IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Survey on Various Image Encryption Technique and challenges

Akansha Dongre[1], Prof. Chetan Gupta[2], Sonam Dubey[3]
M. Tech. Scholar, Department of CSE, SIRTS, Bhopal, India[1], Assistant Professor, Department of CSE, SIRT, Bhopal, India[2],
Assistant Professor, Department of CSE, SIRT, Bhopal, India[3]

Abstract

The security of information, or data, in today's communication environment is the most significant problem. The image encryption approach should be constructed in such a manner that it improves the efficacy of communication while also keeping data safe from unwanted access. The business world, health care, military activities, and multimedia systems all use image encryption. Encryption is the process of converting plain text into cipher text, whereas decryption is the act of converting cipher text back to plain text. Encryption and decryption techniques make up cryptography. We have discussed the different encryption terminology, the purpose of cryptography, and its kinds in this article.

Keywords: Encryption, Data Encryption Standard, integrity, authenticity, cryptography.

I. Introduction

The security and integrity of data has been a major concern in recent years. In today's world, practically all data is sent across computer networks, making it exposed to many types of assaults. To safeguard data from various threats, we should encrypt it before broadcasting it via any means from sender to recipient. The encryption procedure involves altering data using an algorithm or a mathematical function to render it unintelligible to everybody save the intended receiver who has access to the private key. In today's society, electronic communication is growing at a breakneck speed, making the necessity to secure our data the most pressing concern [1]. When transferring data across communication networks, data security is a must [2][3]. To address this issue, many techniques are employed to protect data from unauthorized access during transmission [4][6][6]. The aforementioned challenge can be solved by employing data encryption techniques such as cryptography, watermarking, and steganography. Cryptography is the process of encrypting and decrypting data to safeguard it from unwanted access, whereas Steganography is the process of hiding information in images. DES, AES, and IDEA is some of the algorithms that are used to protect data from unauthorized access. [7][8][8][10][11].

Image encryption is a technology that allows us to turn an original image into a more difficult-to-understand format. With the growing use of multimedia applications that combine text, music, video animation, and photos, data security has become a major concern. To address this, several techniques such as encryption and data concealing are available. Without a decryption key, no one can view the material. [1][2][3]. Compression is used to protect data from unwanted access since it utilizes less disc space (saving money) and allows for more data to be transferred over the internet. It is the technique of encoding or transforming a picture such that it takes up a fraction of the space of the original file. It is a method of removing unneeded data from an image without affecting its quality. It improves the speed of data transmission from disc to memory.

Normally, an image is a collection of pixels. In its most basic form, Image Encryption is a mechanism for converting an image into cipher text. Various digital services require trustworthy security in picture transfer from one end to the other. Future multimedia Internet applications will require image encryption. Data privacy can also be protected with image encryption. Over unsecured networks, images are often shared between two parties.

The basic goal of picture encryption is to secure image data's authenticity, secrecy, and integrity [4][5]. With the rapid advancement of electronic data sharing, it is critical to secure the security of picture data against unwanted access. Users' privacy and reputation may be harmed as a result of security breaches. As a result, data encryption is commonly employed in open networks like the internet to ensure security. The aforementioned challenge can be solved by employing data encryption techniques such as cryptography, watermarking, and steganography.

Cryptography is the process of encrypting and decrypting data to safeguard it from unwanted access, whereas Steganography is the process of hiding information in images. DES, AES, and IDEA are some of the algorithms that are used to protect data from unauthorized access. Image encryption plays a significant part in data concealment, and these algorithms are also capable of defending against brute force and differential assaults, indicating its real-time applications while delivering data over the internet [6].

Encryption Algorithms

1. Triple DES: The method of encrypting a picture, text, or video utilising 56 bit two keys or 128 bit keys is known as Triple-DES. In comparison to other algorithms, this method is regarded to be the most secure. Without having to create a whole new block cypher algorithm, Triple DES gives a reasonably easy means of boosting the key size of DES to guard against such assaults. Three 64-bit keys are required for a total key length of 192 bits. Triple DES is three times slower than ordinary DES, but when implemented correctly, it is substantially more secure.

2. RSA: Ron Rivest, Adi Shamir, and Leonard Adleman created the RSA algorithm in 1977. One of the first public key cryptosystems, the RSA algorithm is frequently used to protect data transfer. Because it requires two keys for encryption and decryption, RSA is classified as an asymmetric key algorithm [26][27]. The factoring issue is based on the product of two huge prime integers. The RSA technique encrypts the original picture and uses various keys to decode it.

3. Blowfish: Blowfish was created by Bruce Schneier in 1993 as a quick and free alternative to existing encryption techniques. It was created to take the place of the Des algorithm. It is appropriate and efficient for hardware implementation, and there is no need for a licence, which implies that anybody can use it because it is freely accessible in the public domain [28][14]. Blowfish is a cypher based on Feistel rounds, and the F-function utilised was designed to simplify the ideas used in DES.

