Image Encryption Techniques: A Review

Ashish Pant[1], Palika Jajoo[1], Dolly Mittal[2], Richa Sharma[3]

[1]Department of Computer Science & Engineering, Swami Keshvanand Institute of Technology, Management & Gramothan, Jaipur-302017 (INDIA)

[2]Department of Information Technology, Swami Keshvanand Institute of Technology, Management & Gramothan, Jaipur-302017 (INDIA)

[3]Department of Computer Science & Engineering (AI), Swami Keshvanand Institute of Technology, Management & Gramothan, Jaipur-302017 (INDIA)

Email: **ashish.pant@skit.ac.in, palika@skit.ac.in, dolly.mittal@skit.ac.in, richasharma@skit.ac.in**

Received 01.09.2023 **received in revised form** 30.09.2023, **accepted** 16.10.2023

DOI: 10.47904/IJSKIT.13.2.2023.14-22

Abstract- **The increased reliance on digital images in various domains has led to a growing need for effective image encryption techniques. This study provides a thorough analysis of image encryption methods, providing an overview of their principles, advantages, and limitations. The review covers symmetric and asymmetric encryption algorithms, chaos-based encryption, visual cryptography, and transform domain techniques.**

By exploring these techniques, researchers and practitioners gain valuable insights into their security, computational efficiency, and applicability in different scenarios. Comparative analysis helps in understanding the trade-offs involved in selecting the most suitable technique for specific requirements. The review also addresses challenges in image encryption, such as maintaining image quality, ensuring data integrity, and countering attacks.

The findings of this review aid in decision-making processes, enabling the selection of appropriate image encryption techniques for secure digital image communication and storage. Moreover, it highlights potential research directions and emerging trends, encouraging further improvements in image encryption technology.

Keywords– **Image encryption, symmetric encryption, chaos-based encryption, data integrity**.

1. INTRODUCTION

The internet's explosive growth and information technologies has led to the widespread use of digital technology for communication purposes, including images, audio, and video. Images are essential in many fields, including the military, national security, and diplomatic relations due to the highly sensitive information they often contain. It is imperative to ensure the utmost security of these images, both when stored in vulnerable archives and during transmission over unstable networks.

One effective technique for enhancing image security is encryption. Encryption involves transforming an image into an unreadable form using a specific key, rendering it unintelligible to unauthorized users. By applying the appropriate decryption process, which essentially reverses the encryption operation, the original image can be recovered.

To illustrate this process let us shortly describe a encryption method which is called image scrambling using Arnold transformation [14]. Figure 1 represents the original image, which undergoes encryption to generate a srambled or encrypted version as depicted in Figure 2. The encoding procedure yields the encrypted image. Conversely, when the intended recipient receives the encrypted image, decryption procedure can be applied, as shown in Figure 3, to retrieve the original information. This ensures the confidentiality and integrity of the image during transmission or storage.

The primary objective of image protection is to preserve anonymity, integrity, and authenticity [1]. Encryption techniques serve as a critical means to achieve these goals, as they offer defense against a wide range of security threats.

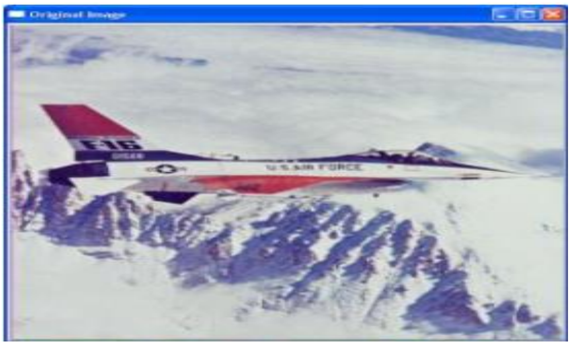

Figure 1: Plain image [14]

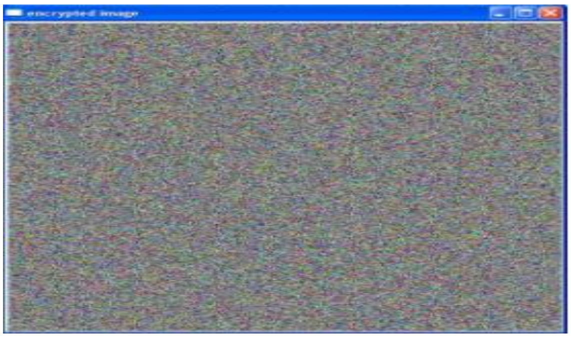

Figure 2: Encrypted Image [14]

