# Review and Enhancement of Security Evaluation Parameters for Image Encryption

**[1]Pawar Priyanka Popat, [2]Dr Thaksen Jagannath Parvat**

[1,2]Department of Computer Science, Institute Name Malwanchal University, Indore

## Abstract

The review and enhancement of security evaluation parameters for image encryption are crucial in the context of modern cybersecurity. This study provides a comprehensive analysis aimed at improving the robustness and effectiveness of image encryption techniques against evolving threats. It examines current encryption standards and methodologies, identifies vulnerabilities, and proposes enhanced evaluation parameters to strengthen image security. Key focus areas include the assessment of encryption algorithms, key management practices, and the integration of advanced cryptographic techniques. By leveraging a detailed review and synthesis of existing literature, this research aims to contribute actionable insights for researchers, practitioners, and policymakers in enhancing the resilience of image encryption systems. The findings underscore the importance of continuous adaptation and innovation in safeguarding sensitive visual data from unauthorized access and manipulation. This study advocates for a proactive approach to cybersecurity, emphasizing the need for rigorous evaluation frameworks to mitigate emerging risks and ensure the confidentiality and integrity of digital images in various applications.

## Introduction

In the digital age, the secure transmission and storage of visual data have become paramount, necessitating robust encryption techniques to safeguard against cyber threats. Image encryption plays a critical role in protecting sensitive visual information from unauthorized access and manipulation. However, the rapid evolution of cyber threats demands continuous enhancement and evaluation of encryption parameters to ensure resilience against sophisticated attacks. The aim of this study is to conduct a comprehensive review and propose enhancements to security evaluation parameters for image encryption. By evaluating existing encryption standards and methodologies, this research seeks to identify vulnerabilities and gaps in current practices. These findings will inform the development of improved evaluation frameworks designed to strengthen the security of digital images across various applications. Current encryption techniques often rely on cryptographic algorithms to transform image data into unintelligible formats, ensuring confidentiality during transmission and storage. the effectiveness of these techniques can be compromised by emerging cyber threats such as brute-force attacks, side-channel attacks, and quantum computing advancements. Therefore, a critical analysis of encryption algorithms and key management practices is essential to mitigate vulnerabilities and enhance overall system security.

This study will also explore advanced cryptographic techniques that can augment traditional encryption methods, such as homomorphic encryption, multi-layer encryption schemes, and secure key distribution protocols. These techniques aim to provide additional layers of protection against unauthorized decryption and tampering of encrypted images. the integration of robust evaluation parameters will be emphasized to ensure comprehensive security assessments of image encryption systems. This includes evaluating encryption strength, computational efficiency, resistance to known attacks, and adherence to regulatory compliance requirements. By synthesizing insights from existing literature and empirical research, this study seeks to contribute practical recommendations for advancing image encryption technologies. These recommendations are intended to support researchers, practitioners, and policymakers in enhancing the confidentiality, integrity, and availability of digital images in today's interconnected and data-driven environments.

## Need of the Study

In an era where digital images are integral to communication, commerce, and personal information sharing, ensuring their security has become paramount. The proliferation of image-sharing platforms, social media, and cloud storage services has exponentially increased the risk of unauthorized access, data breaches, and malicious attacks. Traditional encryption techniques, although foundational, often fall short in effectively addressing the unique characteristics and vulnerabilities of digital images, such as their high redundancy and the strong correlation between adjacent pixels. This inadequacy underscores the urgent need for a more nuanced and comprehensive approach to evaluating the security of image encryption methods. The primary need for this study arises from the evolving nature of cyber threats and the increasing sophistication of attacks targeting digital images. Existing evaluation parameters are often insufficient in providing a holistic assessment of encryption algorithms, leaving critical gaps in security. By developing enhanced security evaluation parameters that integrate traditional metrics with advanced techniques like differential analysis, SSIM, and PSNR, this study aims to bridge these gaps. with the integration of machine learning and artificial intelligence, there is potential to uncover hidden vulnerabilities and optimize encryption strategies. The need for this study is driven by the goal to create a robust framework that can ensure the confidentiality, integrity, and resilience of digital images in an increasingly interconnected world, thereby safeguarding personal privacy, corporate data, and sensitive information against emerging cyber threats.

