DOI: http://dx.doi.org/10.26483/ijarcs.v8i7.4209

ISSN No. 0976-5697

Volume 8, No. 7, July – August 2017

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

IMAGE ENCRYPTION TECHNIQUES: A LITERATURE REVIEW

Reema Dhiman
Student
Department of Electronics and Communication Engineering
GNDU, Regional Campus,
Jalandhar, India

Butta Singh
Associate Professor
Department of Electronics and Communication Engineering
GNDU, Regional Campus,
Jalandhar, India

Abstract: In recent years, it is very important to protect the multimedia applications in which security becomes an important issue to store images. Encryption is the process which is used to encrypt the data and protect these multimedia applications. Present cryptography provides crucial techniques for securing information and these encryption techniques are used to protect the private data from the unauthorized user. In this paper a literature review on various encryption techniques has been explained and the pollster can get an idea for competent techniques to be used.

Keywords: Cryptosystem, Image Encryption techniques, Permutation and Substitution.

I. INTRODUCTION

With the continually expanding development of multi-media applications, security is an imperative issue in communication and storage of pictures. Image encryption [1] is one of the valuable technology for image security. Scientists and people who work to find information are always in search to improve the existing systems. Regular up gradation and optimization of ways of doing things is an everlasting need of technologies. In cryptography, we have two operations-encryption operation and decryption operation [2]. A unique message is known as the plain content, while the coded message is called figure content. The way toward changing over plain content to figure content is known as enciphering or encryption. To bring back the plain content from the figure content is unscrambling or decryption. It is an effort to review the different input from the people who work to find information around the world and identify the extent of the further making things up on the spot. In this paper, the different techniques of image encryption and its literature review have been studied from various research papers, journals and books.

A. *Goals of Cryptography*

Encryption is a study of techniques [3] that are used to accomplish the following four goals: confidentiality, data integrity, authentication, non-repudiation. The investigation of the strategies used to break existing cryptosystems is called cryptanalysis. Let us try to attempt to see every one of the four objectives of cryptography.

1) Confidentiality alludes to the insurance of data from unauthorized user. An undesired conveying party, called an adversary, must not have the capacity to get to the correspondence material. This objective of cryptography is a fundamental one that has dependably been tended to and upheld all through the historical backdrop of cryptographic practice.

2) Data integrity guarantees that data has not been controlled in an unapproved way. On the off chance that the data is changed, all conveying gatherings can recognize this modification.

3) Authentication strategies are grouped into two classes: entity authentication and message authentication. Entity authentication is the procedure by which one gathering is guaranteed of the character of a second party required in a convention, and that the second has really taken an interest quickly preceding the time of proof is gained. Message authentication is a term utilized comparably with information starting point verification.

4) Non-repudiation implies that the recipient can demonstrate to everybody that the sender send the message without a doubt. That is, the sender can't guarantee that he or she didn't scramble or sign certain computerized data.
Luckily, present day cryptography has created procedures to deal with every one of the four objectives of cryptography.

B. *Principles of Cryptography*

The essential thought of encryption [3] is to change the message such that exclusive a lawful beneficiary can reproduce its substance. A discrete-value cryptosystem can be described by:

- a set of possible plaintexts *P*
- a set of possible ciphertexts *C*
- a set of possible cipher keys *K*
- a set of possible encryption and decryption transformations *E* and *D*

An encryption framework is likewise called a cipher, or a cryptosystem. The basic diagram for cryptosystem is shown in Figure 1.

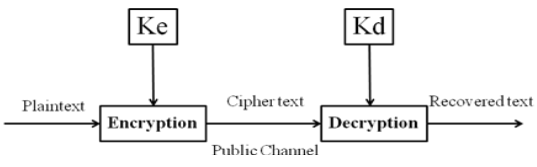

Figure 1 Cyptosystem

The message for encryption is called plaintext, and the scrambled message is called cipher text. Indicate the plaintext and the cipher text by P and C, individually

$$C=Eke\ (P)$$

where *Ke* is the encryption key, and *E* is the encryption function. Likewise, the decryption procedure is characterised as

$$P=DKd\ (C)$$

where *Kd* is the decryption key, and *D* is the decryption function. The security of a cipher depends upon the decryption key *Kd* as an adversary can recover the plaintext from the observed cipher text once the adversary gets *Kd*.

