IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

# A REVIEW ON VARIOUS IMAGE ENCRYPTION TECHNIQUE AND CHALLENGES IN THE CURRENT SCENARIO

[1]Hariom Singh, [2]Prof. Chetan Gupta, [3]Dr. Ritu Shrivastava

[1]M. Tech. Research Scholar, [2]Assistant Professor, [3]Professor

[1]Department of CSE,

[1]SIRTS, Bhopal, India

***Abstract:*** The fundamental issue in the current communication environment is the security of information or data. The method for encrypting images should be designed to increase transmission effectiveness while also limiting unauthorized access to data. Image encryption is used in commerce, the medical field, and the military and multimedia systems. Decryption is the process of turning encrypted data back to plain text. Encryption is the process of converting plain text into cypher text. Cryptography consists of encryption and decryption methods. In this piece, we've covered the many names for encryption as well as the function and types of cryptography.

***Index Terms*-Encryption, Data Encryption Standard, integrity, authenticity, cryptography.**

## I.INTRODUCTION

Data integrity and security have become serious issues in recent years. Today, practically all data is sent across computer networks, making it vulnerable to many types of assaults. We must encrypt data before sending it from sender to recipient using any technique in order to shield it from threats. An algorithm or mathematical function is used to alter the data during the encryption process so that only the intended receiver, who has access to the private key, can decipher it. The necessity to preserve our data is of the utmost importance in today's society due to the quick growth of electronic communication [1].Moving data over communication networks requires the utmost data protection. [2][3]. This problem is addressed by a variety of techniques that protect data against unauthorized access while it is being sent. [4][6][6]. The aforementioned issue can be handled by employing data encryption methods including cryptography, watermarking, and steganography. Steganography is a technique for hiding data in images, whereas cryptography is the process of encrypting and decrypting data in order to keep it safe from unauthorized access. DES, AES, and IDEA are a few algorithms that are employed to stop unauthorized access to data. [7] [8] [8] [10][11].

In its early years, we witnessed a quick advancement in every facet of life. In the last two decades, social media and the communication industry underwent a transformation. The way we interact and communicate with one another has been fundamentally transformed by the internet. We have to deal with digital photos in many of the online programmers we use on a daily basis, such as Facebook, WhatsApp, video conferencing, Skype, etc. Some critical institutions, such as the military image database and the medical imaging system, employ digital picture transmission as well. Researchers evaluate, identify, and solve issues in the actual world using image-based data.

With the use of modern technology, we may convert an original image into a more cryptic format. Data security has become a serious worry with the rise in popularity of multimedia apps that integrate text, music, video animation, and photographs. Several methods, including data concealment and encryption, are available to overcome this. No one can access the data without a decryption key. [1][2][3].Since compression uses less disc space (saving money) and enables more data to be delivered over the internet, it is employed to safeguard data from unauthorized access. It is a method of converting or encoding a photograph so that it uses a small portion of the original file's space. It is a technique for getting rid of extra information from an image without sacrificing its quality. It accelerates the rate at which data is transferred from the disc to memory.

Typically, a picture is made up of a number of pixels. Image encryption is a process that turns an image into encrypted text in its most basic form. Different digital services demand reliable security while moving pictures from one place to another. Image encryption will be necessary for next multimedia Internet apps. Image encryption can also safeguard data privacy. Images are often transferred between two parties across unprotected networks.

The three basic goals of photo encryption are to ensure the authenticity, secrecy, and integrity of image data [4][5]. Given the rapid increase of electronic data sharing, it is essential to safeguard photographic data against unauthorized access. A breach in security might harm users' reputations and privacy. As a result, data encryption is commonly employed to preserve security on open networks like the internet. The aforementioned issue may be overcome by utilizing data encryption techniques including cryptography, watermarking, and steganography.