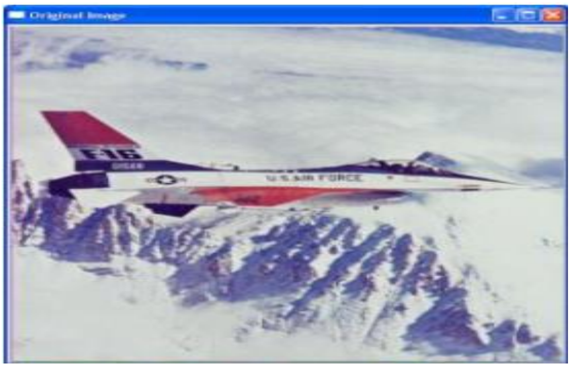

Figure 3: Decrypted Image [14]

2. CATEGORIES OF ENCRYPTION TECHNIQUES & CRYPTOGRAPHY

Encryption techniques can be broadly categorized into the following three categories. Figure 4, Figure 5 and Figure 6 represent the flowcharts of each of the categories. At the end Table 1 gives the structured overview of the encryption techniques.

- Position Permutation Techniques: In this technique, the order of pixels in an image is rearranged, resulting in a modified image where the original information becomes invisible. By shuffling the positions of pixels, the visual structure of the image is altered, providing a form of encryption. [2] The goal is to make the original information invisible by changing the order of pixel locations which introduces confusion and makes it difficult for unauthorized users to decipher the original information. One common example of position permutation technique in image encryption is the Block Permutation technique. In this method, the image is divided into blocks, and the positions of these blocks are shuffled based on a secret key. The blocks can be of fixed size, such as 8x8 pixels, and the permutation of these blocks provides a form of encryption.
- Value Transformation Techniques: This method includes changing a network's weights and biases depending on a binary sequence generated by a chaotic system. These modified network parameters are then used for encrypting or decrypting individual signal elements. By transforming the picture pixel values calculated using a chaotic sequence, encryption is achieved [3]. Example of value transformation techniques can be chaotic maps. Chaotic maps, such as logistic maps or Arnold cat maps, can be used to scramble pixel values in an image. These maps generate chaotic sequences that are applied to pixel values, providing a form of encryption.
- Combination Techniques: This category combines approaches for position permutation and value transformation. First, the pixels of the image are rearranged using position permutation, changing their spatial order. The image is further altered based on a specified encryption key by replacing the pixel values with a key generator.[4] A common example of this technique is Cascade Encryption. Applying multiple encryption algorithms sequentially. For example, encrypting an image with algorithm A, followed by encrypting the output with algorithm B. This adds an extra layer of security.

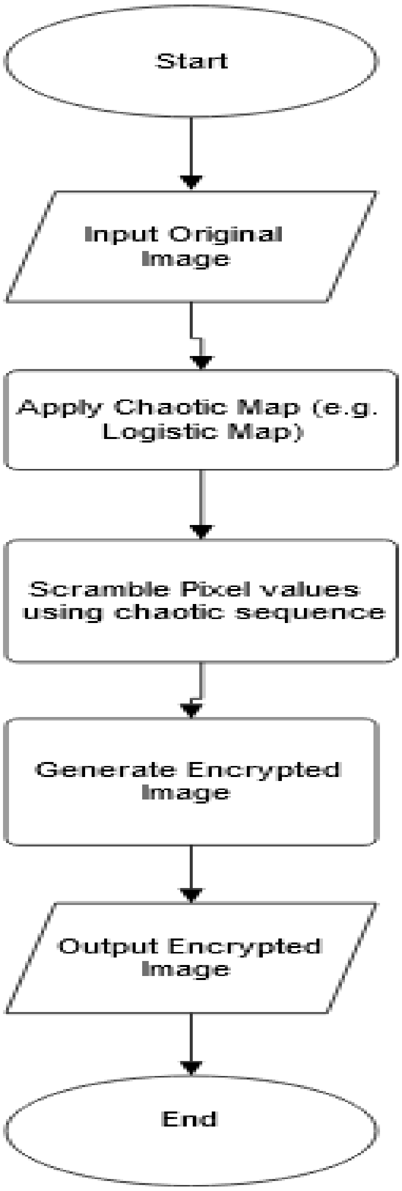
Start
Input Original Image
Apply Chaotic Map (e.g. Logistic Map)
Scramble Pixel values using chaotic sequence
Generate Encrypted Image
Output Encrypted Image
End

