Al-Rafidain Journal of Computer Sciences and Mathematics (RJCM)

www.csmj.mosuljournals.com

Steganography Traditional Methods and M2PAM in Social Media Environments: A Survey

Omar Abed Najm[1], *, Ahmed Sami Nori[2]

[1,2]Department of Computer Science, College of Computer Science and Mathematics, University of Mosul
Emails: omar.a.n@uomosul.edu.iq, ahmed.s.nori@uomosul.edu.iq

Article information

Article history:
Received: 4/3/2024
Accepted :28/5/2024
Available online: 25/6/2024

Abstract

Steganography is considered as one of the most important topics in the field of data security. This is because of the exponential progress and secret communication of prospective computers. Secret communication in image Steganography was accomplished to insert a message into a cover image (as the transferor to insert message into) and create a stego-image. More precisely, steganography uses over non-secret data to hide secret data and it is not able to be deleted, such as image, text, voice or multimedia content for copyright, military communication, authentication and many other purposes. Therefore, its job is to hide data in bits that epitomize the identical color pixels recurrent in a row of an image file. This research aims critically to analyze various stenographic techniques and covers steganography literature. Moreover, it supports the apprehensive developers to understand the limitations of most popular techniques to be used based on stenography techniques.

Keywords:
Steganography, WebP image, Social Media security.

Correspondence:
Author: Omar Abed Najma
Email: omar.a.n@uomosul.edu.iq

1. Introduction

Data security refers to the procedure of protecting digital information from illegal access, deterioration, or thefts. It includes data encryption, and crucial management performs to keep data of applications and systems [1][3]. In other words, there are rules and standards to protect information from intentional data sabotage, and for this reason many techniques are used in order to apply them to information security and then identify malicious and unauthorized users to access private information or sensitive information [4], so there is great concern for the security of data and basic information. [2][5]. The reason behind that is data plays in both large and small businesses, so the position of protecting data from security threats becomes more efficient today than it has ever been [6]. Indeed, it uses two procedures to offer data security, such as cryptography technique and steganography technique.

The cryptography technique is widely applied, as long as it changes secret data into inapprehensible data by encoding it, so only the sender and the receiver have the ability to decrypt it by using a common key. Hence, various algorithms and methods were developed by the cryptographers in order to protect many encryption algorithms which had been broken using reverse engineering. Therefore, if the encrypted data is discovered by malicious users, it is considered a disadvantage of encryption technology [7]. Consequently, developers and researchers should consider another technique instead. On the other hand, steganography can be a useful technique for hiding data within seemingly innocuous files, such as images or audio recordings. This can make it harder for unauthorized users to detect the presence of hidden data. However, it is important to note that steganography alone may not provide sufficient security against determined attackers, especially if they have access to advanced detection and extraction tools [8].

To enhance the security of steganography, efficient algorithms and robust security measures should be employed. These could include strong encryption of the hidden data, secure key management, and regular assessments of the steganographic techniques used to ensure they remain effective against evolving threats. The Mod 2 Plus Average Method (M2PAM) is indeed a powerful algorithm used in steganography for embedding and extracting secret data within cover files while maintaining the cover file's resolution and appearance. Here's a breakdown of the algorithm based on your description:

The data that needs to be protected and hidden from unauthorized access, and the cover file is the file used to carry the secret data. It remains unchanged and maintains its resolution during the embedding process. The algorithm has two directions, one is for embedding the secret data into the cover file.

The embedding process ensures that the cover file's appearance and resolution are preserved. The eyes are used in the cryptography process to enhance security. There are two types of keys: symmetric and asymmetric (public and private keys). Symmetric keys are used for encryption and decryption by the same key, while asymmetric keys use a pair of keys for encryption and decryption, and the output of the embedding process is the stego file.

The stego file is the cover file after the embedding process, carrying the hidden secret data. It's worth noting that while the M2PAM algorithm provides a method for securely embedding and extracting data, the security of the overall steganographic process also depends on factors such as the strength of the encryption used, key management practices, and the resilience of the algorithm against attacks aimed at detecting hidden data. Regular evaluation and updates to the algorithm are important to ensure it remains effective against evolving threat, as shown in **Fig. 1**.

