A survey: Different techniques used for Image encryption

[1]Ritu Devi, [2] Navneet Kaur

[1]P.G. Student, Department of Computer Science & Engineering, Global Research Institute of Management & Technology, Kurukshetra, Haryana, India[1]

[2]Asst. Professor, Department of Computer Science & Engineering, Global Research Institute of Management & Technology, Kurukshetra, Haryana, India[2]

ABSTRACT

Abstract: *Users of Internet daily send and receives many images through social media. These images are vulnerable to hack and tamper by attackers. Therefore, it is necessary to develop methods for the security of these images against attackers. Here it is need to develop a non-traditional encryption method for Image encryption so that images can be more and more protected and secured. So presented an overview of digital images and its formats, classification of encryption algorithm, basic concepts of image encryption, some measurements of image security, an overview of soft computing algorithms, its tools and applications and a literature review of image encryption. Based previous proposed techniques we will work on building strong encryption algorithm through implementing the substitution and transposition operations on colors' values of the pixels. In order to make image more secured and protected.*

IndexTerms – *Mage Encryption, Image Logistic map (ILM), Chaotic Mapping, And Discrete Encryption System.*

---

1. INTRODUCTION

Image Encryption is one of the extensively used techniques for data security. In this Data Encryption technique, data is transformed from its innovative to other form so that information cannot be access from the data without decrypting the data i.e. the invalidate process of encryption. The imaginative data is usually referred as basic data and the transformed form is called cipher data. Encryption of image can be definite as the art of convert data into coded form which can be decoded by intended recipient only who poses knowledge about the decryption of the cipher data. Encryption can be functional to text, image, and video for data protection. Responsiveness in digital image processing techniques and methods division from the following most important application areas: enhancement of pictographic information for human understanding; and dispensation of image data for storage space and communication for machine surveillance. At whatever time an image has to be transmitted, two noteworthy issues require to be addressed. One is to accommodate the image contained by the selected bandwidth and the other is to ensure protected transmission of images. Image density and image encryption are two elementary image processing techniques expansively used towards meeting the prerequisite of efficient consumption of bandwidth and security [1][2].

1.1 What is Image Encryption?

Here Image Encryption resources changing convert the image into indecipherable format. This can be done by modifying the image pixels in terms of its (place, Value) in order to protect the information. There can be many technique to encrypt image which involve may be key mapping or hiding of fusion of image ,but basically the image is changed at pixel level i.e. value of pixels or their in original array [3].

1.2 Image Encryption Procedure

The main purpose of keeping images secured is to preserve confidentiality, reliability and authenticity [4]. Different techniques and methods are available for creation images secured and one technique is by encryption method. Normally, Encryption is a process that transformed an image into a cryptic image by utilizing a key. In addition, a user can recover the original image by applying a decryption method on the cipher image [4], which is frequently a reversed implementation of the encryption process. For further description, Figure 1 represent a primary image; a user operate an encryption technique and generated a secrete image; Figure 2 showed an encrypted image that is the output of an encoded process. Alternatively, when a receiver gets this unknown image, he applied the decryption process and recovered the original information. Figure 3 illustrates the recovered image

Fig 1: Panda

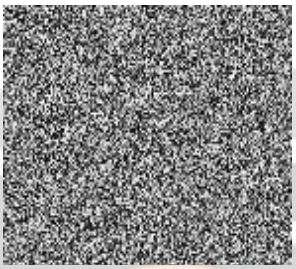

Fig 2: Cipher

Fig 3: Recovered image (Panda)

Cryptography has two main categories given as follows; (1) symmetric key cryptography and (2) asymmetric key cryptography [4]. In symmetric or secret key cryptography, senders and recipients use a same key in encryption and decryption [4].