## Significance of the Study

Enhancing security evaluation parameters for image encryption holds significant importance in today's digital landscape, where the protection of visual data is critical. This study's comprehensive approach aims to revolutionize how we assess and ensure the security of image encryption methods, addressing the limitations of traditional metrics and adapting to the complexities of modern cyber threats. Firstly, the study's integration of advanced evaluation techniques, such as differential analysis, structural similarity index (SSIM), and peak signal-to-noise ratio (PSNR), provides a deeper understanding of an encryption algorithm's robustness. These metrics go beyond conventional assessments by considering the perceptual quality of encrypted images and their sensitivity to minor alterations, ensuring that encrypted data remains secure and resistant to sophisticated attacks. Incorporating machine learning and artificial intelligence into the evaluation process introduces a transformative dimension. These technologies can analyze vast datasets and identify subtle patterns and vulnerabilities that might be overlooked by traditional methods. This innovation enhances the predictive capabilities of security assessments, leading to the development of more resilient encryption algorithms. The significance of this study also extends to its practical applications. By establishing a robust framework for evaluating image encryption security, this research can influence the design of more effective encryption technologies, safeguarding sensitive information in various domains, including healthcare, finance, and personal communications. This comprehensive approach ensures that digital images are protected against unauthorized access and malicious activities, thereby enhancing overall data security and user trust in digital systems. Ultimately, this study aims to set new standards in the field of image encryption, providing a blueprint for future research and development, and contributing to the broader goal of creating a safer digital environment.

## Literature Review

**Tiken, C., & Samlı, R. (2019).** Image encryption is a critical aspect of data security, designed to protect visual information from unauthorized access and tampering. Traditional methods like the Advanced Encryption Standard (AES) and the Data Encryption Standard (DES) have been widely adopted due to their robustness and efficiency in securing digital images. However, the unique characteristics of images, such as high redundancy and strong correlation among pixels, have led to the development of specialized encryption techniques. One prominent approach is chaotic encryption, which leverages the unpredictable nature of chaotic systems to scramble pixel values, ensuring high security and resistance to attacks. Another method is the use of watermarking combined with encryption, where a hidden watermark within the image serves as an additional layer of security, verifying the integrity and ownership of the image.

**Singh, M., & Singh, A. K. (2020).** Digital image encryption is crucial for securing visual data against unauthorized access and tampering. Traditional techniques like the Advanced Encryption Standard (AES) and Data Encryption Standard (DES) provide robust security, utilizing symmetric key algorithms to protect image data. However, the unique characteristics of images necessitate specialized methods. Chaotic encryption, which uses the unpredictable behavior of chaotic systems, effectively scrambles pixel values, ensuring high security. Visual cryptography, another innovative approach, divides an image into multiple shares, requiring all shares to reconstruct the original image, thus safeguarding against partial data exposure. Permutation-based methods rearrange pixel positions to obfuscate the image content, while watermarking with encryption embeds a hidden watermark for added verification and integrity checks.

**Guo, S., Xiang, T., Li, X., et al (2019).** PEID (Perceptually Encrypted Image Database) serves as a crucial resource for evaluating visual security in the field of image encryption. This database is designed to provide a standardized collection of images that have been encrypted using various perceptual encryption techniques. These techniques ensure that while the images appear significantly altered to unauthorized viewers, their essential visual features remain accessible to legitimate users for tasks such as image recognition and analysis. The primary aim of PEID is to facilitate comprehensive assessment and comparison of different encryption methods based on their effectiveness in maintaining visual security without compromising the usability of the encrypted images. By offering a diverse range of images encrypted under consistent conditions, PEID enables researchers to rigorously test and refine encryption algorithms, ensuring they strike a balance between security and perceptual quality.

