Journal of Advanced Research in Image Processing and Applications
Volume 6, Issue 2 - 2023, Pg. No. 5-10
Peer Reviewed Journal

Review Article

Enhanced Image Encryption Technique: A Hybrid Approach using Scrambling and Genetic Encryption

Shivam Sharma

B.Tech., SASTRA University.

I N F O

E-mail Id:
sshivamsharma376@gmail.com
Orcid Id:
https://orcid.org/0009-0005-3621-2181

How to cite this article:
Sharma S. Enhanced Image Encryption Technique: A Hybrid Approach using Scrambling and Genetic Encryption. *J Adv Res Res Imag Proc Apps* 2023; 6(2): 5-10.

Date of Submission: 2023-09-17
Date of Acceptance: 2023-10-23

A B S T R A C T

Traditional image encryption methods often suffer from security vulnerabilities, image quality degradation, diffusion issues, low latency, poor key sensitivity, and significant correlation. In response, this study proposes an advanced image encryption technique based on a combination of scrambling and discrete wavelet transform. The scrambling process alters the pixel locations without changing their values, preserving statistical properties. The proposed hybrid encryption method incorporates genetic encryption to enhance both image security and quality. The developed approach undergoes rigorous testing against brute force and equivalent key attacks, demonstrating statistical effectiveness, robust performance, and key sensitivity advantages. The results indicate that the hybrid approach meets the criteria for photo security and real-time performance.

Keywords: Discrete Wavelet Transform, Grayscale, Image Encryption, Scrambling, Genetic Encryption

Introduction

In the current era of technological advancements, secure communication of multimedia information, including enhanced photos, music, and videos, is crucial. However, concerns about unauthorized access, illegal use, malicious alterations, and disruptions necessitate robust image encryption solutions.[1] Encryption transforms an original image into a more complex, difficult-to-understand format, enhancing data security.[2] This paper introduces a hybrid encryption technique combining scrambling and genetic encryption to address the shortcomings of traditional methods. In the contemporary landscape of rapid technological evolution, the seamless exchange of multimedia data has become the cornerstone of communication across the web, mixed media platforms, and remote enterprises. This paradigm shift, however, brings forth an array of challenges, including the imperative need for safeguarding enhanced photos, music, and videos from unauthorized access, illicit use, malevolent alterations, and potential disruptions.[3] Over the years, substantial strides have been made in addressing these challenges, with a prevailing consensus on the internet's pivotal role as the primary conduit for information transfer, encompassing text, messaging, and, notably, images.[4] The pervasive use of images in communication today underscores their significance. However, in the course of transmitting information over the internet, the dual concerns of 'security' and 'integrity' loom large. Information security, defined as the protection of data from unauthorized access, emerges as a crucial aspect, with encryption standing out as a stalwart solution.[5] Image encryption, a technique that transforms an original image into a cryptic format that is challenging to decipher without the appropriate unscrambling key, has become indispensable across various domains.

Significance of Encryption in Image Security

Cryptography, a discipline encompassing encryption and decryption techniques, plays a pivotal role in fortifying information security.[6] The crux of the matter lies in the transformation of 'plain text,' the original message intended for communication, into 'cipher text,' an encrypted form that renders the message unintelligible without the corresponding decryption key.[7] The encryption process, requiring both an encryption algorithm and a key, unfolds at the sender's end, ensuring that sensitive data traversing unreliable channels remains confidential.

The Evolution of Cryptography

Cryptographic techniques have evolved to encompass diverse objectives, including confidentiality, authentication, integrity, and non-repudiation.[8] Confidentiality ensures that shared computer information is accessible only to the authorized party, while authentication demands frameworks to verify the sender's identity. The integrity principle dictates that only the authorized entity can modify provided data, preventing tampering by intermediaries.

The Imperative of Image Encryption

In this context, image encryption emerges as a linchpin for securing data in various sectors, including corporate enterprises, healthcare, military operations, and audio-visual systems.[9] Encryption serves as the transformative agent, converting plain text, or in this case, original images, into coded messages, with decryption seamlessly reverting these coded messages to their original form. This intricate dance between encryption and decryption serves diverse security purposes, ensuring information security, data non-change, and more.

