Vol 6, Issue 11, 2023 **Impact Factor: 5.355** DOI: https://doi.org/10.31426/ijamsr.2023.6.11.6913

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

Enhancing Real-Time Image Encryption: Exploring Chaos-Based and Non-Chaos-Based Block Ciphers with Security Metrics

Salunke Nilesh Tatyasaheb [1], Dr. Vinod Kumar [2]

[1] Research Scholar, Dept. Of Management, Sunrise University, Alwar
[2] Dept. Of Management, Sunrise University, Alwar, Rajasthan

Email: Nilsalunke2302@Gmail.Com

ABSTRACT

This research explores image encryption technology, focusing on chaos-based and non-chaos-based block ciphers, and categorizing them by compression methods. Traditional encryption methods, such as AES and RSA, face challenges with image encryption due to pixel correlation and data volume. Chaos theory offers a promising alternative, with its sensitivity to initial conditions and stochastic behaviour aligning well with encryption needs. The study employs both qualitative and quantitative analyses, using primary and secondary data to assess security metrics like KA, NPCR, HA, UACI, IE, and CC. Practical limitations such as resource constraints and access to proprietary algorithms are acknowledged. The findings aim to enhance real-time image encryption applications, although generalizability may be limited.

Keywords: Image Encryption, Chaos Theory, Block Ciphers, Security Metrics.

Introduction

Image encryption technology transforms original images into complex forms that are challenging to decipher, classified based on operation modes into chaos-based and non-chaos-based block ciphers, and further by encryption extent (fully, partially, or combined) and compression (compression or non-compression methods). Traditional encryption methods like AES, RSA, and IDEA are less suitable for image encryption due to pixel correlation, redundancy, and data volume, making them impractical for real-time applications. Chaos theory, characterized by deterministic nonlinear systems and sensitivity to initial conditions, aligns well with encryption due to its stochastic behavior and sensitivity to minor changes. The Euclidean algorithm, one of the earliest algorithms used in number theory and cryptography, helps simplify fractions and find the greatest common divisor (GCD) efficiently. In encryption, terms like unencrypted images, ciphertext images, encryption and decryption processes, and keys (alphabetic or numerical) are crucial for securing image data. Various image encryption methods have been developed, categorized into spatial, transformation, optical, and

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

compressed sensing-based methods, and evaluated using parameters like KA, NPCR, HA, UACI, IE, and CC, indicating their effectiveness and considerations in security metrics.