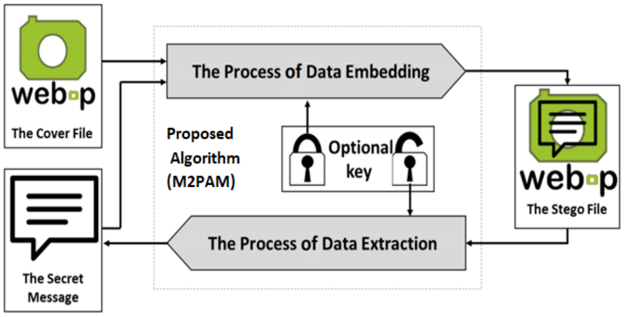

Fig. 1. A M2PAM diagram.

Furthermore, Yadav and Tiwari [9] showed that the best active image security performances are image encryption algorithms to cover its attendance, steganography inserts information into media consideration. It enables another proposed user to know the existence of information due to the mechanism of the hiding algorithm. The digital subjects are combined in the digital watermark with a superior unique signal named the watermark. So, it is eliminated from the watermark representation at the end of the receiver to confirm the digital data. “Fig 2”, shows the organization of the several data security arrangements proposed to date.

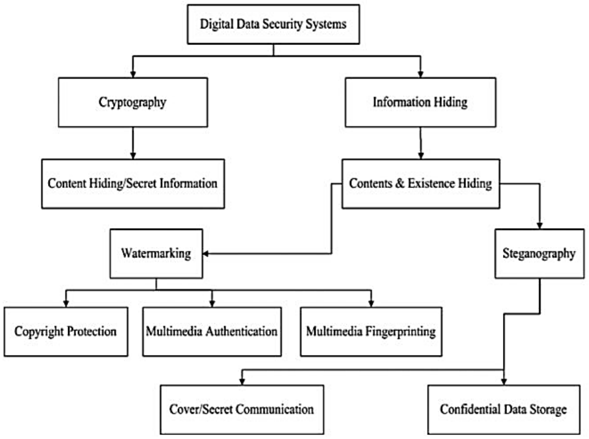
Digital Data Security Systems
Cryptography
Information Hiding
Content Hiding/Secret Information
Contents & Existence Hiding
Watermarking
Steganography
Copyright Protection
Multimedia Authentication
Multimedia Fingerprinting
Cover/Secret Communication
Confidential Data Storage

Fig. 2. Digital Data Security Structure Organization [9].

The usage of steganography technique without help only in unspecific system possibly will not meet the condition of the information security [10]. For example, secret information was secured using the steganography technique, set in an image, and delivered to a particular user. In contrast, if the system of the receiver was hacked by someone else, this means the system was controlled by the hacker and the files have secret data. In this case, the usage of the steganography technique individually is not sufficient [10][11].

The contribution of this survey presents the state-of-the-art in the field of image steganography in terms of the current trends and the most efficient approach that can be adopted. This survey is different from the other approaches in the literature because it can be considered a guide for the researchers in this field.

This survey is organized as follows: Section 2 presents the principles of cryptography versus the steganography and the differences between them. Section 3 elaborates the state-of-the-art in the field of steganography. Section 4 concludes this survey with some recommendations.

1. Cryptography Vs. Steganography

The system design is a combination of cryptography and steganography techniques as an essential condition for providing secure data transmission to confirm that secret data will be authorized and safe. Besides, data encryption has been considered as the most challenging than unencrypted data which is set in the cover file. On this occasion, when a malicious user attempts to attach the encrypted data, it will face big difficulties to obtain it while it has used one of the encryption algorithms. In other words, when combining the cryptography and steganography techniques, the data will be more secure. As long as, if the steganography technique down the hidden data will keep its secured status [12].

Therefore, there are differences between the cryptography and steganography techniques as presented below:

2.1 Cryptography It is hard with exploiting agreements that save attackers from obtaining different characteristics of information security, such as data privacy, data reliability, and validation [13]. Also, the recognised message is approved, it modifies the structure of the message, the crucial key is required, used to encode the message, typically text is used, attack on Cipher Text is named Crypto-analysis, throughput is Ciphertext [14]. "**Fig. 3**", shows the Cryptography technique and "**Fig. 4**" shows its secret key.