Cryptography, on the other hand, is the process of encrypting and decrypting data to keep it safe from unauthorised access. Steganography is the technique for hiding information in images. DES, AES, and IDEA are a few of the algorithms used to guard against unauthorized access to data. Image encryption is crucial for data concealment, and these methods are useful for delivering data over the internet in real-time since they can withstand brute force and differential assaults [6].In block cypher systems like Advanced Encryption Standard (AES) and Data Encryption Standard, an S-box is a vital module that significantly contributes to confusion and dispersion (DES). A nonlinear map S: 0; 1n; 0; 1n, where 0; 1n denotes the vector spaces of n elements from GF, is known as a n n S-box (2)

The security protection of picture data is an important and active area of study due to the fast growth of computers and the Internet, which has drawn considerable interest from academics and business. Researchers have created a variety of approaches to ensure the security of photos, including image encryption [1-3], watermarking [4,5], and data concealment [6,7], with image encryption being the most straightforward and efficient approach.

### ENCRYPTION ALGORITHMS

**1. Triple DES:**Triple-DES is a technique for encrypting images, text, or videos using either 56-bit two-keys or 128-bit keys. This approach is thought to be the most secure when compared to other algorithms. Triple DES offers a relatively simple way to increase the key size of DES to thwart such attacks without having to develop a completely new block cypher algorithm. For a 192-bit key length, three 64-bit keys are needed. Triple DES is three times slower than regular DES, but it is far more secure when used properly.

**2. RSA:** Leonard Adleman, Adi Shamir, and Ron Rivest created the RSA algorithm in 1977. Data transit security frequently uses the RSA algorithm, one of the earliest public key cryptosystems. Due to the fact that RSA requires two keys for encryption and decoding, it is categorized as an asymmetric key algorithm [26][27]. Factoring is challenging because of the product of two large prime numbers. The RSA encryption algorithm is used to encrypt the original picture, and other keys are required to decode it.

**3. Blowfish:** In 1993, Bruce Schneier created Blowfish as a quick and affordable alternative to the then-current encryption techniques. This system was designed to take the role of the Des algorithm. It is suitable and efficient for hardware implementation, and as it is in the public domain and free to use, no license is necessary [28][14]. The F-function, which is utilized in Blowfish, was developed to simplify the DES ideas. A cypher based on Feistel rounds is called blowfish.

**4. AES:**AES-128, AES-192, and AES-256 are the three distinct iterations of the AES algorithm. The degree of security is determined by the size of the key, and as the key size increases, the degree of security increases as well. Alternative algorithms that depend on different parameters are contrasted with the AES approach, which is notably more secure. the four separate byte-oriented modifications that make up the round function of the AES algorithm. Because AES's round transformation is parallel by design, it can be executed on specialised hardware much faster. According to one study, AES delivers encryption that is error-free and significantly less error-prone even when subjected to satellite radiation. Cipher Feedback always use the AES algorithm, one of the best encryption and decryption methods available today.

### IMAGE SECURITY PARAMETERS

The image is the most widely used method of communication in a range of industries, including the military, business, and scientific disciplines. The security of digital image/video has taken on more significance in applications in the highly networked and computerised world of today. Security systems now use steganography, encryption, or a combination of the two. Some techniques for protecting images include steganography, cryptography, reversible watermarking, digital watermarking, and encryption. The security of digital images on a shared communication channel is a crucial but challenging topic.

## I.LITERATURE SURVEY

The data in images are secured using the image encryption approach. The review of various encryption methods utilized is presented in this section.

Digital photo security has recently attracted a lot of attention. In this study [1], we provide a novel three-layered picture encryption and decryption method that encrypts and decodes multiple pictures of various dimensions using the Genetic Algorithm (GA) and certain inherent features of the Residue Number System (RNS). The extremely big key space in this new proposed GARN system is built at different stages of the programmer. The proposed method was evaluated on many picture types, and the simulated results show that it can survive cryptographic attacks, has a high throughput rate, and the simulated output is chaotic enough to find any underlying pattern. This method's minimal power use is a result of the residual bits that were employed.