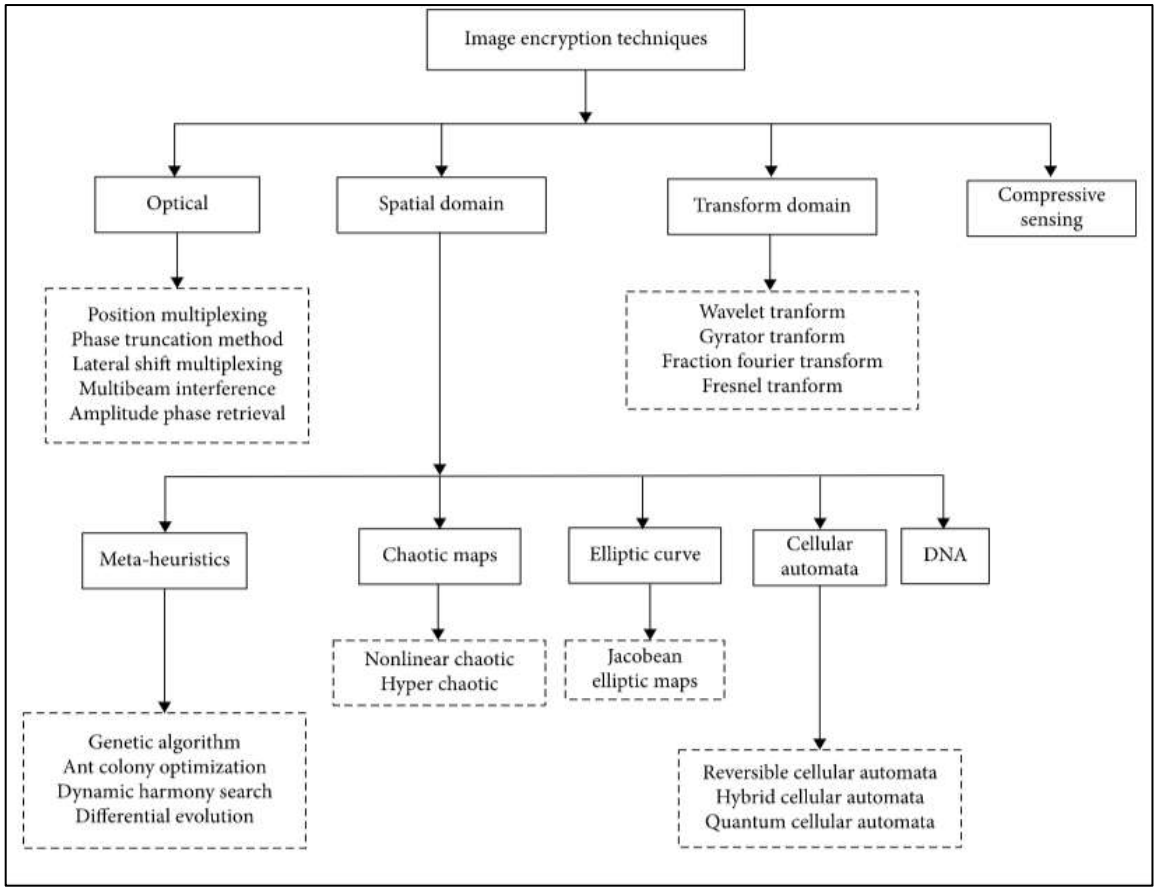

Figure 1.1: Categorization Of Image Encryption Approaches

REVIEW OF LITERATURE

Mustafa et.al., (2019, April) This vulnerability resulted in compromise of confidential information and integrity. Cryptography is a technique for converting plaintext into ciphertext and is used for secure Internet communications, allowing only specific recipients to understand the message. Steganography, meanwhile, hides messages within images, ensuring that everyone but the sender and receiver are unaware of their existence. This article reviews the comprehensive impact of cryptography and steganography technologies in enhancing network information security, and evaluates aspects such as encryption technology, key length, security, and data hiding capabilities.

Konyeha, S., & John-Otumu, A. M. (2020) Increasingly, individuals are becoming aware of the significance of data security in information networks, which is driving them to continually investigate and develop more advanced encryption solutions. The hybrid approach was meant to protect sensitive information. The results of this evaluation reveal that the throughput of material encryption is somewhat lower when compared to DES alone, which indicates that there is a better

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

use of resources. Notably, the decryption throughput of the hybrid approach is significantly lower than DES alone, highlighting its higher security. The findings suggest the application of this hybrid approach to enhance data security in contemporary applications and communication networks.

Siddiqui et.al., (2020) A mathematical algorithm is designed via the process of cryptography in order to safeguard data communications that take place across unprotected networks. For this particular instance, the encryption method encrypts the sensitive information and transforms it into text that the opponent is unable to read. Data obfuscation is provided via the replacement box, sometimes known as the S-box, which is an important nonlinear component in the Advanced Encryption Standard (AES). A unique algebraic approach that utilizes matrices on the Galois field GF (2^8) is suggested specifically for the purpose of constructing S-boxes in order to tackle this issue. The algorithm that is produced via this process generates 1.324×10^14 distinct 8 × 8 S-boxes. Standard tests validate the encryption strength of these S-boxes, indicating that they include characteristics that are considered to be state-of-the-art. In addition, the efficacy of these algorithms in picture encryption applications has been proved by employing the majority of reasonable criteria.

Wang et.al., (2020) Because of the exponential increase in the number of photographs, a great variety of content-based image retrieval techniques have become more prevalent in our everyday lives. For the most part, picture retrieval services are quite costly in terms of the amount of compute and storage required. It is for this reason that picture owners might consider outsourcing their services to cloud servers as a viable alternative. On the other hand, since cloud servers may only be trusted to a certain extent, protecting users' privacy might become a significant challenge for picture owners. An innovative method for retrieving images is presented in this research. The usefulness of this approach has been shown via a series of experiments and analyses.

Melkemi, M., and Hammoudi, K., (2020), A novel visual cryptography (VC) method is introduced, in which two encrypted images are generated from a secret image, transmitted through separate channels, and then superimposed by the receiver to recover the secret image. This marks the first application of Voronoi tessellation in visual cryptography. Compared with traditional VC schemes, Voronoi-based visual cryptography (VVC) technology significantly reduces the information encoded and transmitted, making it suitable for secure transmission in communication networks with low bandwidth or memory constraints. The enhanced security of this technology is due to the random arrangement of Voronoi polygons, and the sender and receiver use private random point generators to further ensure security. Furthermore, the article highlights the shape reconstruction properties of image-based Voronoi representations.

