A Review: On Various Image Encryption with Two Way Encryption Technique using DES Algorithm and Random Password

Ritesh Shivhare
M.Tech. Research Scholar, Department of CSE
riteshshivhare21051989@gmail.com
SIRTS BHOPAL

Dr. Ritu Shrivastava
Associate Prof., Department of CSE
ritushrivastava08@gmail.com
SIRTS BHOPAL

Prof. Chetan Gupta
Assistant Prof., Department of CSE
chetangupta.gupta1@gmail.com
SIRTS BHOPAL

Abstract — **A secure environment would not be possible without the existence of encryption technology. Image covers a large percentage of the multimedia data and its protection is very important in the current scenario. It becomes a critical issue that how we can protect our data. The term encryption refers that a piece of information is encoded in such a way that it can only be decoded, read and understood by people for whom it was meant and protect it from attackers who want to access the information in unauthorized way by breaking the security. Encryption is the process in which the data is passed through a series of mathematical operations that generate an alternate form of that data. We called the sequence of these mathematical operations as an algorithm. In This paper we have done survey on various research papers reviewed various encryption techniques that exist, based on our survey we also discuss two way encryption for better analysis with data encryption standard (DES) encryption.**

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

I. INTRODUCTION

Image encryption is a technique in which we can convert original image to another form which is difficult to understand by converting them. The ever-increasing growth of multimedia applications, security is an important issue in communication and storage of images. Encryption is one of the ways to ensure security. Nobody can access the content without a key for decryption. [1]. Images are generally the collection of pixels. Basically Image Encryption means that convert the image into unreadable format. Many digital services require reliable security in storage and transmission of digital images. Due to the rapid growth of the internet in the digital world today, the security of digital images has become more important and attracted much attention. The prevalence of multimedia technology in our society has promoted digital images to play a more significant role than the traditional texts, which demand serious protection of user's privacy for all applications. Encryption techniques of digital images are very important and should be used to frustrate opponent attacks from unauthorized access [2]. Along with the fast progression of data exchange in electronic way, it is important to protect the confidentiality of image data from unauthorized access. Security breaches may affect user's privacy and reputation. So, data encryption is widely used to confirm security in open networks such as the internet. Due to the substantial increase in digital data transmission via public channels, the security of digital images has become more prominent and attracted much attention in the digital world today. The extension of multimedia technology in our society has promoted digital images to play a more significant role than the traditional texts, which demand serious protection of users' privacy for all applications. Each type of data has its own features; therefore, different techniques should be used to protect confidential image data from unauthorized access. Most of the available encryption algorithms are used for text data. However, due to large data size and real time requirement, it is not reasonable to use traditional encryption methods [3].

II. TYPES OF CRYPTOGRAPHY:

Cryptography technique is used when secret message are transferred from one party to another over a communication line. Cryptography technique needs some algorithm for encryption of data. Nowadays when more and more sensitive information is stored on computers and transmitted over the Internet, we need to ensure information security and safety. Image is also an important part of our information .Therefore it's very important to protect our image from unauthorized access. There are so many algorithms available to protect image from unauthorized access.

Secret key cryptography: Secret key cryptography is also known as symmetric key cryptography. With this type of cryptography, both the sender and the receiver know the same secret code, called the key. Messages are encrypted by the sender using the key and decrypted by the receiver using the same key.

Public key cryptography: Public key cryptography, also called asymmetric key cryptography, uses a pair of keys for encryption and decryption. With public key cryptography, keys work in pairs of matched public and private keys [12].

Figure1. is showing about Image encryption scheme.

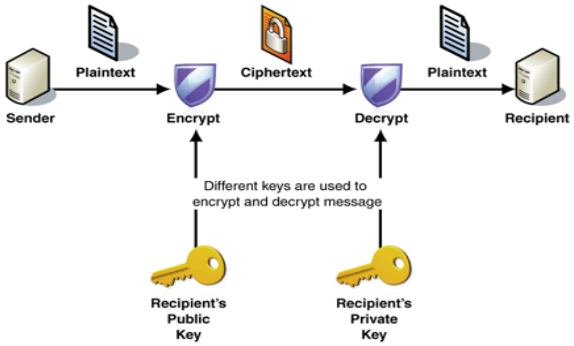

Figure 1: Image Encryption Scheme

III. CHARACTERISTICS OF IMAGE ENCRYPTION:

The image security requires the following characteristics-

1. The encryption system should be computationally secure. It must require an extremely long computational time to break.
2. The encryption and decryption algorithm must be simple and fast.

3. The security mechanism should be flexible.
4. There should not be a large expansion of the encrypted image data.
5. The security mechanism should be as widespread as possible. It must be widely acceptable to design a cryptosystem like a commercial product.[4]

IV. LITERATURE SURVEY

The image encryption technique is used for securing the data in image. This section presents the literature review of various encryption techniques that we have studied for this work.

In 2016 Nooka Saikumar, R. Bala Krishnan, S.Meganathan, N.R. Raajan [1] proposed an efficient Key based Pattern enciphering scheme for digital color images, which follows pixel value reordering fashion using Adaptive key based block selection algorithm. The proposed scheme is having high resistance against various cryptographic attacks. Multiple pixels reordering patterns have been generated and are applied to a single image by partitioning the image into blocks. The Key (Secret) is used to decide the enciphering pattern on the partitioned image block and it results a final encrypted image. The image can reform in to the parental form with the help of same key and pattern to apply the pixel value reordering scheme to its associated blocks of the image. The main advantage of such a proposed technique is its lossless decomposition, efficiency and simplicity. The experimental outcome shows the efficiency of the proposed technique, which resist the usual existing cipher attacks.

In 2010, Alireza Jolfaei, Abdolrasoul Mirghadri, [3], had done a Survey on Image Encryption Using Salsa20. In this paper author survey Salsa20 as a method for protecting the distribution of digital images in an efficient and secure way. So, we performed a series of tests and some comparisons to justify salsa20 efficiency for image encryption. These tests included visual testing, key space analysis, histogram analysis, information entropy, encryption quality, correlation analysis, differential analysis, sensitivity analysis and performance analysis. Simulation experiment has validated the effectiveness of the Salsa20 scheme for image encryption.

In 2017 Yong Zhang, Xueqian Li, Wengang Hou [4] has proposed A fast image cryptosystem based on AES in this paper the image is divided into data blocks of size 128 bits. Here AES in CBC mode is used for image encryption. First block of plain image is permutated by an initial vector. After that, AES in cipher block chaining mode is used to encrypt every block in sequence. The initial vector and cipher image are transmitted to the decryption party through the public information channel. It uses the secret key and initial vector to decrypt the cipher image to obtain the original image. Simulation results show that this image cryptosystem is both secure and high-speed, which can be used as the comparison basement of newly proposed image cryptosystems based on chaotic systems.

In 2016 Arul Thileeban S. [5] proposed image encryption using XOR Cipher to encrypt the binary data in images pixel by pixel rather than securing it with an application so that it cannot be exploited or cracked easily. Proposed method is tested in a python environment to generate results. This model explains multiple ways to encrypt the Image using XOR Cipher and the analysis shows that by using the proposed model, the images are properly encrypted. The proposed model was tested on various images including Mona Lisa, Apollo 11 and NebulaM83. The future work would include developing a random function with high entropy factors.

In 2017 May H.Abood [6] proposed efficient image cryptography algorithm by using encryption with steganography. These algorithms are performed by using MATLAB program. The proposed system ensure the encryption and decryption using RC4 stream cipher and RGB pixel shuffling with steganography by using hash-least significant Bit (HLSB) that make use of hash function to developed significant way to insert data bits in LSB bits of RGB pixels of cover image. Image encryption using RC4 and Shuffling encryption has a considerable security quality factor which implies the intensity distributions for the original images and mutilated image are distinctive. The security evaluations are presented by calculating a peak signal to noise ratio and mean square error. For secret image, PSNR is infinity and MSE is 0. For cover image, PSNR is about 63 db and MSE is about 0.03.

In 2001 C-C Chang [7], proposed a new Image encryption algorithm based on vector quantization, this is a fast image encryption algorithm based on vector quantization (VQ), cryptography and number theorems. In vector quantization, the image was first decomposed into vectors and the sequentially encoded vector by vector. Then traditional cryptosystem from commercial applications was used, for enhancing security and reducing computational complexity of encryption-decryption, some number theorems were applied. VQ is an efficient approach to low bit-rate image compression, therefore speeds up the encryption process and achieve high security.

In 2016 Parameshachari B D, K M Sunjiv Soyjaudah, Chaitanyakumar M V [8], A Study on Different Techniques for Security of an Image. In this paper author review on the aspects and approaches of design an image cryptosystem. In this they give general introduction on cryptography, images encryption and different types of techniques in image encryption and related works for each technique surveyed. And also compare result of encryption algorithms based on complexity, speed, memory, key type, key length, key space size, and security level. Finally, general security analysis methods for encrypted images are mentioned.

In 2011, Kamlesh Gupta, Sanjay Silakari [9], have proposed New Approach for Fast Color Image Encryption Using Chaotic Map. In this paper author presents a technique which replaces the traditional preprocessing complex system and utilizes the basic operations like confusion, diffusion which provide same or better encryption using cascading of 3D standard and 3D cat map. They generate diffusion template using 3D standard map and rotate image by using vertically and horizontally red and green plane of the input image. They then shuffle the red, green, and blue plane by using 3D Cat map and standard map. Finally the Image is encrypted by performing XOR operation on the shuffled image and diffusion template. Theoretical analyses and computer simulations on the basis of Key space Analysis, statistical analysis, histogram analysis, Information entropy analysis, Correlation Analysis and Differential Analysis confirm that the new algorithm that minimizes the possibility of brute force attack for decryption and very fast for practical image encryption.

In 2010, A.Masmoudi, M.S. Bouhlel, and W. Puech [10], have proposed a new image cryptosystem based on chaotic map and continued fractions. In this paper author proposes a new scheme for image encryption based on the use of a chaotic map with large key space and Engle Continued Fractions (ECF) map. The ECF-map is employed to generate a pseudo random sequence which satisfies uniform distribution, zero correlation and ideal nonlinearity to achieve higher level of security. The proposed scheme is resistant to the known attacks. Theoretic and numerical simulation analyses indicate that our scheme is efficient and satisfies high security.

In 2011, Jawad Ahmad, Fawad Ahmed [11], have proposed an Efficiency Analysis and Security Evaluation of Image Encryption Scheme. In this paper author presents a framework to evaluate image encryption schemes proposed in the literature. Instead of visual

inspection, a number of parameters, for example, correlation coefficient, information entropy, compression friendliness, number of pixel change rate and unified average change intensity etc., are used, to quantify the quality of encrypted images. Encryption efficiency analysis and security evaluation of some conventional schemes like the Advanced Encryption Standard (AES) and Compression Friendly Encryption Scheme (CFES) is also presented. The security estimations of AES and CFES for digital images against brute-force, statistical, and differential attacks are explored. Experiments results are presented to test the security of these algorithms for digital images. After analysis of AES and CFES, some weaknesses have been discovered in CFES. These weaknesses were mainly related to low entropy and horizontal correlation in encrypted.

In 2013, Abhinav Srivastava [13], had presented a survey report on Different Techniques of Image Encryption. In this paper author review the various image encryption techniques and also discuss the general introduction about the cryptography and its types.

In 2011, Sesha Pallavi Indrakanti and P.S.Avadhani [14], had presented a paper Permutation based Image Encryption Technique. In this paper the author describe the random pixel permutation based image encryption by maintaining the image quality using shares key. In this technique the author uses three types of classifications like position permutation, value and visual transformation. The proposed technique provides confidentiality to color image with less computations Permutation process is much quick and effective.

In 2012, K. John Singh and R. Manimegalai [15], had done a Survey on Joint Compression and Encryption Techniques for Video Data. This paper is based on the Joint Compression and Encryption for fast and secure transmission of the video data. They classified various types of compression and encryption algorithms.

In 2012, E. Thambiraja, G. Ramesh and Dr. R. Umarani [16], had done a Survey on Various Most Common Encryption Techniques. In This paper the author focuses on the different types of encryption techniques that are existing and study all the techniques like basic term used in cryptography, key, purpose of cryptography, and classification of cryptography. And he also focuses on image encryption techniques, information encryption techniques. This survey extends to the performance parameters used in encryption processes and analyzing on their security issues.

In 2013, Yasaman Hashemi [17], had presented a paper i.e. Design a new image encryption using fuzzy integral permutation with coupled chaotic maps. In this paper the author introduces a novel image encryption algorithm based on DNA addition combining and coupled two dimensional piecewise nonlinear chaotic map. The proposed algorithm combines good permutation and diffusion properties which can be applied to the encryption of color images. The proposed algorithm is suitable for practical use to protect the security of digital image information 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 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.

VII. CONCLUSION AND FUTURE WORK

There are so many techniques to make an image secure. In general, in today's digital world where nothing is secure, the security of images over network is very important. In our paper we have discussed so many techniques of image encryption. We have surveyed different image encryption techniques from various research papers. We conclude that all techniques are good for image encryption and have their own advantages and disadvantages and they also gives better security at their level so that no unauthorized access can be done on images, which is in the open network. Each technique has its own suitability and its own limitations. But still lot more has to be done in this context. On the basis of above study we provide the following future direction:

1) The Powerful encryption technique like 3DES and MD5 can improve the security.
2) A large key size can be used to improve the image security and protect form brute force attack.

3) We can work on double key encryption in image for the security improvement.
4) Provide 3 way securities to give more strength in encryption.
5) It must require an extremely long computational time to break.
6) The combinations of Pixel Permutation will be shuffled in such manner that it reduces the 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).

[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.