Figure 4: Value Transformation

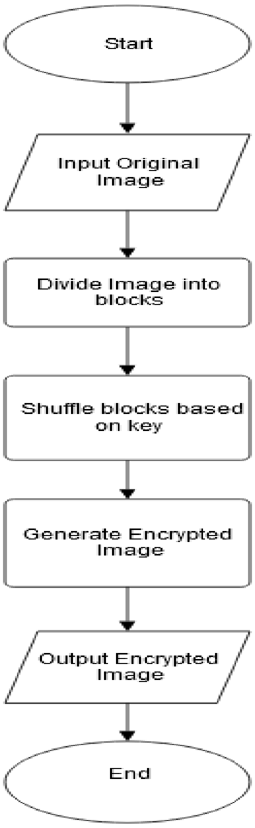

Figure 5: Position Permutation

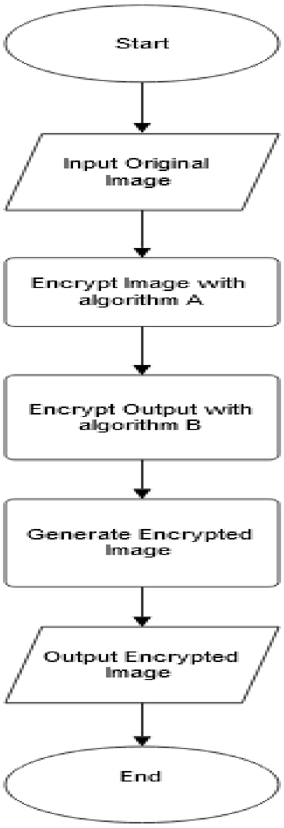

Figure 6: Combination Technique

Table 1: Structured overview of encryption techniques

Encryption Technique Type	**Definition**	**Key Strengths**	**Key Weaknesses**	**Area of Application**
Value Transformation	Network weights and biases are changed based on a chaotic sequenceChaotic maps (e.g., logistic or Arnold cat maps) can scramble pixel values in an image.	Chaotic sequences enhance unpredictability - Can be applied to various data types, not limited to images	Sensitivity to initial conditions in chaotic maps - Computational intensity may be high	Multimedia encryption, signal processing
Position Permutation	Order of pixels in an image is rearranged, altering the visual structure. Block Permutation is an example where blocks are shuffled based on a secret key.	Provides visual alteration Block-based permutation adds complexity to decryption	Susceptible to attacks if key space is limited May not be suitable for all types of images	Visual encryption, image security
Combination Techniques	Pixels are rearranged using position permutation , and pixel values are further altered based on an encryption key. Cascade Encryption is an example of applying multiple algorithms sequentially .	Combines benefits of both position permutation and value transformation - Adds an extra layer of security	Complexity may impact performance - Requires careful implementation to avoid vulnerabilities	Multi-layered security, sensitive data protection

Cryptography: Cryptography is the field of study that encompasses various methods and techniques used for enciphering data. It involves the transformation of plaintext into ciphertext to ensure secure communication.

Types of Cryptography: There are two primary categories of cryptography [3]

1. ***Secret Key Cryptography:*** Secret key cryptography, also known as symmetric key cryptography, is based on a shared secret code, or key, between the sender and the receiver. The key is used by the sender to encrypt the communication, and the recipient uses the key to decode it. This type of cryptography is suitable for scenarios where both parties have prior knowledge of the secret key.

2. ***Public Key Cryptography***: Public key cryptography, also known as asymmetric key cryptography, employs two keys for encryption and decoding. Using matching public and private keys is the fundamental component of this technique. The public key is made available and used for encryption, while the private key is kept secret and used for decoding. Public key cryptography is highly useful when secure communication is required between parties who do not already have a shared secret key.

The following are the various objectives that cryptography aims to achieve: [4]

1. Confidentiality: Cryptography ensures that information transmitted over a computer system can only be accessed by authorized parties and remains inaccessible to anyone else.
2. Authentication: By using cryptographic methods to confirm the sender's identity, the receiving system may determine if the information is coming from a reliable source or an impostor.
3. Integrity: Only authorized parties can modify transmitted information. Cryptography ensures that the message remains unaltered during transmission, preventing unauthorized tampering by any intermediaries between the sender and receiver.
4. Non-repudiation: Cryptography provides a means to prevent both the sender and the receiver from denying the transmission of a message. It establishes a mechanism to validate the authenticity and integrity of the communication, making it difficult for either party to refute their involvement.
5. Access Control: Cryptography enables the restriction of information access solely to authorized parties. It ensures that only those with proper authorization can retrieve and utilize the given information.