Cryptography technique has the most command techniques like One-Time Pad (OTP). OTP is used in the cryptography technique as the public key that used in Rivest, Shamir, and Adleman algorithm (RSA) [16]. The OTP algorithm was born from a previous cipher named Vernam Cipher [17]. Therefore, it combines a message with a keystream, and it has two expectations, such as (a) the keystream utilized as completely random, and (b) the key that using for once. OTP has a famous feature that depends on enabling the key completely secret. Moreover, is characteristically applied by using a modular addition to gather plain text elements with key stream elements, as well as the key can be used for encryption and decryption too [18].

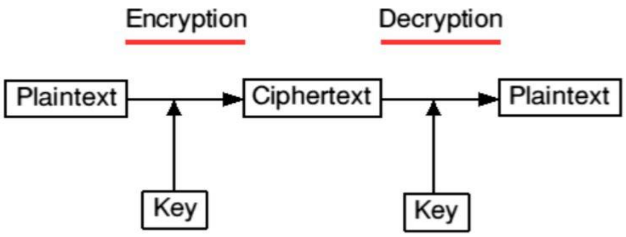

Fig. 3. Cryptography technique [13].

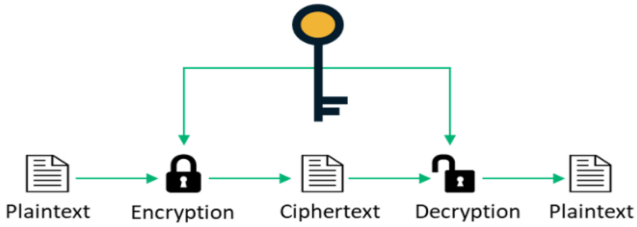

Fig. 4. Secret key cryptography methods [15]

2.2 Steganography

It uses over non-secret data to hide secret data and it is not able to be deleted, such as a normal file. In this technique, using a superior algorithm for encrypting data is to be complicated as a particular file format such as JPEG image, audio or video based on some methods. Its job is to hide data in bits that epitomise the identical colour pixels recurrent in a row in an image file. Finally, the outcome will be an identical file compared to the original file, but it has noise shapes and unencrypted data [19]. In addition, it has many features like the unidentified message which is approved, it does not change the structure of the message, the key is not obligatory, able to hide the message, transporter divided into various media, such as text, audio, image and video, and output are Stego File [14].

The easiest methodology to hide data inside an image file is named Least Significant Bit (LSB). Using LSB in the Steganography technique has no much effect compared with the cover audio and the stego audio. The reason behind that is LSB small in signals of the original position, it also requires fewer resources, such as memory and time consumption as long as it has low computational complication [20]. "**Fig. 5**" shows the description and analysis of steganography work.

3. Literature Review and Indicators

The conventional steganography techniques address the issue of security (for example, confidential information is represented as text). A brief summary of traditional approaches is shown in **Table 1**.

The field of steganography contains a wealth of notable contributions, with numerous methods proposed employing a wide range of algorithms and techniques. Thenmozhi and Chandrsekran [24] introduced a steganographic technique for concealing secret messages within WebP images using their proposed Mod 8 Plus Average Method (M8PAM) algorithm, which hides three bits in a single pixel of the cover file [25]. They suggested a new approach grounded in Discrete Wavelet Transform (DWT) to shift the spatial domain of original image steganography to the frequency domain. This utilization of (2-D DWT) enhanced the cover image and highlighted the efficiency of DWT, especially in low-frequency sub-bands. Furthermore, Dasgupta et al. [26], They developed a secure method for concealing data within digital images, utilizing the Least Significant Bit (LSB) technique.

This involved embedding sensitive information in the spatial domain using the LSB insertion method for image steganography. As a result, the image values and Peak Signal-to-Noise Ratio (PSNR) demonstrated positive outcomes. Additionally, Yu and Wang in [27], They addressed the integration of image steganography with pre-processing of Data Encryption Standard (DES) encryption and LSB steganography algorithms. Their analysis revealed that utilizing image steganography with pre-processed DES encryption yielded superior results compared to using LSB steganography algorithms directly. Furthermore, Manjula [28] proposed a method for concealing a color secret image within a color cover image.