1.3 Block Diagram of Encryption and Decryption

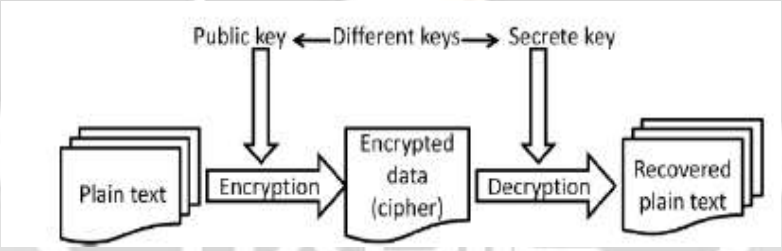

Fig. 4 Symmetric key encryption

Asymmetric or public key cryptography used different keys in encrypting image and decrypting messages received [4]. This procedure applied a public key and a private key to encode and decode an image correspondingly. on the other hand, both keys are exceptional, but scientifically have a connection.

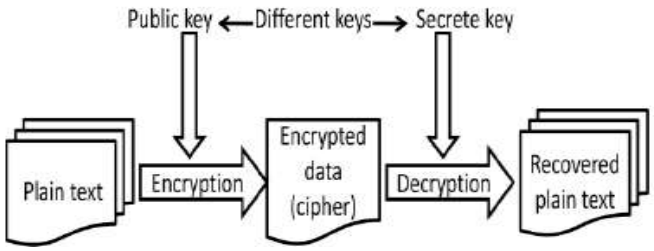

Fig.5 Asymmetric key encryption

The miscellaneous algorithms are available to encrypt information, particularly RSA, DES, AES, etc. nonetheless these algorithms are dominant to encipher a text data, however, inept for the image encryption [4]. Since, images have essential characteristics such as abundant dismissal and a strong connection between adjoining pixels [4]. So, one can effortlessly infer the values of neighbours of a pixel. Hence, images necessitate an efficient method to accomplish an invulnerable safety.

1.4 Image security

The High image Security conception here can be seen in three steps:

- Image Hiding
- Image Encryption
- Image Compresscryption (Compress +Encrypt)

For image Encryption chaotic mapping techniques are used for scrambling the image pixels. And it can encrypt images by dealing out image widen and fold procedure. First of all a square image is divided into two isosceles triangles according the diagonal. Operating the difference of the pixel statistics of two adjacent columns of the triangles, each pixel in a column is interleaved to the adjacent column. The simple image can then be rigid to a line. [3]This line of image value can then be converted to 2D array for i.e. inform of encrypted image. Some of available scheme for image compression are JPEG-LS, SPIHT, JPEG2000, CALIC etc. Renovate like DWT or DCT are generally functional currently. The avail- able techniques use the transformation of pixels but the proposed method here doesn't transform rather it uses basic mathematical operations. Subsequent the numeral theoretic approach afford an additional advantage of image encryption, concurrently, using keys, making the transmit data both short and secure. And in casing of image hiding, the information will be in the form of image. This image is said to be the furtive image. Hence we are providing protection in the form of image. Fig.1 showed that how the process implicated in in sequence hiding. The secret image is first split into 9 parts. Suitable target image have to be particular. The selection procedure depends upon the database. The objective image should be picked from the database and that objective image should be a appropriate match for the source image. The objective image we have preferred should be double in size then the resource image. Mosaic image is then created. The tile images can be used constantly. By resources of a secret key, the mosaic image has been placed beneath the process and thus we are achievement the secret image after embedded process. The hacker without knowing the key cannot restructure back the mosaic image and thus the secret image cannot be viewed.[5]

1.5 Why new methods for image Encryption.

1) More and more images are transmitted over the Internet with the fast developments of information technology. How to protect images has increasingly become an important issue. The encryption is an important tool to protect important information from attackers.[1]

2) Some intrinsic features of images, such as Bulk Data Capacity, High Correlation among Pixels, And DES or AES methods incur large number of computational cost and show poor analysis, prevalent encryption technology such as DES and RSA, and other algorithms are not absolutely fit to image encryption

2. LITERATURE REVIEWS

Jiun In Guo et al. 1999 [6] This paper presented an algorithm which was reflect like. In this algorithm there were 7 steps. In the first, 1-D chaotic system is resolute and its initial point x (0) and sets k = 0. Then, the chaotic progression is generated from the chaotic system. Also binary sequence is produced from chaotic system. And in last 4 stages image pixels are reorganize using swap function according to the binary sequence.