4. AES: AES algorithm is of three types i.e. AES-128, AES-192 and AES-256. The size of the key defines the amount of security; as the key size grows, so does the level of security. When compared to other algorithms based on various parameters, the AES method is far more safe. The round function used by the AES algorithm is made up of four separate byte-oriented changes. Because the round transformation is parallel by design, AES provides for much quicker execution on dedicated hardware. AES provides an error-free encryption scheme, according to some research, and error is greatly minimised even in satellite radiation. The AES algorithm is always used in Cipher Feedback mode, and its effective implementation is one of the finest encryption and decryption standards currently available.

Image Security Parameters

The picture is the most extensively utilized communication form in a variety of fields, including medicine, research, industry, and the military. The security of digital image/video has become more important in applications in today's highly computerized and networked world. Currently, security frameworks rely on encryption, steganography, or a mix of the two. Encryption, watermarking, digital watermarking, reversible watermarking, cryptography, and steganography are some of the methods used to safeguard photographs. On a shared communication channel, the security of digital pictures is a critical but difficult challenge. The following are some of the most frequent Image Security Parameters:

1. Large key space
2. Uniform Image histogram
3. Information entropy
4. Correlation analyses

II. Literature Survey

The image encryption technique is used for securing the data in image. This section presents the review of various encryption techniques that are being used.

The security of digital photographs has recently received a lot of attention. In this research [1] , we offer a unique three-layered picture encryption and decryption technique that uses the Genetic Algorithm (GA) and certain intrinsic aspects of the Residue Number System to encrypt and decode various images of various dimensions (RNS). This new suggested GARN system features a very large key space that is constructed at various stages of the scheme. The suggested system was tested on a variety of pictures, and the simulated results demonstrate that it can withstand cryptographic assaults, has a high throughput rate, and the simulated output is chaotic enough to discover any underlying pattern. The power consumption of this approach is also negligible due to the residual bits used.
The suggested method is based on pixels value transformation. Author [2] developed an efficient solution for digital color pictures based on Key Pattern encoding scheme in this paper. This study shows that this method is superior for data security applications. The hybrid technique's effectiveness is demonstrated by the strategy of examining nearby pixels.

The author of this study presented [4] a system for picture encryption based on the AES algorithm. This method proposes a fast picture encryption method that use the AES algorithm to accomplish both encryption and decryption operations. The chaotic technique is used to produce the initial vector (IV) in this system, and the look-up table approach is used to perform AES. Because AES is a safe technique, the image cryptosystem that has been tested is secure. Furthermore, experimental results show that chaotic image cryptosystems are slower than AES image cryptosystems. This demonstrates the efficacy of the recommended strategy.

The binary data of pictures is encrypted on each pixel in this encryption approach, which is based on the XOR Cipher, as suggested in this study [3]. There are several approaches to encrypting the picture in this technique, demonstrating the usefulness of the provided approach and demonstrating that the proposed model encrypts the image appropriately. They also proposed that in the future, we include a random algorithm that creates a more complicated combination of encrypted images, which will protect us from brute forcing.

The examination of all encryption and decryption methods such as DES, 2DES, 3DES, and other substitution techniques is done in this article [5]. The DES algorithm is the most efficient in terms of speed, according to study. They also indicated that by applying more than one algorithm to data, the security provided by this approach might be enhanced.

The author of this study [18] suggested an efficient Key based Pattern encoding system for digital colour pictures that ses an adaptive key based block selection algorithm to follow pixel value reordering manner. The suggested technique is resistant to a wide range of cryptographic assaults. Multiple pixel reordering patterns have been created and applied to a single image once the image has een partitioned into blocks. The Key (Secret) determines the encrypting pattern on the partitioned image block, resulting in a final encrypted picture. With the use of the same key and pattern, the picture may be reformatted into its parental form by applying the pixel value reordering technique to the image's related blocks. Lossless decomposition, efficiency, and simplicity are the primary advantages of the suggested approach. The experimental results demonstrate the efficacy of the suggested approach, which is resistant to the most common cipher assaults currently in use.

In this study [19], numerous types of image encryption schemes are compared based on various parameters, and an image encryption survey using Salsa20 is presented. They propose a novel approach to picture protection. They do this by doing a number of tests to prove salsa20's image encryption efficacy. Visual testing, key space analysis, histogram analysis, information entropy calculation, encryption quality factor, correlation analysis factor, differential analysis method, sensitivity analysis parameter, and performance analysis parameter are some of the techniques used. The Salsa20 algorithm for picture encryption is shown to be successful in an experiment.
They also recommended using big key space techniques to encrypt images with high complexity, which would result in more secure data and increase secure communication across an insecure network.