3. IMAGE SECURITY PARAMETERS

Several key parameters are frequently used to assess image security [5]. These parameters include:

1. Large key space: The term 'key space' refers to the number of potential encryption or decryption keys. A larger key space enhances the security of the image, making it more challenging for unauthorized parties to access the original content.
2. Uniform image histogram: The distribution of pixel intensities in a picture is shown by an image histogram. A uniform image histogram indicates that the pixel values are evenly distributed, which can be desirable in image security as it makes it harder for attackers to identify specific regions or features within the image.
3. Information entropy: Entropy gauges how unpredictable or uncertain a picture is. Images with higher entropy have a greater level of randomness, which can make them more resistant to cryptographic attacks or steganalysis techniques.
4. Correlation analyses: Correlation analyses examine the statistical relationships between different image elements, such as pixels or regions. By assessing correlations, it is possible to detect any hidden patterns or modifications within an image, providing a measure of image integrity.

Practitioners use these image security parameters, practitioners can design and implement robust security measures to protect digital images and ensure their confidentiality, integrity, and authenticity. It is important to continuously evaluate and enhance these parameters as new security threats and vulnerabilities emerge.

4. LITERATURE REVIEW

In this section, we have done literature review on various encryption techniques. The literature review is summarized at the end of this section using Table 2 which provides a comparative overview of various image encryption techniques, outlining their key features, strengths, weaknesses, evaluation metrics, and applications, facilitating a comprehensive understanding of each method's characteristics

A. Digital Image Encryption and Decryption based on RSA Algorithm

In order to test encryption and decryption, the RSA method was simulated in this study [6]. The two prime numbers were used to create an improved algorithm that generates encryption and decryption keys and improves data security objectives including confidentiality, authenticity, secrecy, and integrity. Input Image was the image which must be encrypted. Before employing the public key cryptosystem, a pair of keys must be generated. With the use of an algorithm, picture hash functions were employed to give the image a distinct hash value. Image Hash is used in place of cryptographic hash techniques like SHA-256 and MD5 to assure the correctness of the images.

Radhakrishna M, et al. (2022) used the Pearson autocorrelation function to look for patterns in the data. The autocorrelation plot shows distinctive patterns for each original picture. In contrast, the correlation plot of the encrypted data displayed randomness without any discernible patterns. This characteristic significantly mitigated the risk of statistical analysis attacks on the encrypted image.

The horizontal, vertical, and diagonal positions of the pixels in the images, both encrypted and unencrypted, are chosen at random. The correlation degree, r_{xy} based on these randomly selected pixels was calculated as:

$$r_{xy} = \frac{E((x - E(x))(y - E(y)))}{\sqrt{\frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2}\sqrt{\frac{1}{N}\sum_{i=1}^{N}(y_i - E(y))^2}},$$

where, N is the number of data points or pixels. x and y are neighboring pixels in different directions. x_i and y_i are the individual data points of variables x and y, respectively and

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$$

is the sample mean for x. Similarly, *E(y)* is the sample mean for y.

SSIM and MSE were used for Image Quality evaluation [6]

B. New Image Encryption Technique Based on Combination of Block Displacement and Block Cipher Technique

In this research, a new picture encryption method that combines the "block displacement" and "block cypher" approaches is presented [7]. Blocks from the original image were split up and moved both horizontally and vertically. The generated image was then divided into blocks of pixels and converted to binary representation for each block. At the same time, a key value was selected and transformed into its binary representation. The proposed block-based algorithm XORed the key value with each corresponding image value, resulting in the generation of an encrypted image.

To make it easier to encrypt and decode photos with a key that the user defines, a dedicated algorithm was developed. It is important to note that the size of the cipher image produced through this method could differ from the original image, as the scaling process was implemented to ensure 128-bit blocks at a time. This approach proved to be well-suited for the safe transfer of sensitive data across the Internet.

The original picture was resized and split into blocks of size n*n in the first stage. This scaled image was then utilized for encryption. The scaling process was employed to ensure that the image's block size matched the desired n*n dimensions. By displacing the blocks, the correlation between adjacent pixels was reduced, thereby increasing the entropy.