S.S. Maniccam et al. 2001 [7] this paper presented innovative algorithm which do two works: lossless compression and encryption of binary and gray-scale images. The encryption and compression schemes are based on SCAN pattern generate by the SCAN methodology. The SCAN is a recognized language-based 2D spatial-accessing methodology generated a wide range of scanning path or space substantial curves.

Aloka Sinha et al. 2003 [8] Proposed a new system in which the digital autograph of the original image is supplementary to the encoded version of the original image. A most excellent suitable error code is follow to do encoding of the image, ex: (BCH) Bose-Chaudhuri Hochquenghem code. And at the recipient end, after decryption of that image, the digital autograph verified the validity of the image.

M.-R. Zhang et al. 2004 [9] Here H. technique based on T-matrix, used a T-matrix for image scramble. The T-matrix has a simple conformation and a episode twice of the Arnold matrix. This can be practical to image encryption and pre-processing in image handing out such as image watermarking algorithms and etc.

Deng Shaojiang et al. 2005 [10] Image encryption Chaotic Neural method completed an image encryption by a chaotic neural association and the cat map. Here presented a method for making the technique chaos in which networks was used. J. Technique for Image Encryption using chaos technique, it was done in order to improve the pseudorandom distinctiveness of chaotic sequence and an optimized treatment and a cross-sampling discarding is used.

Huang-Pei Xiao et al. 2006 [11] K. Technique for Image Encryption using chaos technique, presented an algorithm using two chaotic structure. One chaotic structure generates a chaotic sequence, which was distorted into a binary stream using a threshold function. The other chaotic structure was used to build a permutation matrix. . Firstly, using the binary stream as a key stream, haphazardly the pixel values of the images was personalized.

M. Zeghid, M et al. 2007 [12] Here investigated the (AES) associated Encryption Standard and in their image encryption procedure they add a key stream generator (W7,A5/1) to AES for make sure the encryption arrangement.

Mohammad Ali Bani Younes et al. 2008 [13] this paper proposed a block-based uprising algorithm which is based on the agreement of image renovation and a well-known encryption and decryption algorithm called Blowfish. The original image was separated into blocks, and using the revolution algorithm it was rearrange, and then the Blowfish algorithm is used for encrypting the distorted image their results show that the correlation between image fundamentals was significantly decrease. Their results also show that increasing the figure of blocks by using smaller block sizes resulted in a lower relationship and higher entropy.

Bibhudendra Acharya et al. 2009 [14] This Image Encryption technique Using Self-Invertible Key Matrix of Hill Cipher Algorithm have proposed an advanced Hill (Advil) cipher algorithm which uses an Involuntary key matrix for encryption. They proposed Advil cipher algorithm using the old one. And it is undoubtedly seen that original Hill Cipher is incapable to do its working appropriately as it did not encrypt the images accurately if the image consists of large area enclosed with same color or gray level. But their planned algorithm works for any images with different gray scale as well as color images.

Seyed Mohammad Seyedzade et al. 2010 [15] Novel Image Encryption Algorithm base on Hash Function and presented an algorithm depend on SHA-512 hash function, which was novel algorithm. It had 2 sections. First of all does pre-processing method to shuffle one half of image then hash function to generate a random number mask? The mask is then XORed with the other part of the image which is disappearing to be encrypted.

Amitava Nag et al. 2011 [16] This method of Image Encryption used Affine convert and XOR procedure, investigated a new algorithm using affine convert and was based on shuffled the image pixels. It was two phase encryption decryption algorithm. By utilized XOR gate operation they encrypted the resultant image and then used the affine renovated pixel value that is redistributed to diverse position with 4 bit keys. In the case of imprecise image then separated into 2 x 2 pixels blocks and all block is encrypted using XOR gate operation by four 8-bit keys. The result proves that the connection between pixel values was significantly reduced after the affine renovate.