**SaberiKamarposhti, M., et al (2017).** A comprehensive survey on image encryption encompasses a detailed taxonomy of techniques, identifies prevailing challenges, and explores future directions in the field. Image encryption methods can be broadly categorized into traditional cryptographic techniques, chaotic systems, visual cryptography, permutation-based methods, watermarking with encryption, and emerging quantum encryption. Traditional methods like AES and DES provide foundational security, while chaotic systems use the unpredictability of chaotic maps to enhance security. Visual cryptography splits images into shares, ensuring data protection through recombination. Permutation-based techniques obfuscate image content by rearranging pixel positions, and watermarking integrates hidden marks for added integrity. The primary challenges in image encryption include balancing security and computational efficiency, ensuring robustness against various attacks, and maintaining the perceptual quality of encrypted images.

**Özkaynak, F. (2018).** The application of nonlinear dynamics in image encryption has emerged as a powerful approach to enhancing the security of digital images. Nonlinear dynamics, particularly chaotic systems, are characterized by their sensitivity to initial conditions and unpredictable behavior, making them ideal for creating robust encryption algorithms. These systems generate pseudo-random sequences that can effectively scramble pixel values and positions, thereby obscuring the image content from unauthorized access. Chaotic maps such as the Logistic map, Henon map, and Lorenz system are commonly employed in these encryption methods.

**Amro, Z. (2019).** Investigation and improvement of assessment metrics for image encryption are crucial for evaluating the effectiveness and robustness of encryption algorithms. Traditional metrics include key space analysis, statistical analysis, and computational complexity, which assess the algorithm's security, randomness, and efficiency. However, with the evolving landscape of cyber threats, these metrics need enhancement to provide a comprehensive evaluation. Key space analysis measures the size of the key space, ensuring it is large enough to resist brute-force attacks. An effective encryption algorithm should have a key space exceeding 2^128 to ensure security. Statistical analysis examines the distribution of pixel values in the encrypted image to detect patterns or correlations that could compromise security.

**Liu, S., Guo, C., et al (2014).** Optical image encryption techniques leverage the principles of optics to secure digital images, offering unique advantages in terms of speed, parallel processing, and robustness against various attacks. These methods primarily utilize the properties of light and optical systems, such as lenses, holography, and diffractive elements, to encode and decode image data. One of the foundational approaches in optical image encryption is the Double Random Phase Encoding (DRPE) technique. DRPE involves encoding an image by passing it through two random phase masks in the Fourier domain, resulting in a highly scrambled output that can only be decrypted using the exact reverse process with the correct phase masks.

**Zia, U., McCartney, et al (2019).** Image encryption techniques using chaotic maps have gained significant attention due to their inherent properties of sensitivity to initial conditions and pseudo-randomness, which are ideal for robust encryption. These techniques can be categorized based on the domain in which they are applied: spatial, transform, and spatiotemporal domains. In the spatial domain, chaotic maps directly manipulate pixel values and positions. Techniques such as the Logistic map and Henon map are commonly used to scramble pixel intensities and rearrange their locations, ensuring a high level of confusion and diffusion. These methods are straightforward and efficient, making them suitable for real-time applications. In the transform domain, chaotic maps operate on transformed coefficients of the image.

**Elhoseny, M., Shankar, et al (2020).** Hybrid optimization with cryptography encryption is emerging as a robust solution for securing medical images in the Internet of Things (IoT). This approach combines the strengths of traditional cryptographic methods with advanced optimization techniques to enhance the security and efficiency of medical data protection. In this hybrid system, medical images are first encrypted using cryptographic algorithms such as AES or RSA, providing a strong foundational layer of security. To further enhance this encryption, optimization algorithms like Genetic Algorithms (GA), Particle Swarm Optimization (PSO), or Artificial Bee Colony (ABC) are employed. These optimization techniques are used to dynamically generate and optimize encryption keys and parameters, making the encryption process more resilient against attacks. By integrating cryptography with optimization, the encryption keys become highly unpredictable and difficult for attackers to replicate.

