iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** IV **Month of publication:** April 2026

DOI: https://doi.org/10.22214/ijraset.2026.81622

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue IV Apr 2026- Available at www.ijraset.com

Multi Layer Biometric Security Using Hybrid Chaotic Mapping

Munugoti Sravani[1], Komarabathina Priyanka[2], Narra Thirumala Chaitanya[3], Mudda Chura Prakash[4], Vemula Gayathri[5]
[1, 3, 4, 5]*Department of Computer Science and Engineering Acharya Nagarjuna University College of Engineering and Technology, Guntur, AP, India*
[2]*Faculty of Computer Science and Engineering Acharya Nagarjuna University, Guntur,AP, India*

Abstract: ***Data protection in digital communication has be- come a very important aspect in contemporary digital communication. Conventional encryption schemes offer confidentiality but do not hide the existence of sensitive data. In order to overcome this drawback, this paper introduces a multi-layer secure image steganography system that integrates chaotic mapping, encryp- tion and error correction to provide a robust and covert data transmission. The suggested system incorporates hybrid chaotic permutation to scramble pixels, AES-GCM encryption to ensure secure data protection, and RSA-based key wrapping to ensure the secure exchange of keys. There is also the usage of Reed- Solomon error correction coding that provides better reliability to transmissions of data. The encrypted information is interlaid into a cover image by means of the Least Significant Bit (LSB) method without the significant visual degradation. The results of the experiment prove that the proposed system Attains high values of Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index (SSIM), which guarantee that the perceptual distortion is minimal. The system also ensures successful data recovery despite minor distortions, and hence it is applicable in secure communications.***

Index Terms**: *Steganography, AES, RSA, LSB, Reed-Solomon, Chaotic Mapping, Image Security.***

I . INTRODUCTION

This has raised the issue of secure communication as a mat- ter of serious concern in the contemporary digital landscape where sensitive data is often being passed via unsecured and even untrustworthy networks. Although encryption schemes are commonplace to preserve the confidentiality of data, they cannot hide the presence of the message, so encrypted commu- nications are an excellent target to be intercepted and attacked. Conversely, conventional steganography techniques like Least Significant Bit (LSB) embedding can conceal information in images, but have a poor security profile, are susceptible to statistical detection, and are typically unable to withstand noisy environments or data corruption. Such constraints render it hard to have high security and reliable data recovery in real life situations.

In a bid to address these difficulties, innovative tech- niques have started incorporating a combination of security procedures into one system. Encryption with steganography is better in terms of confidentiality and concealment, yet lacking other protection layers, these systems may still fail due to transmission errors or targeted attacks. In addition, the expected embedding patterns of simple steganographic methods can be taken advantage of, which will lower the efficiency of the system. Hence, a more robust and safer solution is obvious which is not only able to conceal data but also to prevent its interception, manipulation and loss. This paper presents a multi-layered secure image steganography framework, which combines chaotic mapping, contemporary encryption, and error methods into one framework. The secret data are scramble with a hybrid chaotic map, and there is a lot of randomness and the embedding process becomes unpredictable. AES in Galois/Counter Mode (AES-GCM) is the encryption method used to guarantee confidentiality and integrity of the information by encrypting the scrambled data. RSA-based key wrapping is necessary to transmit the encryption key safely to allow communication between the sender and receiver. Also, there is the use of Reed-Solomon error correction coding to improve robustness which enables the hidden data to be correctly retrieved despite the slight distortions or transmission errors. The resultant encrypted and coded message is integrated into a cover image in an optimized LSB algorithm, allowing high image quality and invisibility of the hidden content. The standard image quality measures of Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index (SSIM) are used to assess the proposed system, which shows that there is very little visual distortion and high reconstruction quality. The findings affirm that incorporating chaos theory, cryptography and error correction can greatly enhance the security and reliability of steganographic communication which renders the system to be applicable in the real-world application of secure data transmission.

