IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 7, July 2024

DOI: 10.17148/IJARCCE.2024.13717

A Comprehensive Review of Image Encryption Techniques and Current Challenges

Sona Kalabat[1], Prof. Chetan Gupta[2]

M. Tech. Scholar, Dept. of CSE, SIRTS, Bhopal, India[1]

Assistant Professor, Dept. of CSE, SIRT, Bhopal, India[2]

Abstract: A secure environment is unattainable without the implementation of encryption technology. Given that images constitute a significant portion of multimedia data, safeguarding them is crucial in the modern context. The major challenge lies in how we can effectively protect our data. Encryption involves transforming a piece of information by encoding it such that only authorized individuals can decode, read, and understand it. This protects the information from unauthorized access by malicious entities. The encryption process involves subjecting the data to a series of mathematical transformations, producing an alternative form of the original data. This sequence of mathematical operations is known as an algorithm. In this paper, we have conducted a survey of various research papers and reviewed existing encryption techniques. Based on our survey, we also discuss the concept of two-way encryption, analyzing it in conjunction with the Data Encryption Standard (DES) for improved security.

Keywords: Encryption, Encoding, multimedia, confidentiality, integrity, authenticity, cryptography.

I. INTRODUCTION

Image encryption is a method used to transform an original image into an unintelligible form, making it difficult to comprehend without decryption. With the rapid expansion of multimedia applications, ensuring the security of image communication and storage has become a critical issue. Encryption is one of the primary ways to guarantee this security, as it prevents unauthorized access to the content without a decryption key. Images are composed of pixels, and image encryption essentially converts these images into an unreadable format. Many digital services necessitate robust security measures for the storage and transmission of digital images. Given the exponential growth of the internet, safeguarding digital images has become increasingly important and has garnered significant attention. The widespread use of multimedia technology has elevated the importance of digital images, surpassing that of traditional text and highlighting the need for stringent privacy protection. Encryption techniques for digital images are crucial for preventing unauthorized access and thwarting potential attacks. As electronic data exchange continues to grow, protecting the confidentiality of image data from unauthorized access is imperative. Security breaches can compromise user privacy and damage reputations, making data encryption essential for ensuring security in open networks like the internet. The significant increase in digital data transmission over public channels has further emphasized the importance of digital image security. Multimedia technology's proliferation in our society has enhanced the role of digital images, necessitating serious privacy protection for all applications. Different types of data require unique protection techniques, and most existing encryption algorithms are designed for text data. However, due to the large data sizes and real-time requirements of images, traditional encryption methods are often impractical [3].

II. TYPES OF CRYPTOGRAPHY

Cryptographic methods are employed when confidential messages need to be sent from one party to another over a communication channel. These methods require specific algorithms to encrypt the data. In today's world, where increasing amounts of sensitive information are stored on computers and transmitted via the Internet, it is crucial to ensure the security and safety of this information. Images are a vital component of our data, making it essential to protect them from unauthorized access. Numerous algorithms are available to safeguard images from unauthorized access.

Secret Key Cryptography: Also referred to as symmetric key cryptography, this method involves both the sender and receiver sharing the same secret code, known as the key. The sender encrypts the message with this key, and the receiver decrypts it using the same key.

Public Key Cryptography: Also known as asymmetric key cryptography, this approach uses a pair of keys for encryption and decryption. In public key cryptography, there is a matched pair of keys: a public key and a private key.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 7, July 2024

DOI: 10.17148/IJARCCE.2024.13717

Figure 1: Image Encryption Scheme

III. FEATURES OF IMAGE ENCRYPTION

1. Image security necessitates the following characteristics:
2. The encryption system must be computationally secure, requiring an extremely long computational time to break.
3. The encryption and decryption algorithms should be simple and fast.
4. The security mechanism needs to be flexible.
5. There should be minimal expansion of the encrypted image data.
6. The security mechanism should be widely applicable and acceptable, ideally designed to function as a commercial product [4].

IV. LITERATURE SURVEY

Image encryption techniques are essential for securing data within images. This section reviews various encryption methods explored in our study.