Leo Yu Zhang et al. 2012 [17] in today's era colour image encryption algorithm based on chaos was presented by cascade two locality permutation operation and one switch over operation, which are all unwavering by some pseudo-random number sequences generate by iterating the logistic map. This paper evaluated the protection level of this encryption algorithm which find out the locality permutation-only part and the replacement part can be autonomously broken with only $\lceil(\log_2(3MN))/8\rceil$ and 2 chosen plain-images, correspondingly, where MN is the size of the plain-image. The efficiency of the planned chosen-plaintext attack is maintain by concise theoretical analysis and is established by experimental results.

Yogita Verma et al. 2013 [18] Here proposed encryption technique is used to defend multimedia data. There are diverse techniques used to protect private image data from unauthorized access. In this paper presented a susceptibility to investigated on reachable work that is employed totally dissimilar practice for image encryption and that furthermore, provide general introduction regarding cryptography. It has been survey about the presented works on the encryption techniques are AES, 3DES, Blowfish and DES.DES key size is too small as contrast to other techniques. 3DES is slower than other block cipher methods and has poor presentation AES is supposed to be better algorithm which was compared to original Blowfish Algorithm.

Dr. Parma Nand Astya et al. 2014 [19] a variety of encryption and decryption algorithms are available to defend the image from unauthorized user. RSA and Diffie-hellman key substitute provide a good level of safety but the size of encryption key in these two is a big problem. ECC is a better substitute for public key encryption. In this paper the image which is measured to be in the form of a grid, is first distorted on an elliptic curve. These points or coordinates are then encrypted and send to the receiver. At the recipient end decryption algorithm is utilized to exchange the encrypted image into the unique image. Brute force attack is infeasible for ECC since of the discrete logarithmic nature of elliptic curves and used technique to encrypt and decrypt the digital image (BMP) from Elliptic Curve Cryptography.

Ali Abdulgader et al. 2015 [20] This paper proposed a technique that overcome the fixed S-box weak points and improved the presentation of AES when used for encrypting images, predominantly when the image data are large. In adding together, the Mix Column stage is replace by chaotic mapping and XOR procedure to reduce the high computation in Mix Column transform. The proposed technique is tested on numerous images, and the results show that the proposed method efficiently engendered cipher images with very low connection coefficients of adjacent pixels and afford better encryption speed and high security as a result of the dependence of the S-box on the key description of the chaotic system

J. Gayathri et al. 2016 [21] A research work supported on chaotic cryptosystem has been presented to convince the specific desires defined for image communication. In spite of all the remarkable development neighbouring the chaotic cryptosystem, many of the proposed methods discuss with the mandatory number of characteristic that influenced the design of the cryptosystems. Associated with this issue, careful cutinisation of the performance of the existing chaos-based encryption technique is needed for its further development towards practical applications. Encryption technique used according to their association with the chaotic system engaged in three dissimilar categories has been propound to assess the protection and efficiency functions and summarised the existing image encryption techniques in all the three categories followed by a discussion on the security and efficiency constriction.

Cheng Qing Li Set al. 2017 [22] complex dynamics of chaotic map and technologies are used in encryption was studied systematically in the past two decades. Chaotic image encryption scheme was intended by iterating chaotic position permutation and value replacement some rounds, which arriving intensive concentration in the field of chaos-based cryptography. By choosing Chosen-cipher text assault on the Fridrich's scheme utilized influenced network between cipher-pixels and the analogous plain-pixels. This paper scrutinizes some properties of Fridrich's scheme with concise arithmetical language. Then, some minor defect of the real performance of Solak’s attack method was given. The proposed work provided some basics for further optimizing attack on the Fridrich's scheme and its variants.