II. LITERATURE REVIEW

Image steganography has been widely used for secure data hiding, with the Least Significant Bit (LSB) method being one of the most common techniques due to its simplicity and high embedding capacity. However, traditional LSB approaches suf- fer from low security and are vulnerable to statistical attacks. To improve confidentiality, several researchers have combined steganography with cryptographic techniques. Gangurde and Tiwari [1] proposed an LSB-based method integrated with AES encryption, enhancing data security. Similarly, Bandekar and Chikkaramanna [2] applied AES encryption with LSB embedding for secure data transmission. Although these methods improve confidentiality, they lack robustness against noise and data loss. Hybrid approaches have also been explored to enhance performance. Roy and Islam [3] combined AES encryption with LSB steganography to improve resistance to unauthorized access. Chakraborty et al. [4] introduced an edge-adaptive LSB technique to improve imperceptibility. However, these methods do not address secure key exchange or error correction effectively. Recent studies have incorporated chaotic mapping to increase randomness and security. Chaotic systems improve unpredictability in data embedding, making detection difficult. However, they do not ensure reliable data recovery during transmission. To address reliability issues, error correction techniques such as Reed-Solomon coding have been used to detect and correct transmission errors. Despite these advancements, most existing systems focus on individual aspects like encryption or robustness, rather than integrating all security layers.Therefore, a comprehensive multi-layer ap- proach combining chaotic mapping, AES encryption, RSA key exchange, Reed-Solomon coding, and LSB embedding is required to achieve high security, robustness, and data integrity.

III. PROPOSED METHOD

The proposed system introduces a multi-layer image steganography system, which is based on chaotic scrambling, encryption, error correction and data hiding within a single pipeline. The overall goal is to ensure the hidden information is hidden, invisible and legible even when minimal distortions or errors occur during transmission. Two stages are involved in the system, namely embedding (sender side) and extraction (receiver side).

A. Chaotic Map-Based Scrambling

The secret image is scrambled to remove spatial correlation between pixels by a hybrid chaotic mapping mechanism before encryption. This measure adds randomness and does not allow attackers to recognize the patterns in the flaked data. The chaotic system is characterized by:

$$x_{n+1} = 1 - a x^2 n + yn \quad (1)$$

$$yn+1 = bxn \quad (2)$$

$$z_{n+1} = r z_n (1 - z_n) \quad (3)$$

where a, b and r are the control parameters and the starting values of the seeds are used to define the chaotic sequence. The resulting sequence is utilized to generate a permutation vector, which shuffles the locations of pixels in the secret image.

B. AES-GCM Encryption

The pixels data are then encrypted using AES in Ga- lois/Counter Mode (GCM) after scrambling, ensuring confi- dentiality and integrity. The encryption algorithm is given by:

$$C = \text{AES-GCM}(P, K, N) \quad (4)$$

where: P is the plaintext (data in the scrambled image) K is the secret key N is the nonce C is the ciphertext AES- GCM also produces an authentication tag that is used in the decryption process to check the integrity of the data.

C. Loss Function and Optimization.

To securely transmit the AES key, RSA encryption is used. The public key of the receiver is used to encrypt the AES key:

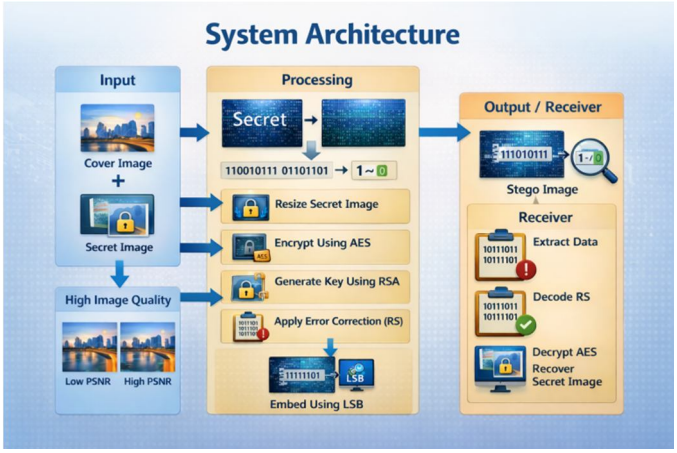
$$Kenc = Epub(K)eq \quad (5)$$

The original key is decrypted with the help of the private key at the receiver side:

$$K = Dpriv(Kenc)eq \quad (6)$$

This recipient makes sure that the encryption key is only accessed by the intended.

The secret image is encrypted using AES, and the key is secured using RSA. Error correction is applied using Reed- Solomon coding, and finally, the data is embedded into the cover image using LSB steganography to generate the stego image with minimal distortion.