The recommended approach is based on the transformation of pixel values. In this study, author [2] devised an effective method for encoding digital colourphotographs using the Key Pattern encoding technique. This study demonstrates how effective this technique is for data security applications. The approach of inspecting neighboring pixels shows the efficacy of the hybrid technique.

According to the encryption method proposed in this work [3], which is based on the XOR Cipher, the binary data of images is encrypted on each pixel. There are several methods for encrypting the image in this methodology, illustrating the value of the suggested method and proving that the suggested model effectively does so. They also suggested that in the future, to protect us from brute forcing, we add a random algorithm that generates a more complex combination of encrypted images.

The author of the study offered an AES-based picture encryption system [4]. This method provides a rapid photo encryption method that utilises the AES algorithm for both encryption and decryption operations. In this system, the look-up table approach is used to do the AES, while the chaotic method is used to construct the initial vector (IV). Since AES is a safe approach, the image cryptosystem that has been reviewed is secure. Experimental results show that chaotic image cryptosystems are also slower than AES image cryptosystems. This demonstrates the potency of the recommended strategy.

This article [5] examines all encryption and decryption algorithms, including DES, 2DES, 3DES, and additional substitution schemes. According to the analysis, the DES algorithm is the most effective in terms of speed. They also suggested that the security offered by this method may be improved by applying multiple algorithms to the data.

The study's author [14] suggested an efficient key-based pattern encoding technique for digital colour pictures that employs an adaptive key-based block selection algorithm to track pixel value reordering. The suggested approach can fend off several cryptographic assaults. A number of pixel reordering patterns have been created and applied to a single image after it has been separated into blocks. The Key (Secret) determines the encryption scheme for the partitioned picture block, resulting in the final encrypted image. By using the pixel value reordering approach to the linked blocks of the image, the image may be reformatted into its parental form while maintaining the same key and pattern.The main benefits of the recommended technique are lossless decomposition, effectiveness, and simplicity. The experimental findings show the effectiveness of the proposed method, which is immune to the most prevalent cypher attacks currently in use.

This paper [15] offers an image encryption survey using Salsa20 and evaluates a number of image encryption algorithms based on several parameters. They provide a cutting-edge method of image security. They carry out a number of experiments to show how well salsa20's photo encryption works. Visual testing, key space analysis, histogram analysis, information entropy calculation, correlation analysis factor, differential analysis method, sensitivity analysis parameter, and performance analysis parameter are a few examples of the techniques used. An experiment demonstrates the effectiveness of the Salsa20 algorithm for picture encryption. Additionally, they recommended using methods with a large key space to encrypt complicated images in order to improve data security and secure communication over insecure networks.

An image cryptosystem built on the AES algorithm was developed by the paper's author [16]. The picture is initially broken up into tiny 128-bit data bits. In this work, CBC mode of AES was used for photo encryption. A beginning vector is created by first permuting the image. The next step is to gradually encrypt each block using AES in a cypher block chaining fashion. The first vector and cypher image are sent via the public channel. The secret key and starting vector are used to decrypt the cypher image in order to recover the original image. Operational statistics demonstrate the security and speed of the proposed cryptosystem. This proves the superiority of the proposed image cryptosystems over earlier work based on chaotic systems.

## III.PROBLEM DOMAIN

Double encryption and decryption-based techniques currently in use are inoperable [1]. This is where algorithms like DES, RSA, and others come in. As a consequence, the algorithm will be able to protect the photographs or data more effectively [2].
To encrypt and decode images, the DES and RSA algorithms must be employed. Additionally, it is possible to use the DES and RSA algorithms, which allow for an increase in key space size and make brute force attacks less effective [3].
A large key with strong random sensitivity is required for key creation [4].
For the loss of information to be as small as possible, entropy should be in equilibrium states [5].
Color histograms with logical key spaces are supported by the algorithm [6].