In [1] this paper author proposed an efficient key-based pattern enciphering scheme for digital color images. This method utilizes pixel value reordering with an adaptive key-based block selection algorithm. The scheme demonstrates high resistance to various cryptographic attacks. Multiple pixel reordering patterns are generated and applied to an image by partitioning it into blocks. The key (secret) determines the enciphering pattern for each partitioned image block, resulting in a final encrypted image. The image can be restored to its original form using the same key and pattern to reorder the pixel values in the corresponding blocks. The main advantages of this technique are its lossless decomposition, efficiency, and simplicity. Experimental results indicate that the proposed method effectively resists common cipher attacks.

In [3] this paper author conducted a survey on image encryption using Salsa20. This paper examined Salsa20 as an efficient and secure method for protecting digital image distribution. Various tests and comparisons were conducted to validate Salsa20's efficiency for image encryption, including visual testing, key space analysis, histogram analysis, information entropy, encryption quality, correlation analysis, differential analysis, sensitivity analysis, and performance analysis. Simulation experiments confirmed the effectiveness of the Salsa20 scheme for image encryption.

In [4] this paper author proposed a fast image cryptosystem based on AES. In this system, images are divided into 128-bit data blocks. AES in CBC mode is employed for image encryption. The first block of the plain image is permuted using an initial vector, followed by AES in cipher block chaining mode to encrypt each block sequentially. The initial vector and cipher image are transmitted to the decryption party via a public information channel. The decryption party uses the secret key and initial vector to decrypt the cipher image and retrieve the original image. Simulation results demonstrate that this image cryptosystem is both secure and high-speed, making it a suitable comparison benchmark for newly proposed image cryptosystems based on chaotic systems.

In [5] this paper author proposed an image encryption method using the XOR cipher to encrypt binary data in images pixel by pixel, rather than securing it with an application, making it harder to exploit or crack. The proposed method was tested in a Python environment, and the results showed that the images were properly encrypted using the XOR cipher. The model was tested on various images, including Mona Lisa, Apollo 11, and NebulaM83. Future work includes developing a random function with high entropy factors to enhance the encryption method.

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 7, July 2024

DOI: 10.17148/IJARCCE.2024.13717

In [6] this paper author proposed an advanced image cryptography algorithm that integrates encryption with steganography using MATLAB. This method utilizes the RC4 stream cipher combined with RGB pixel shuffling and steganography, specifically employing a hash-least significant bit (HLSB) technique. The HLSB method inserts data bits into the least significant bits of RGB pixels in the cover image, enhancing security. The system achieves a high level of security by generating multiple encryption patterns and applying them to the image blocks. The results indicate strong resistance to cryptographic attacks, as evidenced by the high peak signal-to-noise ratio (PSNR) and low mean square error (MSE) for both encrypted and original images.

In [7] this paper author introduced a novel image encryption algorithm based on vector quantization (VQ), cryptography, and number theory. This approach begins by decomposing an image into vectors, which are then sequentially encoded. Traditional cryptosystems from commercial applications are applied to these vectors to enhance security. Additionally, number theoretical methods are used to reduce the computational complexity of the encryption and decryption processes. VQ, known for its efficiency in low bit-rate image compression, speeds up the encryption process while maintaining high security, making it a practical solution for secure image encryption.

In [8] this paper author conducted a comprehensive review of different image encryption techniques. The paper provides an overview of various cryptographic methods and their applications in image encryption. It includes a comparative analysis of these techniques based on factors such as complexity, speed, memory usage, key types, key length, key space size, and security level. The study also highlights general security analysis methods for encrypted images, offering valuable insights into the effectiveness and efficiency of different encryption algorithms.

In [9] this paper author proposed a new approach for fast color image encryption utilizing chaotic maps. Their technique simplifies traditional preprocessing systems by employing basic operations like confusion and diffusion. The encryption process uses cascading of 3D standard and 3D cat maps to generate diffusion templates and shuffle RGB planes of the image. An XOR operation is then performed on the shuffled image and diffusion template to produce the encrypted image. The method is evaluated through theoretical analyses and simulations, demonstrating its effectiveness in minimizing brute-force attack possibilities and providing rapid encryption.

In [10] this paper author developed a new image cryptosystem based on chaotic maps and continued fractions. This system utilizes a chaotic map with a large key space in conjunction with the Engel Continued Fractions (ECF) map. The ECF-map is designed to produce a pseudo-random sequence with uniform distribution, zero correlation, and ideal nonlinearity, achieving a high level of security. The proposed scheme shows strong resistance to known attacks, and both theoretical and numerical simulations confirm its efficiency and high security.