Against this backdrop, this study delves into the nuances of image encryption, critically examining the prevailing challenges and proposing a hybrid approach that amalgamates the strengths of scrambling and genetic encryption.[10] The ensuing sections detail the cryptographic principles, review existing literature in the domain, articulate the methodological approach, present data analysis, and culminate in a comprehensive conclusion.[11] The proposed hybrid image encryption technique not only addresses the drawbacks of traditional solutions but also showcases statistical effectiveness, robust performance, and key sensitivity, thereby meeting stringent criteria for both photo security and real-time performance.

Cryptographic Basics

In the realm of cryptography, foundational concepts play a crucial role in shaping secure communication protocols. Understanding these basics provides a solid framework for developing and evaluating encryption techniques.[12] Let's delve deeper into key cryptographic terms:

- **Plain Text:** At its core, plain text represents the unencrypted, original information that the sender intends to communicate. This could encompass any form of data, from written messages to multimedia content.
- **Cipher Text:** The transformation of plain text into cipher text is the central tenet of encryption. Cipher text is an encrypted version of the original message, rendered unintelligible without the application of the appropriate decryption key.
- **Encryption:** This process involves converting plain text into cipher text, often through complex algorithms and mathematical transformations. Encryption serves as a protective measure, safeguarding sensitive information from unauthorized access during transmission or storage.
- **Decryption:** The inverse of encryption, decryption is the process of converting cipher text back into its original plain text form. This restoration is only possible with the possession of the correct decryption key.
- **Key:** A key serves as a critical component in both the encryption and decryption processes. It can take various forms, such as a unique image, a numerical sequence, or an alphanumeric string. The security of the encryption algorithm heavily relies on the strength and confidentiality of the key.

Types of Keys

- **Symmetric Key:** In this approach, the same key is used for both encryption and decryption. The challenge lies in securely distributing and managing the key among authorized users.
- **Asymmetric Key:** Also known as public-key cryptography, this method employs a pair of keys – a public key for encryption and a private key for decryption. Messages encrypted with the public key can only be decrypted by the corresponding private key.
- **Hashing Key:** Hash functions generate fixed-size outputs (hashes) from variable-size inputs. These outputs, commonly known as hash values, are used for data integrity verification and digital signatures.

Role of Keys in Cryptography

- **Confidentiality:** The key ensures that only authorized parties can access and understand the encrypted information.
- **Authentication:** Keys are integral to verifying the identity of both the sender and receiver. Public and private key pairs contribute to secure digital communication.
- **Integrity:** Keys help maintain the integrity of the transmitted data by ensuring that it remains unchanged during transit.
- **Non-Repudiation:** The use of keys enables the creation of digital signatures, ensuring that the sender cannot deny sending a specific message.

Key Management

Effective key management is paramount in cryptographic systems. It involves key generation, distribution, storage, and rotation. The challenge is to strike a balance between maintaining security and facilitating practical usability.[13] In summary, cryptographic basics provide the foundation for secure communication, and a nuanced understanding of these principles is essential for designing robust encryption algorithms and systems.

Cryptographic Goals

In the realm of cryptography, various overarching goals guide the design and implementation of encryption techniques, ensuring the creation of robust and reliable systems for safeguarding sensitive information.[14] These cryptographic goals are fundamental principles that contribute to the overarching objective of maintaining secure communication channels. Let's delve deeper into each of these goals:

1. Confidentiality

- **Definition:** Confidentiality is the cornerstone of cryptographic endeavors, focusing on the protection of information from unauthorized access or disclosure.[15] It ensures that the content of a communication remains private and accessible only to individuals with the appropriate authorization.
- **Implementation:** Encryption algorithms are designed to transform plaintext into ciphertext, making the information unintelligible to anyone without the corresponding decryption key. Through this process, confidentiality is upheld by rendering the content secure and resistant to eavesdropping.

2. Authentication

- **Definition:** Authentication verifies the identity of communicating entities, ensuring that the information originates from a genuine source rather than a malicious imposter.[16] It safeguards against the insertion of unauthorized content into the communication stream.
- **Implementation:** Cryptographic systems employ various mechanisms, such as digital signatures and authentication protocols, to validate the authenticity of messages and participants.[17] By confirming the identity of the sender, the risk of data manipulation by unauthorized entities is mitigated.

3. Integrity

- **Definition:** Integrity ensures the accuracy and unaltered state of information during transmission. It safeguards against accidental or intentional modifications, providing assurance that the received data is identical to the originally transmitted data.
- **Implementation:** Hash functions and checksums are commonly utilized to generate fixed-size values (hashes) that uniquely represent the content of a message. These hashes are sent along with the message, and the recipient recalculates the hash upon receipt.[18] If the recalculated hash matches the received hash, it signifies the integrity of the message.