## IV.CONCLUSION AND FUTURE WORK

In this paper, existing studies on encryption algorithms including AES, 3DES, Blowfish, and DES has been examined. Cryptography is a means for secure communication. DES key size is too little in contrast to other methods. A sluggish and ineffective block cypher is 3DES. AES is considered to be preferable than the original Blowfish algorithm. The pixels next to each other in a picture are around the same size. A relationship cannot be erased by the AES algorithm. Aside from the security issue, employing these cyphers directly to encrypt images takes a long time and is not suitable for real-time applications. To deal with these problems, a modified advanced encryption Standard technique is proposed. The performance and security of this update may both be enhanced.

## V.REFERENCES

[1] P. A. -N. Agbedemnab, E. Y. Baagyere and M. I. Daabo, "A New Image Encryption and Decryption Technique using Genetic Algorithm and Residual Numbers," 2019 IEEE AFRICON, 2019, pp. 1-9, doi: 10.1109/AFRICON46755.2019.9133919.

[2] NookaSaikumar 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.

[3] Arul Thileeban S, “Encryption of images using XOR Cipher” International Conference on Computational Intelligence and Computing Research 2016 IEEE

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

[5] Yashwantkumar, Rajatjoshi, Tameshwarmandavi, Simranbharti, Miss RoshniRathour, "Enhancing the Security of Data Using DES Algorithm along with Substitution Technique". International Journal Of Engineering And Computer Science ISSN: 2319-7242 Volume 5 Issue 10, Page No. 18395-18398, Oct. 2016

[6] Zhou C, Guo Y, Huang W, et al. Information security defense method of electric power control system based on digital watermark[C], International Conferenceon Materials Engineering, Manufacturing Technology and Control. 2016

[7] E. Chisanga, E.K. Ngassam, Towards a conceptual framework for information security digital divide[C]// Ist-Africa week conference. IEEE, 1–8 (2017).

[8] T. Caulfield, C. Ioannidis, D. Pym, Discrete Choice, Social Interaction, and Policy in Encryption Technology Adoption (Short Paper). In International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg (2016), pp. 271-279

[9] Z. Cai, D. Huang, Research on DES Data Encryption Technology in Network Information Security [J]. Computer Measurement & Control. 25, 241-247 (2017)

[10] Sun Y Q, Wang X H. Information encryption technology with strong robustness based on QR code and matrix mapping [J]. Packaging Engineering. 38, 194-199 (2017)

[11] X. Liao, J. Yin, S. Guo, X. Li, and A. K. Sangaiah, "Medical JPEG image steganography based on preserving inter-block dependencies," Comput. Electr. Eng., Vol. 67, pp. 320–329, 2018.

[12] M. A. Usman, S. M. Ieee, M. R. Usman, and S. M. Ieee, "Using Image Steganography for Providing Enhanced Medical Data security," In 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC), 2018.

[13] A. Banu S and R. Amirtharajan, "A robust medical image encryption in dual domain: chaos-DNA-IWT combined approach," Medical & Biological Engineering & Computing, vol. 58, no. 7, pp. 1445–1458, 2020.

[14] NookaSaikumar 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.

[15] AlirezaJolfaei, AbdolrasoulMirghadri, "Survey: Image Encryption Using Salsa20", IJCSI, International Journal of Computer Science Issues, Vol. 7, Issue 5, ISSN (Online): 1694-0814, September 2010.

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

[17] X. Wang and C. Liu, "A novel and effective image encryption algorithm based on chaos and DNA encoding," Multimedia Tools and Applications, vol. 76, no. 5, pp. 6229–6245, 2017.

[18] S. Kumar, B. Panna, and R. Kumar, "Medical image encryption using fractional discrete cosine transform with chaotic function," Medical & Biological Engineering & Computing, vol. 57, no. 11, pp. 2517–2533, 2019.

[19] Abd-El-Latif, A.A.; Abd-El-Atty, B.; Venegas-Andraca, S.E.; Mazurczyk, W. providing end-to-end security using quantum walksin IoT networks. IEEE Access 2020, 8, 92687–92696.

[20] Wang, X.; Zhao, D. A special attack on the asymmetric cryptosystem based on phase-truncated Fourier transforms. Opt. Commun.2012, 285, 1078–1081.