Xingyuan Wang et al. 2018 [23] proposed a new chaotic image encryption technique, which employs Josephus traverse and mixed chaotic map. The technique consists of three processes: key stream generation process; three-round scrambling process; and one-round diffusion process. The proposed numerical model is applied for the key stream producer in the first process. The initial values and parameters are sensitive to both the secret keys in the new method and plain images. The second development employs the Josephus traversing in scrambling; then the rows and columns of pixels are exchange the third process can modify the pixel gray level values and crack the strong correlation between adjacent pixels simultaneously. The preliminary conditions for chaotic methods are derived using external secret keys by applying some algebraic transformations to the key. Security analysis indicates that the new scheme is effective which can oppose common attacks.

Rashad J. Rasras et al. 2019 [24] This paper will introduced three methods of image encryption-decryption, these method will be implement and tested, and the obtained investigational results will be compared with experimental results of the projected method in order to do some judgment concerning the efficiency and the security of the p Four methods of color image encryption-decryption were studied and all these methods gave efficient parameters. The

fourth proposed method gave the best parameter by decreasing encryption-decryption time and acceptable values for MSE and PSNR, and it is highly secure because of the private key has several values and the number of values is variable and changeable the window size is variable and unpredictable reposed method.

Shelza Suri et al. 2020 [25] proposed and implemented a Pareto-optimal image encryption technique that used coupled map lattice (CML) chaos function and deoxyribonucleic acid (DNA) arrangement to encrypt an image. The discuss work used multi-purpose genetic algorithm (MOGA) to get the optimized result. The proposed two-step algorithm used pseudo-random numbers generator, the chaotic methods CML and DNA created an initial population of DNA in its early stage. The MOGA algorithm is applied in the second half stage to obtain the best mask for encrypting the given simple image. The focal point is on the generation of Pareto fronts by using the Pareto production method of multi-objective optimization and evaluated the presentation of the implemented work using standard metrics like key sensitivity, secret key space, number of pixel change rate, unified average changed intensity, entropy, histogram and correlation coefficient.

CONCLUSION

The algorithms are to formulate a well-organized and secured approach towards Image encryption. (ILM) image logistic map helps to improve the encoding efficiency of image, and along with it DNA diffusion ensures secured transmissions due to its additional operations XOR. So in future work we can use the effective algorithm (ILM) and DNA approach for further improvement in image encryption so that image can be more secured.

REFERENCES

[1] Xiliang Liu, "Selective encryption of multimedia content in distribution networks: challenges and new directions", Proceedings of Communications, Internet, and Information Technology (CIIT 2003), Scottsdale, AZ, USA, Nov. 2003.

[2] Marwa Abd El-Wahed, Saleh Mesbah and Amin shoukry "Efficiency and Security of some Image Encryption Algorithm". Vikram Jagannathan, Aparna Mahadevan, "Number Theory Based Image Compression Encryption and Application to Image Multiplexing", pp. 59-64. 2007.

[3] Feng Huang, Chao Wang, "A New Image Encryption Arithmetic Based on a Three- dimensional Map" , vol. 58, no. 7, pp. 83-91, 2001.

[4] Akshat Agrawal, Ankit Garg," A Review on Various Digital Image Encryption Techniques and Security Criteria", International Journal of Computer Applications · July 2014

[5] Ali Al- Haj, Hiba Abdel Nabi, "Digital image security based on data hiding and Cryptograpgy", IEEE 3rd international conference on communication technology, 2017.

[6] Jiun-In Guo, Jui-Cheng Yen, "A new mirror-like image encryption algorithm and its VLSI architecture", Department of Electronics Engineering National Lien-Ho College of Technology and Commerce, Miaoli, Taiwan, Republic of China, 1999.

[7] S.S.Maniccam, N.G. Bourbakis,"Lossless image compression and encryption using SCAN‖", Pattern Recognition 34 1229-1245, 2001.