4. Non-Repudiation

- **Definition:** Non-repudiation prevents the parties involved in a communication from denying their actions or intentions.[19] It ensures that both the sender and the recipient cannot disavow their involvement in the exchange of information.
- **Implementation:** Digital signatures play a crucial role in establishing non-repudiation. By using asymmetric cryptographic techniques, a sender can sign a message with their private key, and the recipient can verify the signature using the sender's public key. This process ensures that the sender cannot later deny sending the message.

These cryptographic goals collectively form the foundation of secure communication, providing a framework for designing encryption systems that effectively protect information in an increasingly interconnected and digital world. Whether applied to financial transactions, sensitive communications, or critical infrastructure, the attainment of these goals is paramount for establishing trust and security in cyberspace.

Literature Review

This section reviews previous studies on image encryption techniques, emphasizing their approaches and outcomes. Notable methods include symmetric key cryptography, image encryption based on RGB pixel rendering and shuffling, and enhanced security color visual cryptography.[20] The literature review explores various image encryption techniques proposed in recent studies, highlighting their methodologies and findings.

Symmetric Key Cryptography 2013: A New CRDDBT Using - Relative Displacement (RDC) and Dynamic Base Transformation (DBTC)

This research investigates an encryption method that deviates from pre-programmed keys.[21] The data string is divided into segments, each encoded with a distinct algorithm. The study employs three novel algorithms to encode the split string based on its orientation, enhancing security. The use of two differently resolved keys for higher security levels is a notable aspect. The research focuses on altering both the base and location of specific string segments, contributing to increased security and complexity.

Combining Block Displacement and Block Cipher Methods to Create a New Image Encryption Method 2013

This publication introduces a novel image encryption algorithm emphasizing the relationship between key

length and security.[20] Utilizing a lengthy 128-bit key, the proposed algorithm demonstrates enhanced security, making cryptographic research and key compromise challenging. The absence of floating-point errors enhances the algorithm's efficiency. The study includes an evaluation of the connection efficiency and entropy values, demonstrating the algorithm's robustness against potential attacks.

Image Encryption as part of RGB PIXEL Rendering and Shuffling 2013

This study proposes a unique approach by considering the rendering and reshuffling of RGB components in advance.[19] The additional exchange of RGB values enhances image security against conceivable attacks. The research presents a comprehensive exploration of the impact of pixel grouping based on RGB values, providing insights into potential improvements for image encryption.[22] The application of lossless photo encryption using MATLAB contributes to the practicality and feasibility of the proposed approach.

Improved Security Color Visual Cryptography 2012

This work introduces an alternative algorithm focusing on pixel grouping and structuring based on RGB values.[18] The study identifies the benefits of grouping pixels to reduce correlations and increase entropy. The use of Matlab 6.0.1 for lossless photo encryption showcases the algorithm's practical implementation and includes a histogram for further analysis. The proposal emphasizes the potential for combining additional pixel computations to enhance image encryption further.

Inter-pixel Dislodging of a Pixel's RGB Attributes for Picture Encryption with Explosive Inter-pixel Dislodging, 2011

This research, published in 2011, aims to manipulate the RGB values of pixels through inter-pixel dislodging.[17] By employing different keys for round shifting three halves of a pixel, the study introduces pixel dislodging risk.[23] The findings underscore the importance of controlling the intermixing of RGB values and its impact on the image's security. The study contributes insights into potential vulnerabilities and robustness in image encryption techniques.

An Image Encryption Approach Using a Mixture of Change Techniques and Encryption, 2008

The work presented by Mohammad Ali Bani Younes and Aman Jantan combines video and stage-based encryption.[12] The division of the original image into 4x4 pixel blocks, permutation using a stage interaction, and subsequent encryption with Rijndael result in improved security. The mix method contributes to reduced component connectivity and increased entropy.[24] The research provides valuable insights into the combination of various encryption techniques for enhanced image security.

The literature review illustrates the diverse approaches researchers have taken to address image encryption challenges, emphasizing the continual evolution of techniques to enhance security and overcome vulnerabilities.[25] These studies collectively contribute to the advancement of image encryption methodologies and provide a foundation for the proposed hybrid approach.