The algorithm for horizontal displacement of blocks determined the number of blocks in the picture, both horizontally and vertically. Based on this information, it proceeded to strongly move the blocks in a horizontal direction at a 1:1 ratio. The algorithm for vertical displacement of blocks operated similarly to previous algorithm, but as opposed to moving them horizontally, it moved the blocks vertically. The vertical displacement was carried out in the same 1:1 manner as the horizontal displacement. Blocks were moved vertically, and then encryption was carried out.

To get the original key or to analyse the suggested key using cryptanalysis, an exhaustive number of attempts, approximately 2^{128} times, would be required. This level of difficulty makes it nearly impossible for any hacker to break the key successfully. Furthermore, the proposed algorithm did not involve any mathematical formulas that could introduce floating-point errors.

To evaluate the proposed algorithm, the correlation coefficient and entropy values were calculated for its output [7]

C. Image encryption using block-based transformation algorithm

This paper introduced a novel method for encrypting images, consisting of three essential components. Firstly, the original image underwent encryption using a substantial secret key by performing rightward rotations of pixel bits through XOR operations. Secondly, steganography techniques were applied to the encrypted image by modifying it with the least significant bits (LSBs) derived from the cover image. This process resulted in the creation of a stego image. Finally, to establish ownership, the stego image was subjected to watermarking in both the time and frequency domains. [8]

The proposed approach demonstrated efficiency, simplicity, and high levels of security, effectively mitigating various threats and attacks. Peak signal-to-noise ratio (PSNR) and mean square error (MSE) measurements were made in order to evaluate the findings. A thorough comparison investigation was also carried out, comparing the effectiveness of the suggested strategy with other well-known current procedures.

Proposed Encryption Algorithm

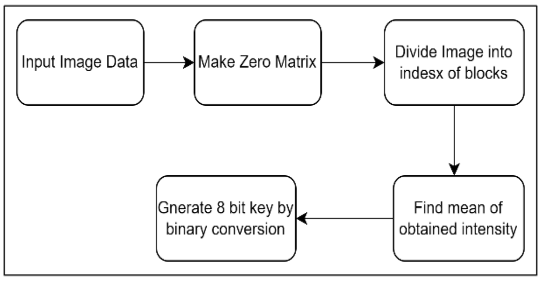
Input Image Data
Make Zero Matrix
Divide Image into indesx of blocks
Find mean of obtained intensity
Gnerate 8 bit key by binary conversion

Figure 7: Algorithm block diagram

This research explored different image encryption algorithms, such as S-boxes substitution combined with chaos random sequence, Digital watermarking using the block cypher RC6 and secure JPEG2000 encryption techniques based on arithmetic coding, the ASE encryption algorithm with digital signal processing technology, and a specialized approach for image encryption.

The objective of this research was to convert images into coded representations that were difficult to understand. The image encryption techniques employed aimed to maintain the privacy and accuracy of the picture's information, enhancing its security, and preventing unauthorized access.[8]

D. An image encryption method based on chaos system and AES algorithm

This study proposed a novel image encryption method based on a chaotic sequence and a modified AES algorithm. The Arnold chaos sequence was used to create the encryption key, and the original picture was encrypted with a modified version of the AES method with round keys generated from the chaos system. This proposed method offered several advantages, including reduced time complexity and enhanced diffusion capability, which made the encrypted images resistant to differential attacks. Additionally, the algorithm's large key space provided robust protection against brute-force attacks.[9]

The suggested approach showed a high level of sensitivity to the starting points and input picture. The encrypted picture underwent considerable modifications as a result of even small changes in these parameters. Statistical analyses confirmed the algorithm's ability to safeguard images against statistical attacks, as the entropy values closely aligned with the expected ideal values. Simulation results further demonstrated the algorithm's effectiveness, as minor alterations in the original image and key produced substantial transformations in the encrypted image, ensuring the original image remained inaccessible to unauthorized parties.

The conventional AES algorithm's general design was used in this study to encrypt images. The suggested approach was modified in several ways to make it especially suitable for picture encryption. The original AES encryption method had two significant alterations as a result of these enhancements. First, permutable operations from the common encryption method were substituted for the recommended propagation procedures. The second change involved replacing the column integration procedure with the linear transformation operation**.** [9]

E. A novel image encryption scheme based on an elliptic curve

The paper introduced a new technique for image encryption that employed Elliptic Curve Cryptography (ECC) to achieve heightened security compared to other cryptosystems with equivalent key sizes.[10]

Two objectives were laid forward for the article. It first presented unique methods for building substitution boxes (S-boxes) and creating pseudo-random numbers (PRNs) by establishing a total order on an elliptic curve (EC) over a prime field. A search strategy was used to quickly construct an EC as opposed to the computationally demanding classical group law. The x-coordinates of the points on an ordered elliptic curve (OEC) were used to generate S-boxes, whilst the Frobenius map and n-norm were generalized to the points on the OEC to create PRNs.