This technique involved setting eight bits of secret data in the least significant bit (LSB) of the Red, Green, and Blue (RGB) pixel values of the cover image separately, with five bits allocated to the R and G pixels and the remaining three bits to the B pixel. As a result, this method achieved better outcomes when compared to the 3,3,2 methods. Similarly, Bawaneh [29] introduced a novel data security approach known as the Greyscale Steganography Process. This method utilized image segmentation to embed secret message bits in the LSB of a random pixel within the greyscale cover image. [30] This introduced a novel data hiding technique aimed at improving visual quality, payload capacity, and maintaining steganography security. The approach comprised two methods: Parity-Bit Pixel Value Difference (PBPVD) and improved Right Most Digit Replacement (iRMDR). The iRMDR method yielded the closest stego-pixels, resulting in excellent visual clarity. The details of these methods are summarized in **Table 2**.

From reviewing **Table 1 and 2**, it's evident that the classical methods fell short compared to the latest advancements. This study's primary objective is to demonstrate the effectiveness of recent steganographic techniques proposed in the literature, particularly for applications in social media platforms. Various factors must be considered when selecting a steganography method, as these factors serve as indicators of the method's quality. The key indicators are outlined as follows:

Hiding Capacity: Opting for methods with a high hiding capacity is preferable. Notably, traditional techniques lag behind the newly developed ones in hiding capacity, with Generative Adversarial Networks (GANs) following suit. According to Convolutional Neural Networks (CNNs) are deemed the most efficient in terms of hiding capacity [29][30].

3.1 Indicators About the Approaches

Numerous considerations come into play when selecting a steganography method, each serving as a quality indicator for the method's efficacy. These key indicators are outlined as follows:

- **Hiding Capacity**: Opting for methods with a high hiding capacity is ideal. Notably, traditional approaches lag behind newly developed ones in hiding capacity, with Generative Adversarial Networks (GANs) following suit. According to [31][32], Convolutional Neural Networks (CNNs) are the most efficient in terms of hiding capacity.
- **Robustness and Security**: Robustness pertains to the successful extraction of the secret image, while security relates to the embedding process. These indicators are vital factors in steganography, as they address the core concept of the field [33][34].
- **Tamper Resistance**: Once a message is embedded into an image (stego-image), altering it becomes challenging [35].
- **Complexity**: Simplicity in approach, devoid of complex computations, is preferred. The cost of an approach is a significant factor that developers aim to minimize [36].

3.1 Steganography Working Domains

Steganography techniques can be classified into the following categories:

- Spatial Domain Approaches: These methods involve altering the values of image pixels to conceal information.
- Transform Domain Approaches: These are more intricate in execution, with many algorithms utilizing transform domains (such as embedding in the frequency domain).
- Distortion Approaches: These techniques necessitate knowledge of the "cover image" during the decoding phase.
- Filtering and Masking Approaches: These methods conceal information using principles similar to watermarking, storing information in the most significant areas.

A summary of the above categories is presented in **Table. 3**.

4. Conclusions

This survey presents the state-of-the-art in the field of image steganography. Many concepts and approaches were presented in this work. Most of the approaches were discussed and analyzed in terms of the limitations and advantages. This survey supports researchers and developers to understand the limitations of the most popular techniques to be used based for applying stenography. It also makes it easy to decide about adopting an approach based on the measurements required. In this context, the main metrics used in evaluating the steganography performance were discussed. Moreover, the main image domains were also presented in terms of the techniques that can be involved and the limitations of each domain.

As a future work, it is planned to incorporate more studies that use deep learning techniques in specific. The limitations and restrictions of these approaches will also be considered.

List of Terms

Term	Description
“Covering Image”	The image that is used in hiding information.
“Stego-Image	It is the cover image after embedding the information.
“Stego-Key”	The key that is used for embedding/extracting the hidden information from a stego-image and a cover image.

Acknowledgments

The authors are grateful to the Computer Science Department/ College of Computer Science and Mathematics/ University of Mosul/ Iraq for supporting this work to be achieved.

Table. 1. Examples of Conventional Techniques.