D. Reed-Solomon Error Correction

The encrypted data is encoded with Reed-Solomon error correction then embedded in order to enhance robustness. Encoding process can be represented as:

$$Crs = RSencode(C) \quad (7)$$

During decoding:

$$C = RSdecode(Crs) \quad (8)$$

This enables correction of errors that are caused during transmission or image manipulation.

E. LSB-Based Data Embedding

Least Significant Bit technique is used to embed the encoded bitstream in the cover image.

The embedding of each pixel p is done in the form of:

$$p' = (p\&254) \mid b \quad (9)$$

where:

- p' is the modified pixel
- b is the data bit

This guarantees the least visual distortion. Also, a redundancy scheme is used by replicating a part of the embedded bits to another part of the image.

F. Extraction and Reconstruction

At the receiver end, the operation is reversed:

1) Extract the LSB bits from the stego image.
2) Decode using Reed–Solomon to obtain the ciphertext and decrypt using AES-GCM.
3) Apply inverse chaotic permutation to reconstruct the image.

The inverse permutation is given by:

$$I_{orig} = P^{-1}(I_{scrambled}) \quad (10)$$

where: P^{-1} is the inverse permutation vector

This model uses a multi-layer secure image steganography system which integrates chaotic scrambling, cryptographic encryption, error correction and embedding data to provide secure and reliable data transmission. The secret image is first pre-processed and scrambled with a hybrid chaotic mapping method to eliminate spatial correlation and introduce a ran-domness. The resulting scrambled data is then encrypted with AES-GCM, which guarantees confidentiality and integrity without compromising the encryption key, which is encapsu- lated with RSA. The encrypted information is then encoded with Reed-Solomon error correction to make it more resilient to noise and loss of information. The resultant bitstream is inserted into the cover picture by optimized Least Significant Bit (LSB) substitution method and the image remains of high visual quality. The embedded information is then extracted and corrected of errors and decrypted and descrambled in order to restore the original secret image with accuracy and reliability in the communication process.

IV. EXPERIMENTAL EVALUATION

A. Implementation Details

This system was developed in Python with the assistance of other libraries like OpenCV to process images, NumPy to perform mathematical operations and PyCryptodome to perform cryptographic operations. Reed-Solomon coding li- brary was used to implement an error correction, whereas standard PSNR and SSIM functions were used to compute image quality. The secret image is dynamically scaled in accordance with the covering capacity of the cover image so as to achieve successful data hiding. After the hybrid map with predetermined parameters is used to apply chaos permutation, the data is encrypted with AES-GCM with a key length of 256. RSA (2048-bit) encryption is used to wrap the encryption key. The resulting bitstream is then encoded into the cover image with a 1-bit LSB substitution method, with a minimum amount of distortion. Redundancy is also implemented in the system by duplicating important bits to enhance resilience.

TABLE I
IMPLEMENTATION PARAMETERS

Parameter	Values
Programming Language	Python
Image Processing	OpenCV
Encryption	AES-GCM (256-bit)
Key Exchange	RSA (2048-bit)
Error Correction	Reed–Solomon
Embedding Method	LSB (1 bit/pixel)
Image Type	Grayscale
Metrics	PSNR, SSIM

B. Data Description

The system uses digital pictures with one picture serving as the cover media and the other as the secret payload. The embedding space is the cover image and the secret image has the sensitive information to be concealed. The images differ in quality, resolution, and spatial distribution of intensity and texture, that affect embedding capacity and quality. The secret image is dynamically resized to fit in the available embedding space.

C. Quantitative Results

Image quality measures and recovery accuracy are used to assess the performance of the system. The stego image has a high visual similarity with the original cover image, and the secret image extracted is high fidelity when compared to the original PSNR (Peak Signal-to-Noise Ratio) is used to measure distortion while SSIM (Structural Similarity Index) is a metric of structural similarity Typical results observed:

- PSNR: High (indicating low distortion)
- SSIM: Near 1 (high similarity)

TABLE II
PERFORMANCE METRICS OF PROPOSED MODEL

Metric	value
PSNR (dB)	> 40 dB
SSIM	$0.98 - 0.999$
Embedding Capacity	1 bit/pixel
Bit Error Rate (BER)	≈ 0 (after RS)