The author of this paper [20] created an image cryptosystem based on the AES algorithm. To begin, the image is divided into little 128-bit data chunks. For picture encryption, AES was utilized in CBC mode in this study. The picture is first permuted into a starting vector. After that, AES is utilized in a cipher block chaining manner to encrypt each block progressively. The public channel is used to send the initial vector and cipher image. To restore the original picture, the secret key and beginning vector are utilized to decrypt the cipher image. The suggested cryptosystem is both secure and fast, according to operational data. This demonstrates that the suggested picture cryptosystems are superior to prior work based on chaotic systems.

III. PROBLEM DOMAIN

After study of several proposed technique we can come with some problem which are following:

1. There is the need of 3DES, MD5 algorithms which can be used for image encryption and decryption.
2. Large Key size is needed to protect from bruit force attack.
3. There will be need of hybrid technique to improve the security.
4. All the above discussed algorithms fail to work on the basis of double encryption and decryption.
5. The combination of XOR with another image in encryption is not use.
6. No use of 3 way hybrid encryption technique to improve the security.
7. Proper pixel shuffling of RGB is not done in efficient manner.

IV. CONCLUSION AND FUTURE WORK

Cryptography is a mechanism for secure communication, and in this study, existing research on encryption algorithms such as AES, 3DES, Blowfish, and DES has been reviewed. In comparison to other approaches, DES key size is too tiny. 3DES is a slow and inefficient block cipher. When compared to the original Blowfish algorithm, AES is thought to be a better option. In a photograph, the neighboring pixels are of similar size. AES algorithm cannot delete a relationship. Apart from the security concern, directly encrypting pictures using these ciphers takes a long time and is not suited for real-time applications. A modified advanced encryption Standard approach is presented to address these issues. This update has the potential to improve security as well as performance.

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] 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.

[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, Wengang Hou, "A Fast Image Encryption Scheme Based on AES" 2nd International Conference on Image, Vision and Computing 2017 IEEE.

[5] Yashwant kumar, Rajat joshi, Tameshwar mandavi, Simran bharti, Miss Roshni Rathour, "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] Shrija Somaraj , Mohammed Ali Hussain "A Novel Image Encryption Technique Using RGB Pixel Displacement for Color Images" 6th International Conference on Advanced Computing (IACC) DOI: 10.1109/IACC.2016.59, Pages: 275 – 279, IEEE 27-28 Feb. 2016.

[7] A.D. Senthil Kumar, T.S. Anandhi "Multi image integration and Encryption Algorithm for security applications" IECON 2016 - 42nd Annual Conference of the IEEE Industrial Electronics Society, DOI: 10.1109/IECON.2016.7793265, Pages: 986 – 991, 23-26 Oct. 2016.

[8] Ramkrishna Das ; Sarbajit Manna ; Saurabh Dutta "Cumulative Image Encryption Approach Based On User Defined Operation, Character Repositioning, Text Key and Image Key Encryption Technique And Secret Sharing Scheme" International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), Pages: 748 – 753, IEEE 21-22 Sept. 2017.

[9] HibaAbdel-Nabi, "Medical Imaging Security Using Partial Encryption and Histogram Shifting Watermarking" International Conference on Information Technology (ICIT), Pages: 802 – 807, 17-18 May 2017.

[10] A.D. Senthil Kumar "Multi Image Integration and Encryption Algorithm for Security Applications", 42nd Annual Conference of the IEEE Industrial Electronics Society (IECON), Pages: 986 – 991, IEEE, 23-26 Oct. 2016.

[11] Y Manjula, "Enhanced Secure Image Steganography Using Double Encryption Algorithms" International Conference on Computing for Sustainable Global Development, IEEE Pages: 705 – 708 16-18 March 2016.

[12] Yinhui Zhang, "Digital Image Encryption And Decryption Algorithm Based On Wavelet Transform and Chaos System" Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), Pages: 253 – 257, IEEE 3-5 Oct. 2016.

[13] B Karthikeyan, Abhilash Choudary Kosaraju and Sudeep Gupta S, "Enhanced Security in Steganography using Encryption and Quick Response code" International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Pages: 2308 – 2312, IEEE 2016.

[14] Sharafat Hossain, Masud An Nur Islam Fahim "A Simple Way of Image Encryption Using Pixel Shuffling and Pixel Manipulation" International Conference of Computer and Information Technology (ICCIT), Pages: 1 – 4, IEEE 22-24 Dec. 2017.

[15] M. Kar, M. K. Mandal ; D. Nandi, "RGB Image Encryption Using Hyper Chaotic System" International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN), Pages: 354 – 359, IEEE, 3-5 Nov. 2017.

[16] Andrei Duluta, Stefan Mocanu "Secure Communication Method Based on Encryption and Steganography" International Conference on Control Systems and Computer Science (CSCS), Pages: 453 – 458, IEEE 2017

[17] K.S. Seethalakshmi, Usha B A; Sangeetha K N "Security Enhancement in Image Steganography Using Neural Networks and Visual Cryptography" International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS) IEEE, Pages: 396 – 403, 2016.

[18] 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.

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

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