Raghunandan et al. (2020), In the realm of computer vision problems, adversarial training has emerged as a formidable rival to supervised learning approaches, according to the findings of research conducted on adversarial training. The focus of previous research has mainly been on generative tasks, especially in the field of image synthesis. In their paper, however, the researchers ventured beyond the traditional scope and applied adversarial training techniques to the discriminative task of mastering steganography algorithms. Steganography, which includes a group

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

of methods for obscuring messages by integrating them into non-secret media such as cover text or images, comes into focus. The results show that adversarial training exhibits the ability to produce powerful steganography techniques. The steganography algorithm that they generate using their unsupervised training approach is on par with other algorithms that are considered to be state-of-the-art. Furthermore, supervised training of adversarial models led to the development of a resilient Steg analyser that is adept at discerning whether images contain hidden information. The researchers introduced a game involving three entities (Alice, Bob, and Eve) to train both the steganography algorithm and the Steg analyser.

Tammineedi et al. (2020) Find a solution to an issue that is prevalent in the apps that are used on the Internet nowadays, particularly in real-time services like core banking and applications that are focused on public service. The challenge is to verify user credentials, and passwords, as a security and authentication mechanism, are vulnerable to online dictionary attacks. Hacking of databases in web-oriented applications has become an inevitable threat, complicating data maintenance in web applications. To address these challenges, the author proposes a novel Integrated Dynamic CAPTCHA (I&D CAPTCHA) in the paper, which is an extension of the existing CAPTCHA. This innovative solution uses visual cryptography to evaluate third-party human-made attacks in web applications and focuses on authentication issues in real-time scenarios. A number of methods for protecting high-level images in network communication environments have been proposed, including visual cryptography, a cutting-edge technology that ensures secure sharing and maintenance of secret images. The authors analyse various visual cryptography security mechanisms for secure sharing of digital imaging data, with an emphasis on maintaining data confidentiality. CaRP, which stands for CAPTCHA as a visual security password, is the foundation of this system. It offers a two-way communication strategy that combines CAPTCHA with visible security measures. The random picking of passwords and the protection of images are the primary focuses of this system. Furthermore, this study presents AMODS, which is an adaptive system that automatically changes detection models in order to identify the most recent assaults that have not yet been discovered. Rely on the adaptive learning method known as SVM HYBRID to reduce the amount of manual labor required.

Naidu et.al., (2020) In the past, information played a vital role in organizations and enhanced their ability to operate. These organizations use a variety of strategies to protect data in transit, but face challenges from information thieves. Despite the use of encryption algorithms such as DES and RSA, existing systems still have shortcomings and therefore recommendations for an integrated model have been made. The model contains two sources of data: algorithmically encrypted user-supplied information and user-supplied images. This dual-tool approach increases protection against a variety of malicious attacks to address the ever-changing data security landscape.

Lizy (2021), Due to the fact that it conceals the content, encryption is an efficient method for preventing unauthorized parties from utilizing the key to read digital information. Verifying the authenticity and dependability of communications may be accomplished via the use of digital signatures, which often make use of the RSA encryption method. Since RSA encryption is

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

considered to be of lower quality and requires a greater investment of resources, it is not used to encrypt the entire communication. The efficiency of the encryption process can be improved by using symmetric key RSA encryption for messages. If we want to continue using this method, only the RSA private key can decode the symmetric key. Euclidean's algorithm is certainly vying for the title of one of the most famous computer programs. The procedure of Euclidean is used in order to ascertain which of two numbers have the greatest common divisor. Making the technique broader, it can also be developed for rings that are not limited to simple integers. This makes the procedure more versatile. The work that is being done will contribute to the strengthening of the data security of smart cards and Aadhaar cards, which will be of great benefit. In addition to the outcomes of the experiments, the material that is presented also provides mathematical logic that supports the proposed techniques.

Bułat & Ogiela (2022), Additionally, the identity of the developer would be validated, which would make it possible to ensure that encoded material cannot be seen by anyone else. Furthermore, the use of such a methodology in steganography has given rise to a new avenue of research, which has been made possible by the approach that has been proposed. This entails encoding information in the picture that the user gives, with the information being safeguarded by the user's biometric sequences (quality vectors). This is done in order to ensure that confidentiality is maintained. Both situations involve the cryptographic procedures taking on sequences that are completely unique to themselves. These sequences are used in lieu of the traditional salt values. Adding this not only gives a construct that would otherwise be completely theoretical an extra degree of security, but it also gives it a layer of really personal touch that would otherwise be absent. It is possible that it will find numerous uses in the expanding realm of IoT, which is a world in which individuals and the specific requirements they have must be included into an expanding network of security protocols.