Methodological Approach

The proposed hybrid encryption method integrates two principles: image scrambling and genetic encryption. Scrambling alters pixel locations, while genetic encryption employs genetic algorithms for key generation.[26] The algorithm undergoes testing against brute force and other key attacks, demonstrating its resilience and security.

Image Encryption Scrambling: Image scrambling involves changing the arrangement of pixels in an image, enhancing security.[27] The proposed method employs a Logistic map for image scrambling, combining control parameters and Arnold mapping to improve the algorithm's efficiency.

Genetic Algorithm for Image Encryption: Genetic encryption utilizes sexual genetic recombination and Darwin's fitness survival and reproduction concept for key generation. Crossover and mutation operations enhance the algorithm's robustness.

Data Collection and Analysis: The study analyzes the algorithm's performance through various attacks, such as brute force and similar key attacks. Correlation graphs, histograms, and decrypted images are presented to illustrate the algorithm's efficacy.

Conclusion

The hybrid image encryption approach demonstrates enhanced security and real-time performance, meeting the demands for secure communication. The algorithm's key sensitivity and resistance against brute force attacks make it a promising solution for image encryption in various applications. In conclusion, the hybrid image encryption approach proposed in this study presents a promising solution to address the limitations of traditional image encryption methods. By combining the strengths of scrambling and genetic encryption, the algorithm not only enhances the security of transmitted images but also improves their overall quality. The robustness of the developed approach is evident in its resistance against brute force attacks and equivalent key attacks, showcasing its ability to withstand exhaustive analyses. The algorithm's key sensitivity is a critical feature, ensuring that the encryption remains secure even in the face of sophisticated attacks. The utilization of genetic encryption techniques, such as crossover and mutation operations, contributes to the algorithm's resilience and adaptability in generating secure

encryption keys. This adaptability is crucial in the dynamic landscape of cybersecurity, where evolving threats demand innovative and sophisticated encryption methods. The study's analysis of the algorithm's performance, including correlation graphs, histograms, and decrypted images, provides a comprehensive evaluation of its efficacy. The results demonstrate a clear improvement in image security compared to traditional methods. The correlation graphs reveal significant differences between the original and encrypted images, ensuring a high level of security against both basic and advanced brute force attacks.

Furthermore, the algorithm's real-time performance is commendable, meeting the demands for swift and secure encryption and decryption in various applications. The encryption time is notably fast, ensuring that the algorithm aligns with the requirements for real-time data processing in scenarios such as secure communication, medical services, military operations, and multimedia systems. In light of the findings, it is evident that the hybrid image encryption technique presented in this study not only addresses the existing flaws in traditional methods but also exceeds expectations in terms of security, key sensitivity, and real-time performance. Future research could delve deeper into optimizing the algorithm for specific application domains and exploring potential adaptations to emerging technologies. The continuous evolution of encryption techniques remains imperative in the ongoing efforts to secure sensitive information in an increasingly interconnected and data-driven world.