Secondly, the study proposed a two-phase image encryption method utilizing the recently developed S-box and PRN generating algorithms. In this system, a dynamic S-box was used to confuse the simple picture after it experienced diffusion through the suggested PRN as a masking mechanism. The suggested approaches' strong cryptographic characteristics, such as the creation of strong S-boxes, PRNs with high entropy, and the best defence against contemporary picture cryptanalysis, were proved by extensive analysis and comparison with current S-box and image encryption techniques. [10]

F. A novel image encryption scheme using both pixel level and bit level permutation with chaotic map

The study discussed here combines a chaotic map, the scan method, and cyclic shift operation to provide a unique symmetric key encryption technique. The Hilbert curve and Henon map were used in the approach to implement confusion and diffusion. To ensure visual scrambling, bit-level and pixel-level permutations were used. Bit-level permutation was implemented using a unique technique that made use of cyclic shift operations. The Henon map was used to produce the key streams for cyclic shift and diffusion operations. The double-scrambled picture served as the basis for the final encrypted image.[11]

The effectiveness of the proposed approach was evaluated using a variety of techniques, such as statistical analysis, entropy analysis, differential attack analysis, key sensitivity analysis, and known plaintext attack analysis. The suggested picture encryption method withstood numerous assaults and provided a high degree of security, according to experimental results. Additionally, it performed better than several established and cutting-edge picture encryption techniques.

G. Digital Image Encryption Algorithm Based on Pixels

This work suggests a brand-new method for pixel-based image encryption. The article included a thorough explanation of all the methods, applications, parameters, encryption and decryption stages, and other significant technologies employed in the technique. The image encryption process began by scrambling the image pixels, followed by applying a watermark to increase the difficulty of decoding. The final encrypted image was created by selecting a camouflaged image and combining its pixels or visual traits with the original image. Elliptic curve encryption (ECC) was used to encrypt the key parameters. Through experimentation, the algorithm's security, dependability, and effectiveness were confirmed and analysed. The outcomes of the experiment and algorithm evaluations showed that the new method for interactive pictures had a wide key space, high degree of security, and relatively long encryption durations. The high-level security needs of interactive information in a variety of industries, including aerospace, the military, secrecy, finance, economics, and national security, were met by this algorithm in a novel way.[12]

H. An Efficient Technique for Image Encryption and Decryption for Secured Multimedia Application

In this paper an approach for image encryption with key generation algorithm was proposed. Process of encryption is described in given Fig.8

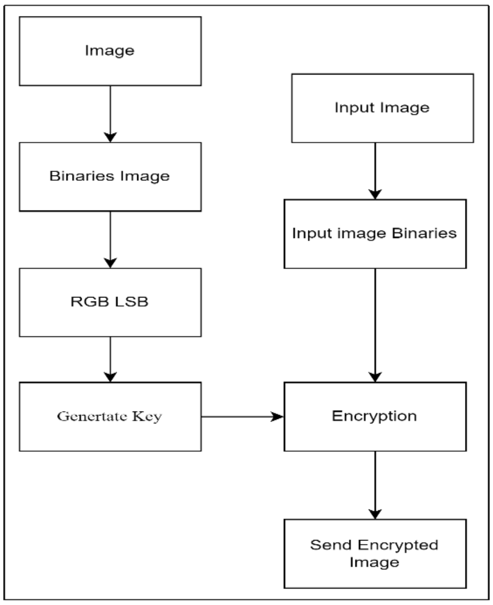

Figure 8: Encryption of Image

i) Binaries Image

Three channels were extracted from the input color image, and their values were converted into binary form. The resulting binary values were stored in three distinct multidimensional arrays, representing the red channel, green channel, and blue channel of the image. The algorithm involved generating three arrays to hold the binary data for each channel, allowing for the separate representation and processing of the color components.[13]

ii) LSB of RGB

In this process, the input image was considered for key generation, and the values of its pixels were converted into binary format. Once converted into binary, the algorithm focused on extracting the Least Significant Bit (LSB) from each pixel.