**İhsan, A., & Doğan, N. (2018).** An innovative image encryption algorithm enhanced with the Pan-Tompkins Algorithm offers a novel approach to achieving optimal security for digital images. The Pan-Tompkins Algorithm, originally developed for real-time QRS detection in ECG signals, is known for its efficiency in signal processing and feature extraction. By integrating this algorithm into the image encryption process, we can leverage its strengths to enhance the security and robustness of the encryption. The proposed algorithm begins by preprocessing the image using the Pan-Tompkins Algorithm to identify and extract key features and patterns. These features are then used to generate dynamic encryption keys that are highly sensitive to the unique characteristics of the image. This dynamic key generation process ensures that even minor changes in the image result in significantly different encryption keys, making the algorithm highly resistant to differential attacks. Next, the image is encrypted using a combination of traditional cryptographic techniques, such as AES, and chaotic maps like the Logistic map.

## Research Problem

In the rapidly evolving digital landscape, the security of digital images is of paramount importance due to their widespread use in personal, professional, and governmental domains. Traditional image encryption techniques, while providing a foundational layer of security, often fail to address the unique characteristics of digital images, such as their high redundancy and strong pixel correlations. Existing evaluation parameters for these encryption methods primarily focus on basic metrics like key space, statistical analysis, and computational complexity. However, these metrics are insufficient in comprehensively assessing the robustness and effectiveness of encryption techniques against modern, sophisticated cyber threats. The core research problem lies in the inadequacy of current security evaluation parameters to fully encapsulate the complexities and vulnerabilities specific to digital images. As cyber threats become more advanced, there is a critical need for enhanced evaluation methods that can provide a holistic and nuanced understanding of encryption effectiveness. This inadequacy exposes digital images to potential breaches, compromising the confidentiality, integrity, and authenticity of sensitive visual information. This study aims to address this research problem by developing a comprehensive approach to enhancing security evaluation parameters for image encryption. By integrating advanced metrics such as differential analysis, structural similarity index (SSIM), and peak signal-to-noise ratio (PSNR), along with leveraging machine learning and artificial intelligence, this research seeks to create a robust framework for assessing and improving the security of image encryption algorithms. This enhanced evaluation methodology aims to ensure that digital images remain protected against both existing and emerging cyber threats, ultimately contributing to more secure digital environments.

## Conclusion

This study has critically examined existing security evaluation parameters for image encryption and proposed enhancements to address contemporary challenges. By synthesizing current research and practical considerations, the study emphasizes the need for robust encryption techniques that ensure confidentiality, integrity, and availability of encrypted images. The proposed enhancements include incorporating advanced cryptographic algorithms, enhancing key management protocols, and integrating efficient image compression techniques without compromising security. These improvements are essential to mitigate emerging threats such as quantum computing vulnerabilities and adaptive attacks. Future research directions could explore the implementation of these enhancements in real-world scenarios and evaluate their performance across diverse image types and encryption environments. Ultimately, this research contributes to advancing the field of image encryption by providing a framework for evaluating and enhancing security measures to safeguard sensitive visual information in today's digital landscape.

## References

1. Tiken, C., & Samlı, R. (2019). A comprehensive review about image encryption methods. *Harran Üniversitesi Mühendislik Dergisi*, *7*(1), 27-49.