Ref.	Data Used	Measurement	Limitations	Strengths

[21]	Single RGB Images	PSNR=62.5332
		Time=0.4524s
			Text representation of secret information	Fast and Robust

[22]	Lena and Baboon (.bmp)	PSNR-R=53.20
		PSNR-G=56.19
		PSNR-B=56.95
		MSE-R=0.31
		MSE-G=0.16
		MSE-B=0.13
			Less secure	Fast and accepts arbitrary image format

[23]	Lena	PSNR=54.25	Less secure	Fast

Table. 2. A Summary of the Approaches.

Ref.	Method	Measurements	Limitations	Strengths
[24]	DWT and 2-D DWT	PSNR=49.54	Not efficient with high frequency	Efficient with low frequency

[25]	OTP, DES and LSB	Message:1250 byte
		Sticker:49k
		MSE=0.0044
		PSNR=71.696
			Includes many steps.	Fast and Robust

[26]	LSB and PSNR	PSNR=48.01
		MSE=1.02
			High computation al cost	Outperfor-med many approaches in the literature in terms of accuracy.

[27]	DES and LSB	Variety of results	LSB was not efficient compared to DES	Efficient performance

[28]	LSB	PSNR=37.6828
		MSE=3.7532
			High computation al cost	Reliable

[29]	LSB and Image Segmen-tation	PSNR=49.54
		MSE=1.25
			Complex	Efficient in terms of security since it uses greyscale steganog-raphy.

[30]	PBPVD and iRMDR	PSNR=38.40	Includes many steps.	Increase visual quality and sustainable security.

Table. 3. A Summary of the Image Domains Used in Steganography.

Domain	Approaches	Limitations	Strengths
[37][38]	LSB, PVD, EBE, RPE, Histogram Shifting, Pixel intensity-based approaches, Texture based, labelling based,	Using LSB the data can be destroyed, and the approach can be less robust	High hiding capacity
[39][40]	DFT, DCT, DWT, Coefficient bit based, Lossless/Reversible based,	Image format restrictions	hiding information in areas that are "less exposed" to compression
[41]	Vary	Vary	Vary
[42][43]	Watermarking approaches	Applied only on Grey Scale	Robust

References

[1] Zainal, N., Hoshi, A. R., Ismail, M., Rahem, A. A. R. T., & Wadi, S. M. (2024). A hybrid steganography and watermark algorithm for copyright protection by using multiple embedding approaches. Bulletin of Electrical Engineering and Informatics, 13(3), 1877-1896.

[2] Bagane, P., Venkatesh, S., Guttikonda, J. B., Badhoutiya, A., Srivastava, A. P., Khan, A. K., ... & Shrivastava, A. (2024). Securing Data in Images Using Cryptography and Steganography Algorithms. International Journal of Intelligent Systems and Applications in Engineering, 12(15s), 17-25.

[3] P. Chinnasamy, S. Padmavathi, R. Swathy, and S. Rakesh, "Efficient data security using hybrid cryptography on cloud computing", Lect. Notes Networks Syst., vol. 145, no. November, pp. 537–547, doi: 10.1007/978-981-15-7345-3_46, 2021.

[4] M. Ashiqul Islam, A. A. Kobita, M. Sagar Hossen, L. S. Rumi, R. Karim, and T. Tabassum, "Data security system for a bank based on two different asymmetric algorithms cryptography," Lect. Notes Data Eng. Commun. Technol., vol. 53, no. January, pp. 837–844, doi: 10.1007/978-981-15-5258-8_77, 2021.

[5] M. T. Gen and M. Vural, "Enhancing The Data Security by using Audio Steganography with Taylor Series Cryptosystem," Turkish J. Sci. Technol., vol. 16, no. 1, pp. 47–64, 2021.

[6] A. Ikhwan, R. A. A. Raof, P. Ehkan, Y. Yacob, and M. Syaifuddin, "Data Security Implementation using Data Encryption Standard Method for Student Values at the Faculty of Medicine, University of North Sumatra," J. Phys. Conf. Ser., vol. 1755, no. 1, p. 11, doi: 10.1088/1742-6596/1755/1/012022, 2021.

[7] H. Rout and B. Kishore Mishra, "Pros and Cons of Cryptography, Steganography and Perturbation techniques," IOSR J. Electron. Commun. Eng., no. December, pp. 2278–2834, 2015, [Online]. Available: www.iosrjournals.org.

