, revisable steganography, fragile steganography, and steganography, which are widely used, lack a well-defined comparison mechanism.
6. The majority of steganography methodologies have used established compression and encryption techniques in order to minimize the volume of covert information and enhance security measures before incorporating a concealed message. These approaches exhibit poor security performance when subjected to steganalysis tools and statistical attacks as they are widely known in the public knowledge domain.
7. Some studies have used Genetic Algorithms (GAs). The performance yielded by these algorithms indicated weak security against statistical attacks as the hiding of information only uses single randomisation stage.
8. Benchmarking process must be considered with reliable measurement parameters.

3. CONCLUSION

This review has outlined important improvements in image steganography, focusing on the core criteria of security, capability, and imperceptibility. The study discloses that while higher loads and enhanced security are realistic, they often compromise image quality and imperceptibility, highlighting the inherent trade-offs in steganography. Frequency-domain methods, such as DCT and DWT, offer improved security at the cost of load capacity, whereas spatial domain techniques like LSB provide higher capabilities with moderate security. Innovative techniques utilizing genetic algorithms and neural networks show promise in enhancing these trade-offs but require further modification to achieve robustness against diverse attack vectors. The study underscores the need for comprehensive benchmarking protocols, multi-criteria evaluation, and novel embedding methods to further the resilience and efficiency of stenographic systems. Future research should prioritize developing adaptive approaches that balance multiple criteria, addressing the identified research gaps, and advancing steganography as a reliable solution for secure data embedding in digital images.

Funding:

No external financial assistance or institutional funding was utilized for conducting this research. The authors assert that all research-related activities were self-financed.

Conflicts of Interest:

The authors declare that there are no competing interests associated with this work.

Acknowledgment:

The authors would like to thank their institutions for their steadfast encouragement and logistical support throughout this research journey.

References

[1] G. Budiman and L. Novamizanti, "White space steganography on text by using LZW-Huffman double compression," *Int. J. Comput. Netw. Commun.*, vol. 7, no. 2, pp. 136A, 2015.

[2] P. Y. Chen and H. J. Lin, "CNN-based image steganalysis using additional data embedding," *Multimedia Tools Appl.*, vol. 79, no. 1-2, pp. 1355–1372, 2023.

[3] S. A. El Rahman, "A comparative analysis of image steganography based on DCT algorithm and steganography tool to hide nuclear reactors confidential information," *Comput. Electr. Eng.*, vol. 70, pp. 380–399, 2018.

[4] Gutub, A. Al-Qahtani, and A. Tabakh, "Triple-A: Secure RGB image steganography based on randomization," in *Proc. IEEE/ACS Int. Conf. Comput. Syst. Appl.*, 2009, pp. 400–403.

[5] R. Ibrahim and T. S. Kuan, "Steganography algorithm to hide secret message inside an image," *arXiv Preprint*, arXiv:1112.2809, 2011.

[6] M. N. Islam, M. F. Islam, and K. Shahrabi, "Robust information security system using steganography, orthogonal code, and joint transform correlation," *Optik (Stuttg.)*, vol. 126, no. 23, pp. 4026–4031, 2015.

[7] N. F. Johnson and S. Jajodia, "Steganalysis of images created using current steganography software," in *Information Hiding*, Springer, Berlin Heidelberg, 1998, pp. 273–289.

[8] H. R. Kanan and B. Nazeri, "A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm," *Expert Syst. Appl.*, vol. 41, no. 14, pp. 6123–6130, 2014.

[9] Kaur, R. Dhir, and G. Sikka, "A new image steganography based on first component alteration technique," *arXiv Preprint*, arXiv:1001.1972, 2010.

[10] N. G. Kini and V. G. Kini, "A secured steganography algorithm for hiding an image in an image," in *Integrated Intelligent Comput., Commun. Security*, Springer, Singapore, 2019, pp. 539–546.

[11] Kolakalur, I. Kagalidis, and B. Vuksanovic, "Wavelet based color video steganography," *Int. J. Eng. Technol.*, vol. 8, no. 3, pp. 165, 2016.

[12] Y. K. Lee and L. H. Chen, "High capacity image steganographic model," *Proc. IEE Vision, Image Signal Process.*, vol. 147, no. 3, pp. 288–294, 2000.

[13] B. Li, J. He, J. Huang, and Y. Q. Shi, "A survey on image steganography and steganalysis," *J. Inf. Hiding Multimedia Signal Process.*, vol. 2, no. 2, pp. 142–172, 2011.

[14] Z. Li, G. Xu, S. Wu, and X. Wang, "A steganography scheme on JPEG compressed cover image with high embedding capacity," *Int. Arab J. Inf. Technol.*, vol. 16, no. 1, pp. 116–124, 2019.

[15] X. Liao, Y. Yu, B. Li, Z. Li, and Z. Qin, "A new payload partition strategy in color image steganography," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 30, no. 3, pp. 685–696, 2019.

[16] H. H. Liu and C. M. Lee, "High-capacity reversible image steganography based on pixel value ordering," *EURASIP J. Image Video Process.*, vol. 2019, no. 1, pp. 54, 2019.

[17] Pandey, B. S. Saini, B. Singh, and N. Sood, "Bernoulli's chaotic map-based 2D ECG image steganography: A medical data security approach," in *Medical Data Security for Bioengineers*, IGI Global, 2019, pp. 208–241.

[18] Parberry, "An efficient algorithm for the Knight's tour problem," *Discrete Appl. Math.*, vol. 73, no. 3, pp. 251–260, 1997.

[19] F. R. Patel and A. N. Cheeran, "Performance evaluation of steganography and AES encryption based on different formats of the image," *Perform. Eval.*, vol. 4, no. 5, 2015.

[20] K. Patel and L. Ragha, "Binary image steganography in wavelet domain," in *Proc. Int. Conf. Ind. Instrum. Control (ICIC)*, 2015, pp. 1635–1640.

[21] J. B. B. Rayappan, "Kubera kolam: A way for random image steganography," *Res. J. Inf. Technol.*, vol. 5, no. 3, pp. 304–316, 2013.

[22] R. Shanthakumari and S. Malliga, "Dual layer security of data using LSB inversion image steganography with elliptic curve cryptography encryption algorithm," *Multimedia Tools Appl.*, pp. 1–17, 2019.

[23] M. Singh, A. Kakkar, and M. Singh, "Image encryption scheme based on Knight's tour problem," *Procedia Comput. Sci.*, vol. 70, pp. 245–250, 2015.

[24] M. F. Tolba, M. S. Ghonemy, I. A. H. Taha, and A. S. Khalifa, "High capacity image steganography using wavelet-based fusion," in *Proc. ISCC*, vol. 1, 2004, pp. 430–435.

[25] Yahya, *Steganography Techniques for Digital Images*. Springer, Cham, 2019.