Goyal, A. (2022) Big data was once a term used to describe the massive sets of digital data generated by technological advances, but the inability to handle such huge amounts of data has challenged traditional analysis tools. Cloud computing emerged as a solution to facilitate remote data storage and processing. However, concerns about data privacy in the cloud have prompted the proposal of a secure storage framework using the Pisces Crypto encryption algorithm based on K-medoids. This approach involves standardizing data, applying Euclidean neural networks for similarity calculations, and using encryption to protect private information. Conducted using Kaggle health data, the experiment demonstrates the efficacy of encryption methods in protecting privacy while optimizing the time and cost of cloud-based data storage.

Scope Of Research

The thesis will explore image encryption technology, focusing on chaos-based and non-chaos-based block ciphers, with particular emphasis on compression and non-compression methods. The study will be confined to contemporary encryption technologies, excluding historical developments, and will not cover geographical variations. Methodologically, it will employ both qualitative and quantitative analyses, utilizing encryption algorithms and chaos theory principles to assess security

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

metrics. Data will be sourced from both primary experiments and secondary literature, ensuring a representative sample. Exclusions include specific subtopics like non-digital encryption methods. Practical considerations such as resource limitations and access to proprietary algorithms will be acknowledged. The study aims to provide insights with potential implications for real-time encryption applications, though its findings may have limited generalizability beyond the studied scope.

Conclusion

This study underscores the potential of chaos-based encryption methods for enhancing image security, addressing the limitations of traditional approaches. By categorizing encryption methods and evaluating their effectiveness, it provides a comprehensive framework for future research and practical applications in real-time image encryption, despite acknowledging certain practical and generalizability constraints.

References

1. Mustafa, G., Ashraf, R., Haq, I. U., Khalid, Y., & Islam, R. U. (2019, April) A Review of Combined Effect of Cryptography & Steganography Techniques to Secure the Information. In *2019 5th International Conference on Computing Engineering and Design (ICCED)* (pp. 1-6). IEEE.
2. Konyeha, S., & John-Otumu, A. M. (2020). An Efficient Hybrid Cryptographic Model for Securing Information over Communication Network. *Egyptian Computer Science Journal*, *44*(2).
3. Siddiqui, N., Khalid, H., Murtaza, F., Ehatisham-Ul-Haq, M., & Azam, M. A. (2020). A novel algebraic technique for design of computational substitution-boxes using action of matrices on Galois field. *IEEE Access*, *8*, 197630-197643.
4. Wang, H., Xia, Z., Fei, J., & Xiao, F. (2020). An AES-based secure image retrieval scheme using random mapping and BOW in cloud computing. *IEEE Access*, *8*, 61138-61147.
5. Melkemi, M., & Hammoudi, K. (2020) Voronoi-based image representation applied to binary visual cryptography. *Signal Processing: Image Communication*, *87*, 115913.
6. Raghunandan, K. R., Ganesh, A., Surendra, S., & Bhavya, K. (2020) Key generation using generalized Pell's equation in public key cryptography based on the prime fake modulus principle to image encryption and its security analysis. *Cybernetics and Information Technologies*, *20*(3), 86-101.
7. Vivek Tammineedi, V. S., & Rajavarman, V. N. (2020) A Novel Analysis of Advanced Visual Cryptography Techniques for Providing Security Against Web Attacks Using Support Vector Machine Technique. *Journal of Computational and Theoretical Nanoscience*, *17*(5), 2097-2114.
8. Naidu, T. J., Aiswarya, V., SowmyaSree, T., Teja, S., & Karthik, J. (2020) Securing Data Using Image Steganography and Encryption Techniques.

IJAMSR

International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

9. Lizy, R. F. S. (2021). Improvement of RSA Algorithm Using Euclidean Technique. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(3), 4694-4700.
10. Bułat, R., & Ogiela, M. R. (2022). Personalized Cryptographic Protocols-Obfuscation Technique Based on the Qualities of the Individual. In *International Conference on Network-Based Information Systems* (pp. 213-218). Springer, Cham.
11. Goyal, A. (2022) An Efficient Method to Enhance Health Care Big Data Security in Cloud Computing Using the Combination of Euclidean Neural Network and K-Medoids Based Twin Fish Cipher Cryptographic Algorithm. *Available at SSRN 4224313*.