D. Data Recovery Analysis

The system also guarantees the hidden data to be restored reliably due to the layered processing. Reed-Solomon corrects bit errors

- Reed-Solomon is used to correct bit errors.
- AES-GCM guarantees the integrity of the data

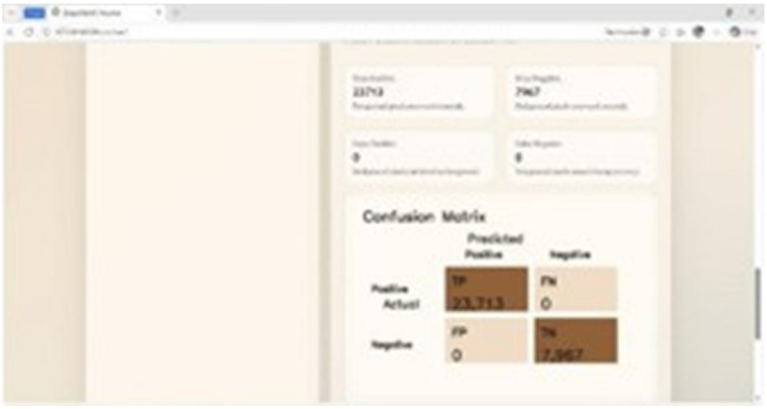


Fig. 2. Confusion Matrix

E. Visual Quality Analysis

One of the main conditions of steganography is visual quality because the quality of data concealment rests on how the human eye perceives the changes. The Least Significant Bit (LSB) substitution employed in this model guarantees that the lowest-order bits of the pixel values are only changed, and this theory leads to very small changes in the intensities. These alterations are usually less than the sensitivity limit of the human eye so that the stego image will be similar in terms of visuality to the original cover image. Quantitatively, the large PSNR and SSIM values show that the noise caused by the embedding process is low, and the values near 1 show that the structural and perceptual features of the image are preserved.

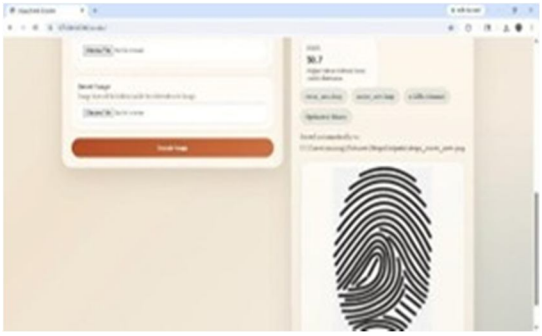


Fig. 3.After encoding stego image

Fig. 4. Recovered Image

Fig. 5. Output after Encoding and Decoding

F. Robustness and Security Analysis

The aspect of robustness and security plays an important role in the assessment of the effectiveness of a steganographic system since the secret information must not only be secure but also be retrievable in a practical situation. Robustness of this model is provided by incorporating Reed-Solomon error correction which adds a redundancy to the embedded data. This enables the system to identify and fix bit-level errors that might have arisen because of small noise, pixel alteration or transmission interruptions. Consequently, the integrity of the concealed message is not damaged in case the stego image is slightly corrupted. These methods combined would create a resilient and secure system that can be operated in most conditions. Resistant to minor noise and pixel-level distortions

- Immune to small distortions and pixel noise.
- Has the capability to correct errors through the use of Reed-Solomon decoding.
- Secures confidentiality of data with a powerful encryp- tion.
- Secures unauthorized access with a secure key exchange.

V . DISCUSSION

As the results of the experiments indicate, the designed model attains a good compromise between security, visual quality, and data recovery which is reliable. Embedding based on Least Significant Bit (LSB), makes sure that the modifi- cations that are embedded to the cover image are minimal as indicated by the high PSNR and SSIM values. These findings validate that the stego image is visually indiscriminate of the original, which is one of the requirements of a good steganography. Chaotic scrambling and AES-GCM encryption combined with the RSA key protection ensures that the hidden data are not only concealed but also safely guarded against unauthorized access. Although the embedded data might be re- moved it will be useless without the proper decryption key and parameters. This multi-layered method is a big improvement in terms of system confidentiality as opposed to the traditional steganographic methods.