iii) Key Generation

Cryptographic keys were generated to facilitate the encryption and decryption of messages. The sender utilized these keys to generate a cipher image, while the receiver performed the reverse process to retrieve the original image. The key generation process involved extracting color channels (red, green, or blue) from the input image. Binary values were calculated for each pixel and stored in an array. The least significant bit (LSB) of each pixel was then obtained, resulting in a new array. Finally, the key was generated by examining each bit of the

LSB array and storing neighboring pixels with an absolute difference of one in a separate array.

iv) Encryption

Three different keys were generated from the image. Using key arrays and binary value arrays, encrypted images were created. The encryption process involved performing XOR operations on the keys and the image's three channels (red, green, and blue). The red channel of the input picture was encrypted using the key created from the red channel of the colour image, and the green and blue channels were encrypted using the corresponding channel keys.[13]

I. Sophisticated Image Encryption Using OpenCV

This paper focused on the utilization of the open-source computer vision library, commonly known as OpenCV, which involved an analysis of the data structure of IPL Image (IPL being the primary data type employed in OpenCV to represent images) and its corresponding member variables. Additionally, the fundamental functions provided by the library for image manipulation and processing were employed. These functions encompassed image loading, window creation, image saving, image creation, and spatial domain pixel access. To ensure image encryption, an approach known as the Arnold transformation, or cat-face transformation, was employed. This transformation entailed the scrambling of pixel coordinates, thus altering their locations. Subsequently, in order to color scramble, the image, the red, green, and blue channels' pixel values were changed using the Arnold transformation. As a result, the image became encrypted. To restore the original image and decrypt it, an inverse Arnold transformation was applied. [14]

J. A RGB image encryption technique using Lorenz and Rossler chaotic system on DNA sequences

The Lorenz-Rossler chaotic map was used in this study to create a strong colour picture encryption method. The suggested encryption method combined the chaotic Lorenz and Rossler systems to produce a random sequence. The red, green, and blue channels of a colour picture were then encrypted with the help of this created sequence. In the suggested method, the plain picture was encoded using the DNA cryptosystem's principles. A cross-channel procedure was developed to increase the simple image's level of unpredictability. In a series of tests, popular images from the USC-SIPI picture collection were utilised to assess the effectiveness of the recommended technique. The trials' findings demonstrated that, in terms of correlation coefficient, the recommended approach performed better than the traditional methods. To verify the security of the recommended encryption method, several security evaluations were carried out, including statistical analysis and key sensitivity analysis. The architecture of the proposed technique ensured that the key space would be large enough to resist brute force attacks. [15]

Table 2. Summary of Literature Review

Encryption Technique	Key Features	Strengths	Weaknesses	Evaluation Metrics	Application
RSA Algorithm	Public key cryptosystem, hash functions for image uniqueness	Confidentiality, authenticity, randomness in encrypted data	Computationally intensive, limited to relatively small key sizes	Pearson autocorrelation, SSIM, MSE	General image encryption, data security
Block Displacement & Block Cipher	Combination of block displacement and block cipher	Resistance to brute-force attacks, safe transfer of data over the Internet	Scaling process may alter image size, complexity in key management	Correlation coefficient, entropy	Secure data transfer
Block-Based Transformation Algorithm	Three components: Rotation, steganography, watermarking	Efficiency, simplicity, high security, resistance to threats	Limited details on the encryption algorithm, reliance on key secrecy	PSNR, MSE	Privacy protection, secure communication
Chaos System and AES Algorithm	Chaotic sequence, modified AES algorithm	Reduced time complexity, enhanced diffusion capability	Sensitivity to starting points and input picture, potential for computational intensity	Statistical analysis, entropy analysis	Robust protection against statistical and brute-force attacks
Elliptic Curve Cryptography (ECC)	S-box and PRN algorithms, two-phase encryption	Strong cryptographic characteristics,	Computational complexity in ECC, potential performance	Analysis and comparison with other techniques	Enhanced security in comparison to

	method	high entropy	impact		equivalent key-sized systems
Chaotic Map with Pixel and Bit Permutation	Chaotic map, scan method, cyclic shift operation	Statistical, entropy, and differential attack resistance	No explicit weaknesses mentioned, high degree of security	Statistical analysis, entropy analysis, key sensitivity	Resistant to various attacks, high security level
Pixel-Based Image Encryption	Pixel scrambling, watermarking, elliptic curve encryption	Wide key space, high security, relatively long encryption durations	Lack of details on specific encryption algorithm	Experiment and algorithm evaluations	Interactive image security in aerospace, military, finance
OpenCV with Arnold Transformation	OpenCV library, Arnold transformation for pixel scrambling	Utilization of open-source library, spatial domain pixel access	No specific weaknesses mentioned, potential dependency on external library	Arnold's Cat Map	General image encryption using open-source library
Lorenz and Rossler Chaotic System on DNA	Lorenz-Rossler chaotic map, DNA cryptosystem principles	High unpredictability, large key space	Limited details on implementation, potential computational intensity	Correlation coefficient, statistical analysis	Resistance against traditional and recently developed encryption met