References

1. Shin CM, Seo DH, Cho KB, Lee HW, Kim SJ. Multilevel image encryption by binary phase XOR operations. InCLEO/Pacific Rim 2003. The 5th Pacific Rim Conference on Lasers and Electro-Optics (IEEE Cat. No. 03TH8671) 2003 Dec 15 (Vol. 2, pp. 426-vol). IEEE.
2. Zhang MR, Shao GC, Yi KC. T-matrix and its applications in image processing. Electronics Letters. 2004 Dec 9;40(25):1.
3. Ying W, DeLing Z, Lei J, Yaoguang W. The spatial-domain encryption of digital images based on high-dimension chaotic system. InIEEE Conference on Cybernetics and Intelligent Systems, 2004. 2004 Dec 1 (Vol. 2, pp. 1172-1176). IEEE.
4. Gu G, Han G. An enhanced chaos based image encryption algorithm. InFirst International Conference on Innovative Computing, Information and Control-Volume I (ICICIC'06) 2006 Aug 30 (Vol. 1, pp. 492-495). IEEE.
5. Pareek NK, Patidar V, Sud KK. Image encryption using chaotic logistic map. Image and vision computing. 2006 Sep 1;24(9):926-34.
6. Panigrahy SK, Acharya B, Jena D. Image encryption using self-invertible key matrix of hill cipher algorithm.
7. El Assad S, Farajallah M. A new chaos-based image encryption system. Signal Processing: Image Communication. 2016 Feb 1;41:144-57.
8. El Assad S, Farajallah M. A new chaos-based image encryption system. Signal Processing: Image Communication. 2016 Feb 1;41:144-57.
9. Chang CC, Hwang MS, Chen TS. A new encryption algorithm for image cryptosystems. Journal of Systems and Software. 2001 Sep 1;58(2):83-91.
10. Dey S, Ghosh R. A review of cryptographic properties of S-boxes with Generation and Analysis of crypto secure S-boxes. Cryptology ePrint Archive. 2018.
11. Farwa S, Shah T, Muhammad N, Bibi N, Jahangir A, Arshad S. An image encryption technique based on chaotic S-box and Arnold transform. International Journal of Advanced Computer Science and Applications. 2017;8(6).
12. Fu C, Wen ZK, Zhu ZL, Yu H. A security improved image encryption scheme based on chaotic Baker map and hyperchaotic Lorenz system. International Journal of Computational Science and Engineering. 2016;12(2-3):113-23.
13. Hariyanto E, Rahim R. Arnold's cat map algorithm in digital image encryption. International Journal of Science and Research (IJSR). 2016 Oct;5(10):1363-5.
14. Huang LC, Hwang MS, Tseng LY. Reversible data hiding for medical images in cloud computing environments based on chaotic Henon map. Journal of Electronic Science and Technology. 2013 Jun 25;11(2):230-6.
15. Liu J, Yin S, Li H, Teng L. A Density-based Clustering Method for K-anonymity Privacy Protection. J. Inf. Hiding Multim. Signal Process.. 2017 Jan;8(1):12-8.
16. Liu L, Cao Z. Analysis of two confidentialitypreserving image search schemes based on additive homomorphic encryption. International Journal of Electronics and Information Engineering. 2016 Sep 1;5(1):1-5.
17. McCarthy S, Smyth N, O'Sullivan E. A practical implementation of identity-based encryption over NTRU lattices. InCryptography and Coding: 16th IMA International Conference, IMACC 2017, Oxford, UK, December 12-14, 2017, Proceedings 16 2017 (pp. 227-246). Springer International Publishing.
18. Rajendran S, Doraipandian M. Chaotic map based random image steganography using lsb technique. Int. J. Netw. Secur.. 2017 Jul 1;19(4):593-8.
19. Sharma H, Khatri N. An image encryption scheme using chaotic sequence for pixel scrambling and DFrFT. InProceedings of First International Conference on Smart System, Innovations and Computing: SSIC 2017, Jaipur, India 2018 (pp. 487-493). Springer Singapore.
20. Su X, Li W, Hu H. Cryptanalysis of a chaos-based image encryption scheme combining DNA coding and entropy.

Multimedia Tools and Applications. 2017 Jun;76:14021-33.
21. Li H, Li H, Wei K, Yin S, Zhao C. A Multi-keyword Search Algorithm Based on Polynomial Function and Safety Inner-product Method in Secure Cloud Environment. J. Inf. Hiding Multim. Signal Process.. 2017 Mar;8(2):413-22.
22. Teng L, Li H, Liu J, Yin S. An Efficient and Secure Cipher-Text Retrieval Scheme Based on Mixed Homomorphic Encryption and Multi-Attribute Sorting Method. Int. J. Netw. Secur.. 2018 Sep 1;20(5):872-8.
23. Wu J, Liao X, Yang B. Color image encryption based on chaotic systems and elliptic curve ElGamal scheme. Signal Processing. 2017 Dec 1;141:109-24.
24. Yin S, Liu J, Teng L. Improved Elliptic Curve Cryptography with Homomorphic Encryption for Medical Image Encryption. Int. J. Netw. Secur.. 2020 May 1;22(3):419-24.
25. Ye G, Huang X. An efficient symmetric image encryption algorithm based on an intertwining logistic map. Neurocomputing. 2017 Aug 16;251:45-53.
26. Yin S, Liu J. A K-means Approach for Map-Reduce Model and Social Network Privacy Protection. J. Inf. Hiding Multim. Signal Process.. 2016 Nov;7(6):1215-21.
27. Zhang Q, Yang LT, Liu X, Chen Z, Li P. A tucker deep computation model for mobile multimedia feature learning. ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM). 2017 Aug 10;13(3s):1-8.