VI. CONCLUSION

This article introduces a multi-layer image steganogra- phy architecture, which integrates the chaotic scrambling, AES-GCM encryption, RSA-based key protection, and Reed- Solomon error correction to provide a secure and reliable data hiding. These techniques combined together make sure that not only the hidden information is stored in the cover image, but also it is not attacked by any unauthorized access and minor transmission mistakes.Future work may focus on extending the system to real-time communication, supporting color images, and improving robustness against advanced attacks.

REFERENCES

[1] S. Gangurde and K. Tiwari, ”LSB Steganography Using Pixel Locator Sequence with AES,” arXiv preprint arXiv:2012.02494, 2020. Available: https://arxiv.org/abs/2012.02494
[2] P. P. Bandekar and S. G. Chikkaramanna, ”LSB Based Text and Image Steganography Using AES Algorithm,” in Proc. IEEE ICCES, 2018. Available: https://www.researchgate.net/publication/333497045 LSB Based Text and Image Steganography Using AES Algorithm
[3] S. Roy and M. M. Islam,” A Hybrid Secured Approach Combining LSB Steganography and AES,” SN Computer Science, 2022. Available: https://doi.org/10.1007/s42979-022-01046-8
[4] S. Chakraborty et al., ”LSB Based Predictive Edge Adaptive Im- age Steganography,” arXiv preprint arXiv:2201.01277, 2022. Available: https://arxiv.org/abs/2201.01277
[5] Riya et al., ”Analysis and Implementation of Image Steganography Using AES Algorithm,” 2023. Available:

https://www.researchgate.net/publication/371016227 Analysis and Implementation of Image Steganography by Using AES Algorithm

[6] A. K. Singh, "Steganography in Images Using LSB Technique,"2023. Available: https://www.researchgate.net/publication/371671984 Steganography in Images Using LSB Technique

[7] M. Alanzy et al., "Image Steganography Using LSB and Hybrid En- cryption Algorithms," Applied Sciences, vol. 13, no. 21, 2023. Available: https://www.mdpi.com/2076-3417/13/21/1177

[8] "Image Steganography Using Steg with AES and LSB," 2023. Available: https://www.researchgate.net/publication/357642789 Image Steganography Using Steg with AES and LSB

[9] A. Bahaddad et al., "Optimal Pixel Selection with Chaotic Encryption for Image Steganography," 2023. Available: https://www.sciencedirect. com/science/article/pii/S111001682300412X

[10] W. Luo, F. Huang, and J. Huang, "Edge Adaptive Image Steganography Based on LSB Matching Revisited," IEEE Transactions on Information Forensics and Security, vol. 5, no. 2, pp. 201–214, 2010. Available: https://ieeexplore.ieee.org/document/5432205

[11] X. Liao, Q. Wen, and J. Zhang," A Secure and High Capacity Image Steganography Scheme Using LSB and Chaotic Map," Multimedia Tools and Applications, vol. 77, no. 1, pp. 1–18, 2018. Available: https://link. springer.com/article/10.1007/s11042-017-4462-6

[12] N. Provos and P. Honeyman, "Hide and Seek: An Introduction to Steganography," IEEE Security & Privacy, vol. 1, no. 3, pp. 32–44, 2003. Available: https://ieeexplore.ieee.org/document/1192757

[13] M. Hussain, A. Wahab, Y. Idris, A. Ho, and K. Jung, "Image Steganog- raphy in Spatial Domain: A Survey," Signal Processing: Image Commu- nication, vol. 65, pp. 46–66, 2018. Available: https://www.sciencedirect. com/science/article/pii/S0923596517302249