[8] M. A. Panhwar, S. A. Khuhro, T. Mazhar, D. ZhongLiang, and N. Qadir, "Quantum Cryptography: A way of Improving Security of Information," Int. J. Math. Comput. Sci., vol. 16, no. 1, pp. 9–21, 2021.

[9] A. Yadav, Sonal. Tiwari, "A Review on Image Encryption Techniques," J. Xi'an Univ. Archit. Technol., vol. XIII, no. 3, pp. 256–260, 2021.

[10] M. H. Muhammad, H. S. Hussain, R. Din, H. Samad, and S. Utama, "Review on feature-based method performance in text steganography," homepage, vol. 10, no. 1, pp. 427–433, doi: 10.11591/eei.v10i1.2508, 2021.

[11] O. Fouad and A. Wahab, "Hiding Data Using Efficient Combination of RSA Cryptography , and Compression Steganography Techniques," IEEE Access, vol. 9, no. 10, pp. 31805–31815, doi: 10.1109/ACCESS.2021.3060317, 2021.

[12] M. H. Rajyaguru, "CRYSTOGRAPHY-Combination of Cryptography and Steganography With Rapidly Changing Keys," Int. J. Emerg. Technol. Adv. Eng., vol. 2, no. 10, pp. 329–332, 2012.

[13] Mazhar, M. A. B., "SECURE VIDEO TRANSMISSION USING STEGANOGRAPHY AND CRYPTOGRAPHY", B.Sc. Project, (2018).

[14] K. I. Rahmani, A. Kumar, and G. Manisha, "Study of Cryptography and Steganography System Study of Cryptography and Steganography System," Int. J. Eng. Comput. Sci., vol. 4, no. August, pp. 10–13, doi: 10.18535/ijecs/v4i8.12, 2015.

[15] S. Thitme and V. K. Verma, "A Recent Study of Various Encryption and Decryption Techniques," Int. Res. J. Adv. Eng. Sci., vol. 1, no. 3, pp. 92–94, 2016.

[16] A. M. Al-Smadi, A. Al-Smadi, R. M. Ali Aloglah, N. Abu-Darwish, and A. Abugabah, "Files cryptography based on one-time pad algorithm," Int. J. Electr. Comput. Eng., vol. 11, no. 3, pp. 2335–2342, doi: 10.11591/ijece.v11i3.pp2335-2342, 2021.

[17] Rachmawanto, E. H., and Christy A. S., "Secure image steganography algorithm based on dct with otp encryption." Journal of Applied Intelligent System 2, no. 1 (2017): 1-11.

[18] Stinson, D. R. Cryptography: theory and practice. Chapman and Hall/CRC, Book, 2005.

[19] Asanbe, M. O. "Hybrid Data Security: A Review of Cryptography And Steganography Techniques." Villanova Journal of Science, Technology and Management 2, no. 1 (2020)..

[20] S. Alhassan and L. Bayor, “Enhancing the Security of Mobile Cloud Computing using Audio Steganography with Least Significant Bit Insertion,” Int. J. Eng. Res. Technol., vol. 10, no. 02, pp. 664–673, 2021.

[21] K. A. Al-Afandy, O. S. Faragallah, A. Elmhalawy, E.-S.-M. El-Rabaie, and G. M. El-Banby, ``High security data hiding using image cropping and LSB least signi_cant bit steganography," in Proc. 4th IEEE Int. Colloq. Inf. Sci. Technol. (CiSt), Oct. 2016, pp. 400_404.

[22] A. Arya and S. Soni, "Performance evaluation of secrete image steganography techniques using least signi_cant bit (LSB) method," Int. J. Comput. Sci. Trends Technol., vol. 6, no. 2, pp. 160_165, 2018.

[23] N. Patel and S. Meena, "LSB based image steganography using dynamic key cryptography," in Proc. Int. Conf. Emerg. Trends Commun. Technol. (ETCT), Nov. 2016, pp. 1_5.

[24] M. Thenmozhi, S. Chandrasekaran, “A novel technique for image steganography using nonlinear chaotic map,” in 7th International Conference on Intelligent Systems and Control (ISCO), pp. 307–311, 2013.