[8] Aloha Sinha, Kehar Singh, "A technique for image encryption using digital signature", Optics Communications, Article in Press, 2003. 1-6, www.elsevier.com/locate/optcom.

[9] M.-R. Zhang, G.-C. Shao and K.-C. Yi, "T-matrix and its applications in image processing‖", IEEE Electronics Letters 9th December, Vol. 40, No. 25, 2004.

[10]Deng Shaojiang, Linhua Zhang, and Di Xiao, "Image Encryption Scheme Based on Chaotic Neural System‖", LNCS 3497, pp. 868-872, 2005.

[11]Huang-Pei Xiao Guo-Ji Zhang,"An Image Encryption Scheme Based On Chaotic Systems", IEEE Proceedings of the Fifth International Conference on Machine Learning and Cybernetics, Dalian, 13-16 August 2006.

[12]M. Zeghid, M. Machhout, L. Khriji, A. Baganne, R. Tourki, A Modified AES Based Algorithm for Image Encryption World Academy of Science, Engineering and Technology 27 2007.

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

[14]Bibhudendra Acharya and Debasish Jen, Image Encryption Using Self-Invertible Key Matrix of Hill Cipher Algorithm 1st t International Conference on Advances in Computing, Chikhli, India, 21-22 February 2008.

[15]Seyed Mohammad Seyedzade, Reza Ebrahimi Atani and Sattar Mirzakuchaki, A Novel Image Encryption Algorithm Based on Hash Function 6th Iranian Conference on Machine Vision and Image Processing, 2010.

[16]Amitava Nag, Jyoti Prakash Singh, Srabani Khan, Saswati Ghosh, Sushanta Biswas, D. Sarkar Partha Pratim Sarkar, Image Encryption Using Affine Transform and XOR Operation ,International Conference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN 2011).

[17]Leo Yu Zhang, Rong Ou, Kwok Wo Wong and Shi Shu," Breaking a novel colour image encryption algorithm based on chaos", Springer, 11 octuber 2012.

[18]Yogita Verma, Neerja Dharmale, "A Survey Paper Based On Image Encryption and Decryption Using Modified Advanced Encryption Standard", International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064,2013.

[19]Dr. ParmaNand Astya , Ms. Bhairvee Singh , Mr. Divyanshu Chauhan," Image Encryption And Decryption Using Elliptic Curve Cryptography", International Journal of Advance Research In Science And Engineering http://www.ijarse.com IJARSE, Vol. No.3, Issue No.10, October 2014.

[20]Ali Abdulgader, Mahamod Ismail, Nasharuddin Zainal, Tarik Idbeaa, "Enhancement Of Aes Algorithm Based On Chaotic Maps And Shift Operation For Image Encryption", **J**ournal of Theoretical and Applied Information Technology ,Vol. 71 No.1, 2015.

[21]J. Gayathri , S. Subashini ," A survey on security and efficiency issues in chaotic image encryption", International Journal of Information and Computer Security , Volume 8, Issue 4,2016.

[22]ChengqingLi SiminYu JinhuLü ," On the cryptanalysis of Fridrich's chaotic image encryption scheme", Science direct, Signal Processing ,Volume 132, , Pages 150-154, March 2017.

[23]Xingyuan Wang, Xiaoqiang Zhu, And Yingqian Zhang," An Image Encryption Algorithm Based on Josephus Traversing and Mixed Chaotic Map," IEEE, volume-6, 2018.

[24]Rashad J. Rasras ; Mohammed Abuzalata ; Ziad Alqadi ; Jamil Al-Azzeh ; Qazem Jaber," Comparative Analysis of Color Image Encryption-Decryption Methods Based on Matrix Manipulation", IJCSMC, Vol. 8, Issue. 3, March 2019, pg.14 – 26, 2019.

[25]Shelza Suri, Ritu vijay," A Pareto-optimal evolutionary approach of image encryption using coupled map lattice and DNA", Springer, Neural Computing and Applications, 2020.