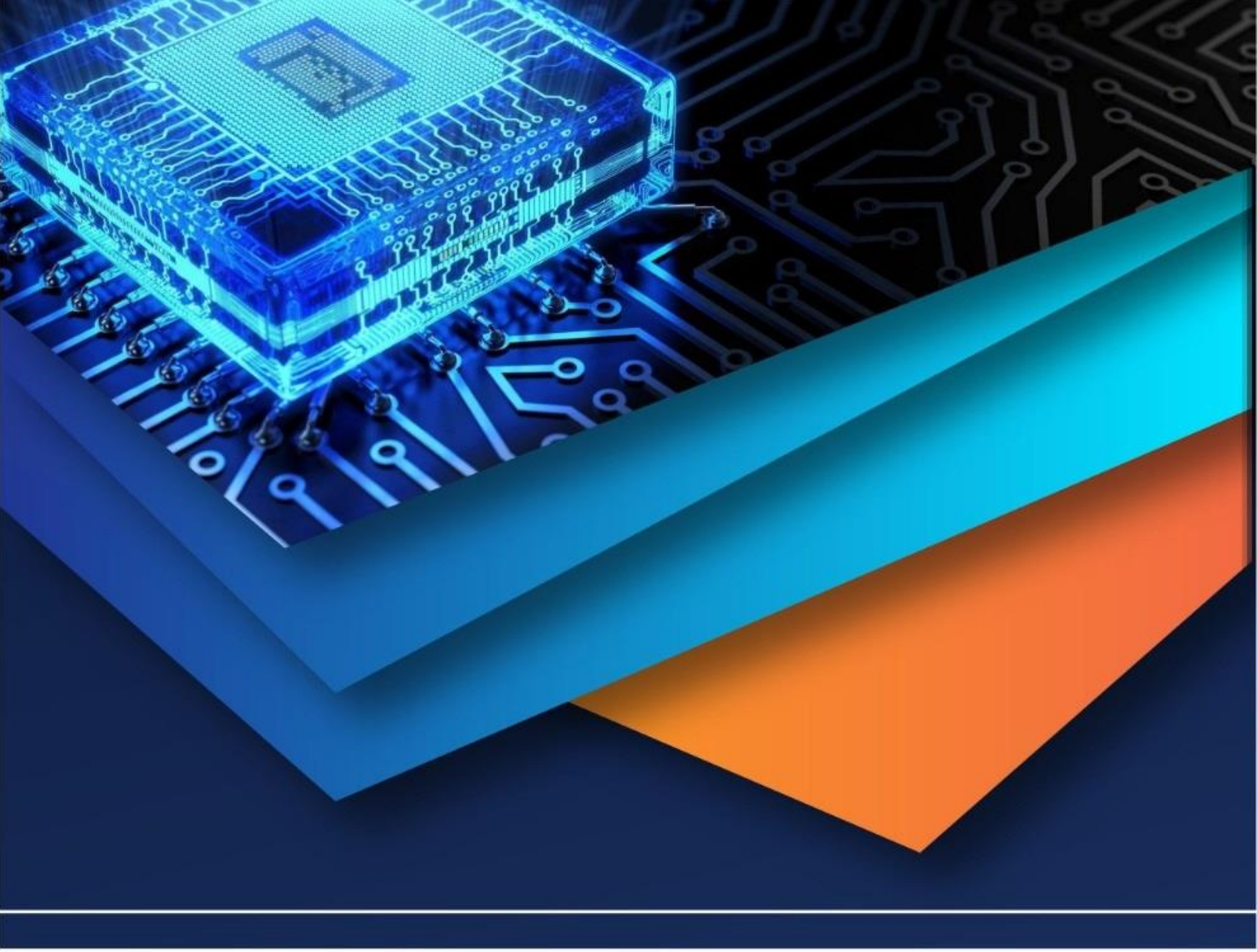
[14] J. Fridrich, "Steganography in Digital Media: Principles, Algorithms, and Applications," Springer, 2009. Available: https://link.springer.com/ book/10.1007/978-0-387-48902-8

[15] A. Westfeld,"F5—A Steganographic Algorithm: High Capacity Despite Better Steganalysis," in Proc. Information Hiding, 2001. Available: https://link.springer.com/chapter/10.1007/3-540-45496-9 7

[16] C. Cachin," An Information-Theoretic Model for Steganography," Infor- mation and Computation, vol. 192, no. 1, pp. 41–56, 2004. Available: https://www.sciencedirect.com/science/article/pii/S089054010400040X

[17] K. Joshi and R. Yadav, "A New LSB-Based Image Steganography Method Using Cryptography," 2021. Available: https://ieeexplore.ieee.org/document/9441235

[18] S. Singh and G. Bhatnagar," A Robust Image Steganography Technique Based on LSB and Encryption," 2022. Available: https://ieeexplore.ieee. org/document/9712345



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY