International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Comparative Analysis of Image Encryption Techniques

[1]Nainee Patel, [2]Dr. Kalpana Rai

[1,2] Sagar Institute of Research & Technology-Excellence, Bhopal, India

ABSTRACT

The Internet has become a primary way for people to share information. Encryption is necessary to prevent eavesdropping during the long-distance transfer of data over a public network. If you're trying to keep data safe over an unsecured network, the network's dependability is crucial. Since e-commerce, e-banking and multimedia technologies are often seen online, many encryption methods have been found to secure the data on the network, and new inventive encryption schemes have been in demand. In recent years, the primary use of cryptographic coding techniques has been the protection of data sent over an unsecured network. In addition, the researchers developed a wide variety of cryptographic algorithms for concealing information and effectively sharing it across an unsecured network. All cryptographic methods employ some kind of image encryption when sending images over an unsecured network. This paper's goal is to present a literature assessment of several techniques, methodologies, and algorithms for the image encryption

Keywords: Image Encryption, Cryptography, Image security, Decryption.

Introduction

It is widely known that images are one of the most common types of multimedia, and they play an extremely significant part in the everyday lives of people. In addition to this, there is a significant necessity for its use in all aspects of life. It is essential to encrypt pictures because, in people's day-to-day lives, photos may readily betray personal privacy, and images have high confidentiality needs in particular specialized sectors. As a result of the fact that the vast majority of images are now stored and displayed in digital form, the encryption method for digital images has also been the subject of a great deal of research in the field of secure communication [1]. A matrix is used for the storage of digital photographs. They may be broken down into a collection of sequences in the two dimensions. When digital pictures are encrypted, the information that is conveyed inside these two-dimensional patterns is hidden from the attackers so that they are unable to read it. However, the technique used to encrypt images is not the same as the typical algorithm used to encrypt data. This is because the algorithm used to encrypt images must simultaneously fulfill high computing efficiency requirements and minimize information loss. Because of the qualities that are intrinsic to the picture, such as a high level of redundancy, a huge volume of data, a strong correlation between neighboring pixels, and real-time transmission, the image may be processed quickly. The Image Encryption techniques are classification in shown in Fig.1

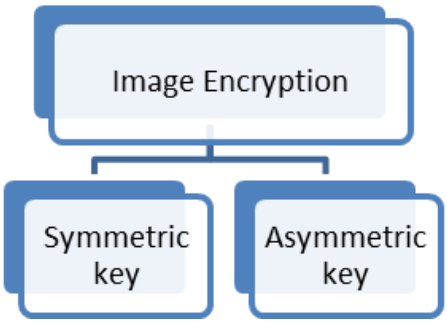
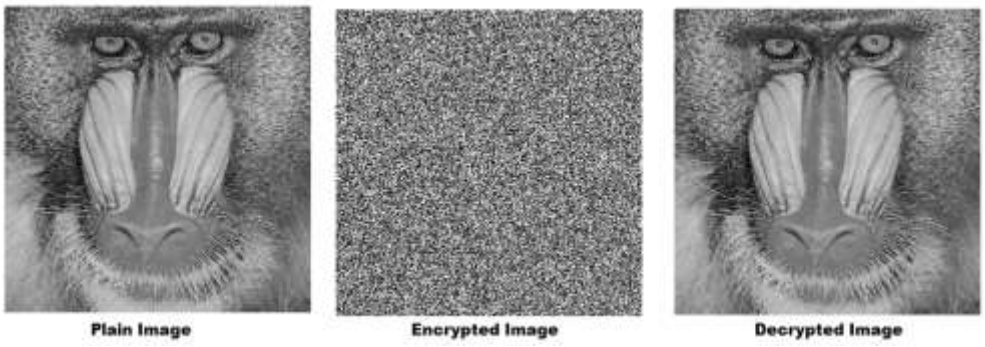


Fig. 1 - Image Encryption Approaches

While symmetric encryption uses a single key that must be shared among the people who need to receive the message, asymmetric encryption uses a pair of public key and a private key to encrypt and decrypt messages when communicating. The single key that is used for symmetric encryption is required to be shared among the people who need to receive the message. Fig. 2 demonstrates the process of image encryption, where original image is called as plain-image while the unreadable image is called as cipher or encrypted image.



Literature Review

A chaotic encryption of a picture has been presented by Jayashree et al. utilizing the integer wavelet transform (IWT), together with global bit scrambling (GBS) [2]. IWT is used to perform picture transformations and decompositions at this stage. After that, a map with a random layout is input into the encryption method. In order to make the encryption more secure, a key-dependent bit scrambling (also known as GBS) has been used instead of pixel scrambling. In addition to the enhanced resistance against intruder assaults, it strengthens the reliance of critical components.

By incorporating chaotic Baker Maps into the discrete Fourier transform, Hala et al. provide a method that is both safe and efficient for the encryption and decryption of visual data (DFT) [3]. The modified picture coefficients are subjected to an action provided by a baker map in the frequency domain, which enables the proposed approach to achieve a high level of encryption efficiency. The development and testing of a simulation for use in statistical analysis using MATLAB. The findings that were obtained proved that the strategy that was provided was better in terms of encryption quality, statistical measures, information entropy, maximum deviation and irregular deviation, differential, and noise immunity tests. Fig. 3 explains the cryptographic process used by Hala et al.

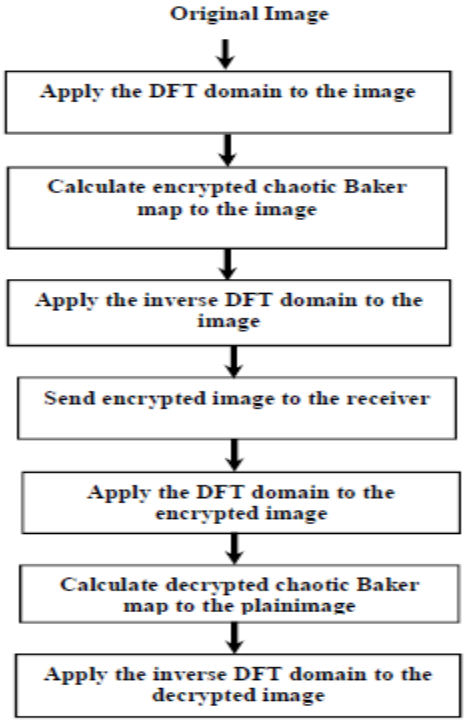


Fig. 3 - Cryptosystem Algorithm [3]

An picture encryption method that is based on a six-dimensional hyperchaotic system and DNA encoding has been proposed by Mengmeng et al. in order to address the issue of inadequate levels of security present in previously developed image encryption algorithms [1]. To begin, the pixel values for the R, G, and B channels are chopped up into blocks and then zeroed out. Second, DNA coding and DNA operations make advantage of the chaotic sequence that is produced by the six-dimensional hyperchaotic system and logistic mapping. Third, the values of the three-channel pixels that have been decoded are jumbled up using diagonal traversal. In the last step, a ciphertext picture should be produced by merging the channels. The simulation tests and performance studies that were conducted revealed that the algorithm had strong security performance, good encryption and decryption effects, and the ability to successfully resist a variety of popular attack techniques. **Fig. 4** explains the cryptographic process used by Mengmeng et al.

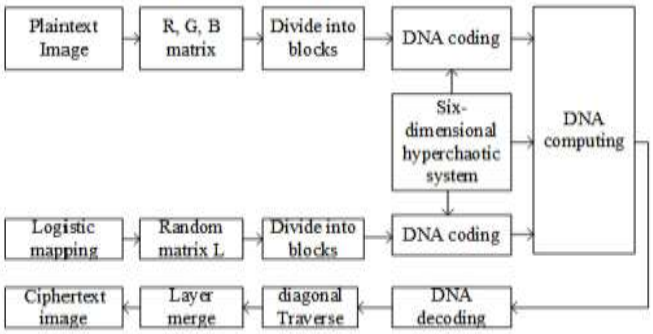


Fig. 4 - Encryption Approach [1]

Dalia et al. proposes AES and RSA based image encryption scheme [4]. The aim of the study is to compare Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA) encryption algorithms in image encryption using MATLAB. The evaluation of the effectiveness of each algorithm's picture encryption is what serves as the basis for the comparison. In addition, doing an analysis of the correlation findings and the histogram. According to the findings, the AES method offers superior quality picture encryption, as seen by the histogram's more converging column positions. In addition, the correlation coefficient for the AES algorithm has a tendency to be closer to zero, which indicates a larger association. The results of this investigation indicated, on the whole, that the RSA method is inferior than the AES algorithm when it comes to picture encryption. Tao et al. proposes a new image encryption algorithm based on two-dimensional Lorenz and Logistic [5]. The complexity of these two chaotic mapping techniques is rather low. The picture is encrypted and decrypted using the two-dimensional Lorenz chaotic model, which generates chaotic sequences that are employed in both processes. The fact that the technique can decrypt a number of well-known pictures demonstrates that it has both excellent security and great resilience. In addition, the paper investigates the safety of encryption algorithms by performing an analysis of the histogram, the entropy process of information, an investigation of correlation, a differential attack, a key sensitivity test, an examination of secret key space, noise attacks, and a contrast analysis. The image encryption algorithm that was proposed in this paper was compared to several other image encryption algorithms that already existed. The comparison revealed that the proposed algorithm possesses the characteristics of having a large secret key space, sensitivity to the key, a small correlation coefficient, and high contrast. In addition to it, the algorithm for encryption is used. It is also able to withstand assaults from loud noises.

An improved picture encryption technique has been presented by Corina et al., which makes use of Haar wavelet packets decomposition and four chaotic maps [6]. In order to scramble the wavelet packets, we suggest using a permutation that is derived from the Baker chaotic map. Both the ciphered picture and the key space of the cryptosystem are increased in entropy via the use of two different chaotic maps. These maps are the three-dimensional Arnold map, which is applied twice, and the tent map paired with the logistic map. Simulations done in Matlab reveal that the use of these chaotic maps raises both the entropy of the encrypted pictures and the degree to which the pixels are no longer correlated with one another. Utilizing all four maps allows for an increase in available key space, which is another advantage gained from doing so. Fig. 4 explained the process used by Corina et al.

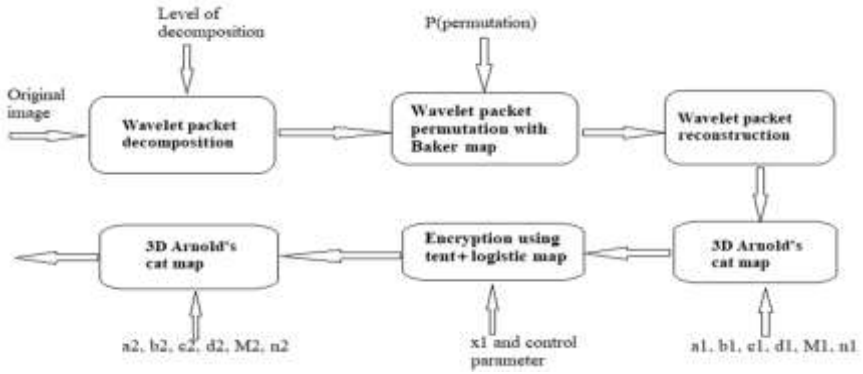


Fig. 4 - Image Encryption Approach [6]

Performance Analysis:

This section provides a visual representation of various performance criteria that are often used and are utilized in the process of evaluating the performance characteristics of any image encryption technique. The several typical performance indicators used in the various types of publications are outlined in Table 1.

Histogram Analysis: The study of the picture's decrypted histogram is one of the simplest and most straightforward approaches of showing the quality of the image encryption. It is desirable to observe a histogram that is uniformly distributed for a ciphertext picture since a competent image encryption technique would typically encrypt a plaintext image into something that seems random [1].

SSIM: The structural similarity index, also known as the SSIM index, is a tool for determining the degree to which two photographs are similar to one another. The SSIM index that was arrived at is a decimal number that falls between -1 and 1 [2].

Correlation coefficient: The correlation coefficient (CC) measures the degree to which two adjacent pixels in a picture are related to one another. In order to protect against statistical assaults, it is essential for the encrypted data to have a very low correlation when compared to the data that was originally collected [4].

Entropy: The amount of unpredictability that can be measured in grayscale is referred as the entropy. It may be deduced that the technique of encrypting data is preferable due to the equal distribution of gray levels [6].

Table 1. Comparison of recent papers based on the evaluation matrices used by them to evaluate performance

References	Histogram	SSIM	CC	Entropy
Mengmeng et al. [1]	✓	×	✓	✓
Jayashree et al. [2]	✓	✓	✓	✓
Hala et al. [3]	✓	✓	✓	✓
Dalia et al. [4]	✓	×	✓	×
Tao et al. [5]	✓	×	✓	✓
Corina et al. [6]	✓	×	✓	✓

4. Conclusion

Throughout the course of this research, a number of different strategies for encrypting images and the literature pertaining to those strategies were explored. In this day and age, one's personal information is more important than anything else, and this is especially true in situations when a breach might result in the loss of financial and social loss. In order to prove that the enumeration of the encryption methods is accurate, a variety of different encryption techniques are researched and analyzed. All of the algorithms, methodologies, and procedures that were used are completely unique to this project. New methods of encryption are being developed each and every day. To the very end of time, there will always be a significant demand for more robust encryption systems that provide a high level of protection.

References

[1]. M. Zhang and W. Wu, “Research on Image Encryption Technology Based on Hyperchaotic System and DNA Encoding,” in 2021 IEEE International Conference on Artificial Intelligence and Industrial Design, AIID 2021, 2021, doi: 10.1109/AIID51893.2021.9456457.

[2]. Karmakar and M. K. Mandal, “Chaos-based image encryption using integer wavelet transform,” in 2020 7th International Conference on Signal Processing and Integrated Networks, SPIN 2020, 2020, doi: 10.1109/SPIN48934.2020.9071316.

[3]. H. S. El-Sayed, A. Afifi, M. A. AlZain, and O. S. Faragallah, “An image cryptosystem using chaotic baker map in DFT,” in 2021 International Conference of Women in Data Science at Taif University, WiDSTaif 2021, 2021, doi: 10.1109/WIDSTAIF52235.2021.9430208.

[4]. D. M. Alsaffar et al., “Image Encryption Based on AES and RSA Algorithms,” in ICCAIS 2020 - 3rd International Conference on Computer Applications and Information Security, 2020, doi: 10.1109/ICCAIS48893.2020.9096809.

[5]. T. Li, B. Du, and X. Liang, “Image Encryption Algorithm Based on Logistic and Two-Dimensional Lorenz,” IEEE Access, vol. 8, 2020, doi: 10.1109/ACCESS.2020.2966264.

[6]. C. MacOvei, M. Raducanu, and O. Datcu, “Image encryption algorithm using wavelet packets and multiple chaotic maps,” in 2020 14th International Symposium on Electronics and Telecommunications, ISETC 2020 - Conference Proceedings, 2020, doi: 10.1109/ISETC50328.2020.9301088