In [11] this paper author introduced a framework for evaluating image encryption schemes based on various parameters. Their approach moves beyond visual inspections to use quantitative metrics such as correlation coefficient, information entropy, compression friendliness, pixel change rate, and unified average change intensity. The paper evaluates the security and efficiency of conventional encryption schemes like the Advanced Encryption Standard (AES) and Compression Friendly Encryption Scheme (CFES). The analysis reveals some weaknesses in CFES related to low entropy and horizontal correlation, highlighting areas for improvement in these encryption methods.

In [13] this paper author presented a survey on different techniques of image encryption. This paper reviews various image encryption methods, providing an overview of cryptography and its different types. The survey discusses the effectiveness and application of various encryption techniques, offering insights into their strengths and limitations. It serves as a comprehensive reference for understanding the landscape of image encryption technologies.

In [14] this paper author proposed a permutation-based image encryption technique. This method focuses on random pixel permutation to maintain image quality while using shared keys for encryption. The approach involves three types of classifications: position permutation, value permutation, and visual transformation. The technique aims to provide confidentiality for color images with minimal computational effort, demonstrating quick and effective encryption through the permutation process.

In [15] this paper author reviewed joint compression and encryption techniques for video data. Their paper discusses methods for combining compression and encryption to achieve fast and secure video transmission. Various algorithms are classified based on their efficiency and effectiveness in performing joint compression and encryption. The review provides valuable insights into optimizing video data security and transmission.

DOI: 10.17148/IJARCCE.2024.13717

In [16] this paper author conducted a survey on common encryption techniques. This paper explores different encryption methods, including basic cryptographic terms, key concepts, and classifications. It also focuses on image and information encryption techniques, analyzing their performance parameters and security issues. The survey offers a detailed examination of various encryption approaches and their applications.

In [17] this paper author introduced a new image encryption algorithm utilizing fuzzy integral permutation with coupled chaotic maps. This novel approach combines DNA addition with two-dimensional piecewise nonlinear chaotic maps to achieve strong permutation and diffusion properties. The proposed algorithm is designed to secure digital image information effectively, making it suitable for practical use in protecting image data over the Internet.

V. ANALYSIS

After analysis various research papers we compare the previous result and identify the good and flaws presented:

S. No	Approach	Information Entropy of Original Image	Information Entropy of Encrypted Image
1	Chaotic System [18]	Lena image 7.5534	7.9669
2	Chaotic System [18]	Circle image 6.0408	7.9652
3	Chaotic System [18]	Clock image 6.7057	7.9667
4	Key Based Partitioning [1]	Baboon 7.3186	6.9341
5	Key Based Partitioning [1]	Cameraman 7.0482	6.6863
6	Key Based Partitioning [1]	Football 7.2143	6.8731
7	Key Based Partitioning [1]	Lena 7.4578	6.8833
8	Block Based Transformation [19]	0.0063	5.4402

VI. PROBLEM DOMAIN

After reviewing several proposed techniques, we have identified the following issues:

1) There is a need for 3DES and MD5 algorithms for effective image encryption and decryption.

2) A larger key size is required to protect against brute force attacks.

3) A hybrid technique is necessary to enhance security.

4) All the previously discussed algorithms do not implement double encryption and decryption effectively.

5) The combination of XOR with another image in encryption is not utilized.

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 7, July 2024

DOI: 10.17148/IJARCCE.2024.13717

VII. CONCLUSION AND FUTURE WORK

There are numerous techniques to secure images. In today's digital landscape, where security is often compromised, protecting images over networks is crucial. This survey outlines various image encryption methods. We have reviewed different image encryption techniques from various research papers.

We conclude that while all these methods are effective for image encryption, each has its own set of advantages and disadvantages, providing a certain level of security to prevent unauthorized access to images in open networks. Each technique has its specific suitability and limitations, but there is still much work to be done in this area. Based on the study, we suggest the following future directions:

1) Implementing powerful encryption techniques like 3DES and MD5 can enhance security.

2) Using larger key sizes can improve image security and protect against brute force attacks.

3) Double key encryption can be explored to further enhance image security.

4) Implementing three-way security measures can strengthen encryption.

5) The encryption should require an extremely long computational time to break.

6) Pixel permutation combinations should be shuffled in a way that minimizes information loss.