[25] Mahmood B., " WebP Image Steganography Using M8PAM for Android Applications", M.Sc. Thesis, 2017.

[26] K. Dasgupta, J. K. Mandal, and P. Dutta, “A Novel Secure Image Steganography Method Based on Chaos Theory in Spatial Domain,” Int. J. Secur. Priv. Trust Manag., vol. 3, no. August 2015, pp. 1–13, doi: 10.5121/ijsptm.2014.3102, 2014.

[27] X. Z. Xiaoyan Yu, Chengyou W., “A Survey on Robust Video Watermarking Algorithms for Copyright Protection,” Recent Adv. Signal Process. Deep Learn. Public Secur. Appl., vol. 8, no. 10, 2018.

[28] [26] A. G.R.Manjula, “A NOVEL HASH BASED LEAST SIGNIFICANT BIT (2-3-3) IMAGE STEGANOGRAPHY IN SPATIAL DOMAIN,” Int. J. Secur. Priv. Trust Manag., vol. 4, no. 1, pp. 11–20, 2015.

[29] A. A. O. Mohammed J. Bawaneh, “A Secure Robust Gray Scale Image Steganography Using Image Segmentation,” J. Inf. Secur., vol. 07, no. 03, p. 13, 2016.

[30] N. and J. Hussain, M, Abdul Wahab, AW, Ho, ATS, Javed, “A data hiding scheme using parity-bit pixel value differencing and improved rightmost digit replacement,” Signal Process. Image Commun., vol. 50, pp. 44–57, 2017.

[31] X. Duan, K. Jia, B. Li, D. Guo, E. Zhang, and C. Qin, ``Reversible image steganography scheme based on a U-Net structure," EEE Access, vol. 7, pp. 9314_9323, 2019.

[32] R. Zhang, S. Dong, and J. Liu, ``Invisible steganography via generative adversarial networks," Multimedia Tools Appl., vol. 78, no. 7, pp. 8559_8575, Apr. 2019.

[33] P. G. Kuppusamy, K. C. Ramya, S. Sheebha Rani, M. Sivaram, and V. Dhasarathan, ``A novel approach based on modi_ed cycle generative adversarial networks for image steganography," Scalable Comput., Pract. Exper., vol. 21, no. 1, pp. 63_72, Mar. 2020.

[34] Subramanian N., Omar E., Somaya A., and Ahmed B., "Image Steganography: A Review of the Recent Advances." IEEE Access (2021).

[35] Jain R., and Jayshree B., "Advances in digital image steganography." In 2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH), pp. 163-171. IEEE, 2016.

[36] Yao, Y., and Nenghai Y., "Motion vector modification distortion analysis-based payload allocation for video steganography." Journal of Visual Communication and Image Representation 74 (2021): 102986.

[37] Prasad, S., Shankar, O. H., and Ilia, P., "Detection of Malicious Spatial-Domain Steganography Over Noisy Channels." In Multidisciplinary Approach to Modern Digital Steganography, pp. 125-145. IGI Global, 2021.

[38] Nassr, D. I., and Sohier M. K., "Applying Permutations and Cuckoo Search for Obtaining a New Steganography Approach in Spatial Domain." International Journal of Network Security 23, no. 1 (2021): 67-76.

[39] Ayub, N., and Arvind S.. "An improved image steganography technique using edge based data hiding in DCT domain." Journal of Interdisciplinary Mathematics 23, no. 2 (2020): 357-366.

[40] Subhedar, M. S., "Cover selection technique for secure transform domain image steganography." Iran Journal of Computer Science (2021): 1-12.

[41] Holub, V., and Jessica F., "Designing steganographic distortion using directional filters." In 2012 IEEE International workshop on information forensics and security (WIFS), pp. 234-239. IEEE, 2012.

[42] Zebbiche, K., Fouad K., and Khaled L., "Robust additive watermarking in the DTCWT domain based on perceptual masking." Multimedia Tools and Applications 77, no. 16 (2018): 21281-21304.

[43] Evsutin, O., Anna M., and Roman M., "Algorithm of error-free information embedding into the DCT domain of digital images based on the QIM method using adaptive masking of distortions." Signal Processing 179 (2021): 107811.