5. CONCLUSION

In this paper, we have presented and analyzed several significant encryption techniques to familiarize readers with other algorithms used for encrypting images transmitted over networks. Through simulation results, it was observed that each algorithm possesses distinct advantages and disadvantages based on the applied techniques for image encryption. It can be concluded that all the examined techniques provide adequate security for image encryption, effectively preventing unauthorized access to images transmitted over open networks.

REFERENCES

[1] Amnesh Goel and Dr. Rakesh K Bhujade, "A review on digital image encryption techniques", International Journal of Advanced Technology & Engineering Research **(2018),** *National Conference on Recent Trends in Science, Technology & Management (NCRTSTM-2018)*

[2] Payal Sharma, Manju Godara and Ramanpreet Singh, "Digital Image Encryption Techniques: A Review", International Journal of Computing & Business Research **(2012)**, ISSN (Online): 2229-6166

[3] Monika Gunjal and Jasmine Jha, "A Survey Paper on Image Encryption Techniques", International Journal for Scientific Research & Development **(2013)**, Volume 1, Issue 9, Pages 1783-1786

[4] Ambika Oad, Himanshu Yadav and Anurag Jain, "A Review: Image Encryption Techniques and its Terminologies", International Journal of Engineering and Advanced Technology **(2014)**, Volume 3, Issue 4

[5] Akansha Dongre, Prof. Chetan Gupta, and Sonam Dubey, "A Survey on Various Image Encryption Technique and challenges", International Journal of Creative Research Thoughts **(2022)**, Volume 10, Issue 6, Pages f496-f499

[6] Radhakrishna M, Shridevi KS, Sowmya BS and Sushmitha TJ, "Digital Image Encryption and Decryption based on RSA Algorithm", International Journal of Scientific Research in Science, Engineering and Technology **(2022)**, Volume 9, Issue 4, Pages 168-173

[7] Keerti Kushwah and Sini Shibu, "New Image Encryption Technique Based on Combination of Block Displacement and Block Cipher Technique", International Journal of Computer Science and Information Technologies **(2013)**, Volume 4, Issue 1, Pages 61-65

[8] Afseen Bano and Prateek Singh, "Image Encryption using Block Based Transformation Algorithm", The Pharma Innovation Journal **(2019)**, Volume 8, Issue 3, Pages 11-18

[9] Alireza Arab, Mohammad Javad Rostami and Behnam Ghavami, "An image encryption method based on chaos system and AES algorithm", The Journal of Supercomputing **(2019)**, Volume 75, Issue 10, Pages 6663-6682

[10] Umar Hayat, Naveed Ahmed Azam, "A novel image encryption scheme based on an elliptic curve", Signal Processing **(2019),** Volume 155, Pages 391-402

[11] Shahna K.U. and Anuj Mohamed, "A novel image encryption scheme using both pixel level and bit level permutation with chaotic map", Applied Soft Computing Journal **(2020)**, Volume 90

[12] Guiliang Zhu, Weiping Wang, Xiaoqiang Zhang and Mengmeng Wang, "Digital Image Encryption Algorithm Based on Pixels", *2010 IEEE International Conference on Intelligent Computing and Intelligent Systems,* Xiamen **(2010)**, Pages 769-772

[13] Ashish S. Dongare, Dr. A.S. Alvi and Prof. N.M. Tarbani, "An Efficient Technique for Image Encryption and Decryption for Secured Multimedia Application", International Research Journal of Engineering and Technology **(2017)**, Volume 04, Issue 04

[14] Ashish Pant, Arjun Arora, Suneet Kumar and Prof. R P Arora, "Sophisticated Image Encryption Using OpenCV", International Journal of Advanced Research in Computer Science and Software Engineering **(2012)**, Volume 2, Issue 1.

[15] Ashish Girdhar and Vijay Kumar, "A RGB image encryption technique using Lorenz and Rossler chaotic system on DNA sequences", Multimedia Tools and Applications **(2018)**, Volume 77, Issue 20