REFERENCES

[1]. Nooka Saikumar R. Bala Krishnan, S.Meganathan N.R. Raajan "An Encryption Approach for Security Enhancement in Images using Key Based Partitioning Technique" International Conference on Circuit, Power and Computing Technologies [ICCPCT] IEEE 2016.

[2]. Ravi Shanker Yadav, Mhd. Rizwan Beg, Manish Madhava Tripathi, "Image encryption technique: A critical comparison", International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR) ISSN 2249-68, Vol. 3, Issue 1, Mar 2013, 67-74.

[3]. Alireza Jolfaei, Abdolrasoul Mirghadri, "Survey: Image Encryption Using Salsa20", IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 5, September 2010 ISSN (Online): 1694-0814.

[4]. Yong Zhang, Xueqian Li, Wengang Hou, "A Fast Image Encryption Scheme Based on AES" 2nd International Conference on Image, Vision and Computing 2017 IEEE.

[5]. Arul Thileeban S, "Encryption of images using XOR Cipher" International Conference on Computational Intelligence and Computing Research 2016 IEEE.

[6]. May H.Abood "An Efficient Image Cryptography using Hash-LSB Steganography with RC4 and Pixel Shuffling Encryption Algorithms" Annual Conference on New Trends in Information & Communications Technology Applications-(NTICT'2017) 7 - 9 March 2017 IEEE.

[7]. Chin-Chen Chang, Min-Shian Hwang, TungShou Chen, "A new encryption algorithm for image cryptosystems", The Journal of Systems and Software 58 (2001), 83-91.

[8]. Parameshachari B D, K M Sunjiv Soyjaudah, Chaitanyakumar M V, "A Study on Different Techniques for Security of an Image", International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-1, Issue-6, January 2013.

[9]. Kamlesh Gupta, Sanjay Silakari, "New Approach for Fast Color Image Encryption Using Chaotic Map", Journal of Information Security, 2011, 2, 139-150 Doi:10.4236/jis.2011.24014 Published Online October 2011 (http://www.SciRP.org/journal/jis).

[10]. A.Masmoudi, M.S. Bouhlel, and W. Puech, "A new image cryptosystem based on chaotic map and continued fractions", 18th European signal processing conference (EUSIPCO-2010), Aaborg, Denmark, August 23-27,2010, ISSN 2076-1465.

[11]. Jawad Ahmad, Fawad Ahmed, "Efficiency Analysis and Security Evaluation of Image Encryption Schemes", International Journal of Video & Image Processing and Network Security IJVIPNS-IJENS Vol: 12 No: 04, 2012.

[12]. Komal D Patel, Sonal Belani, "Image Encryption Using Different Techniques: A Review", International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, Volume 1, Issue 1, November 2011)

[13]. Abhinav Srivastava, "A survey report on Different Techniques of Image Encryption", International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 6 June 2012).

DOI: 10.17148/IJARCCE.2024.13717

[14]. Sesha Pallavi Indrakanti and P.S.Avadhani, "Permutation based Image Encryption Technique", International Journal of Computer Applications (0975 – 8887) Volume 28– No.8, August 2011.

[15]. K. John Singh and R. Manimegalai, "A Survey on Joint Compression and Encryption Techniques for Video Data", Journal of Computer Science 8 (5): 731-736, 2012 ISSN 1549-3636 © 2012 Science Publications.

[16]. E. Thambiraja, G. Ramesh and Dr. R. Umarani, "A Survey on Various Most Common Encryption Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 7, July 2012 ISSN: 2277 128X.

[17]. Yasaman Hashemi, "Design a new image encryption using fuzzy integral permutation with coupled chaotic maps", International Journal of Research in Computer Science eISSN 2249-8265 Volume 3 Issue 1 (2013) pp. 27-34 www.ijorcs.org, A Unit of White Globe Publications doi: 10.7815/ijorcs. 31.2013.058.

[18]. Long Bao, Yicong Zhou,C. L. Philip Chen, "A New Chaotic System for Image Encryption", 2012 International Conference on System Science and Engineering June 30-July 2, 2012, Dalian, China IEEE.

[19]. Mohammad Ali Bani Younes and Aman Jantan, "Image Encryption Using Block-Based Transformation Algorithm", IAENG International Journal of Computer Science, 2008 35:1, IJCS_35_1_03.