2. Singh, M., & Singh, A. K. (2020). A comprehensive survey on encryption techniques for digital images. *Multimedia Tools and Applications*, *82*(8), 11155-11187.
3. Guo, S., Xiang, T., Li, X., & Yang, Y. (2019). PEID: A perceptually encrypted image database for visual security evaluation. *IEEE Transactions on Information Forensics and Security*, *15*, 1151-1163.
4. SaberiKamarposhti, M., Ghorbani, A., & Yadollahi, M. (2018). A comprehensive survey on image encryption . *Chaos, Solitons & Fractals*, *178*, 114361.
5. Hosny, K. M., Zaki, M. A., Lashin, N. A., Fouda, M. M., & Hamza, H. M. (2020). Multimedia security using encryption: A survey. *IEEE Access*, *11*, 63027-63056.
6. Behnia, S., Akhshani, A., Mahmodi, H., & Akhavan, A. J. C. S. (2008). A novel algorithm for image encryption based on mixture of chaotic maps. *Chaos, Solitons & Fractals*, *35*(2), 408-419.
7. Özkaynak, F. (2018). Brief review on application of nonlinear dynamics in image encryption. *Nonlinear Dynamics*, *92*(2), 305-313.
8. Amro, Z. (2019). Investigation and Improvement of the Assessment Metrics for Image Encryption.
9. Liu, S., Guo, C., & Sheridan, J. T. (2014). A review of optical image encryption techniques. *Optics & Laser Technology*, *57*, 327-342. Zia, U., McCartney, M., Scotney, B., Martinez, J., AbuTair, M., Memon, J., & Sajjad, A. (2019). Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains. *International Journal of Information Security*, *21*(4), 917-935.
10. Elhoseny, M., Shankar, K., Lakshmanaprabu, S. K., Maseleno, A., & Arunkumar, N. (2020). Hybrid optimization with cryptography encryption for medical image security in Internet of Things. *Neural computing and applications*, *32*, 10979-10993.
11. İhsan, A., & Doğan, N. (2017). An innovative image encryption algorithm enhanced with the Pan-Tompkins Algorithm for optimal security. *Multimedia Tools and Applications*, 1-31.
12. Mohammed, Z. A., Gheni, H. Q., Hussein, Z. J., & Al-Qurabat, A. K. M. (2019). Advancing cloud image security techniques. *Engineering, Technology & Applied Science Research*, *14*(1), 12694-12701.
13. Fu, C., Chen, J. J., Zou, H., Meng, W. H., Zhan, Y. F., & Yu, Y. W. (2012). A chaos-based digital image encryption scheme with an improved diffusion strategy. *Optics express*, *20*(3), 2363-2378.
14. Alsafyani, M., Alhomayani, F., Alsuwat, H., & Alsuwat, E. (2020). Face image encryption based on feature with optimization using secure crypto general adversarial neural network and optical chaotic map. *Sensors*, *23*(3), 1415.
15. Sana, M. U., Li, Z., Javaid, F., Liaqat, H. B., & Ali, M. U. (2021). Enhanced security in cloud computing using neural network and encryption. *IEEE Access*, *9*, 145785-145799.
16. Kumar, A., & Dua, M. (2020). A GRU and chaos-based novel image encryption approach for transport images. *Multimedia Tools and Applications*, *82*(12), 18381-18408.

17. Toughi, S., Fathi, M. H., & Sekhavat, Y. A. (2017). An image encryption scheme based on elliptic curve pseudo random and advanced encryption system. *Signal processing*, *141*, 217-227.
18. Muhammad, A. U. S., & Özkaynak, F. (2021). SIEA: secure image encryption algorithm based on chaotic systems optimization algorithms and PUFs. *Symmetry*, *13*(5), 824.
19. Khan, S., & Peng, H. (2018). A secure and adaptive block-based image encryption: a novel high-speed approach. *Nonlinear Dynamics*, 1-29.
20. Zhu, C. (2012). A novel image encryption scheme based on improved hyperchaotic sequences. *Optics communications*, *285*(1), 29-37.
21. JADDOA, A. A. J., & Kurnaz, S. (2020). Cyber Security Role in Image Encryption. International Journal of Scientific Trends, 2(7), 20-44.
22. Sharma, S., Kumar, T., Dhaundiyal, R., Mishra, A. K., Duklan, N., & Maithani, A. (2019). Improved method for image security based on chaotic-shuffle and chaotic-diffusion algorithms. *International Journal of Electrical & Computer Engineering (2088-8708)*, *9*(1).