C. *Techniques of Image Encryption*

Encryption techniques are the significant tool for securing the confidential data. The traditional algorithms such as DES, AES, RSA, Blowfish, IDEA etc [4], are also used for image encryption but they are not suitable because of two reasons:

- Size of the image is always greater than the size of the text
- Decrypted text must be equal to the original text.

Due to these issues, we cannot use these algorithms for image encryption. Also the image has special features like bulk data capacity, strong correlation among adjacent pixels, high redundancy etc. Due to these reasons, new algorithms and techniques are proposed for the image encryption. These are:

1) Position Permutation Based Algorithm: This algorithm is mainly used when the rearrangement of elements can be done in the plain image by bitwise, pixelwise and blockwise. By using bitwise operation, the permutation of bits minimizes the perceptual information [6]. If we use pixelwise and blockwise operation then it produces a high level of security.

2) Value Transformation Based Algorithm: This algorithm is mainly used when we change the values of the pixels with some other pixel value [7]. This algorithm uses the mathematical computations and it involves the following procesdure. Here, we take pixel value as input, compute it with some formulas and then produce a new pixel value.

3) Position-Substitution Based Algorithm: This algorithm is the combination of both the above algorithms. In this algorithm, [8] first we change the values of the pixels and then a key is generated which is used to substitute the pixel values. With the help of these algorithms, we can encrypt the images easily and also solve the issues which is arises in the traditional algorithms.

II. LITERATURE SURVEY

Image encryption is a process in which pixel values are changed by that way it changes the strength of that pixel. Change in pixel value leads to change in amount of information in a secret image. The literature review regarding few techniques is discussed in subsequent subsections.

Cheng Yen *et al* proposed a chaotic key based computation to change the pixel estimation of the plain-picture [9]. By utilizing this computation, the gray level of every pixel is XORed or XNORed a little bit at a time to one of the two fore obtained keys. The alluring after effect of the encoded picture being totally confused and the outcomes for scrambled picture has better security. Besides, its VLSI engineering is planned and the design of coordinating the encryption conspires with MPEG2 is likewise proposed.

Maniccam *et al* has intended a technique which accomplishes both lossless compression and encryption of twofold and gray scale pictures [10].The compression ratio and the encryption plans depend upon the SCAN designs produced by the SCAN technique. This SCAN methodology helps in generating better compression ratio. The SCAN is a formal dialect based two-dimensional spatial domain, which can effectively specify and create a wide variety of checking ways or space filling bends.

A new method was projected by Shuqun in which the color images are encrypted by using existing optical encryption systems for gray-scale images [7]. Previously, the color images are first converted into the indexed image formats. In the encryption phase, the image is encoded to stationary white noise for two irregular phase masks, one in the input plane and the other one is in the Fourier plane. At the decryption end, the color images are improved by converting the decrypted indexed images back to their RGB (Red-Green- Blue) formats. The recommended single-channel color image encryption method is more compact and vigorous than the multichannel methods.

Jiancheng Zou. *et al.* introduced another strategy in view of Fibonacci numbers to advanced picture scrambling system. The consistency and periodicity of the scrambling transformation are examined [11]. There are following advantages for scrambling transformation i.e. Encryption and decryption is very easy and they can be applied in real time situations. The scrambling effect is very rational and the image data is to be re- distributed randomly across the whole image. This system could endure little some picture attacks, for example, compression, clamor and passing for information bundle. They urbanized a method to study video scrambling and probe corresponding embedding algorithms for digital watermarks.

Data security is principle worry at present. Image scrambling is one of the best approach to encode the computerized picture information [12]. A novel picture scrambling strategy utilizing Non-Commutative wavelet change and Poker Shuffle change because of appropriateness of Non-commutative Wavelet change for picture scrambling application over ordinary Wavelet change and non-linearity and non-analytic calculation attributes of Poker shufling builds the execution of proposed system. The proposed technique contrasted and distinctive existing picture scrambling calculation on the ground of picture encryption. It is essentially appeared by applying the chosen plaintext and known-plaintext assaults which effectively recuperates the plaintext-picture from the encoded picture without knowing the mystery key. The thought is to demonstrate the ineligibility of the encryption conspire for use in commonsense picture security applications.

Mohammad Ali *et al*. proposed an image encryption algorithm [13] which is based on block-based transformation and the conventional Blowfish algorithm. When we combine both the transformation algorithm and Blowfish algorithm together then the resulted algorithm shows lowest correlation and the

highest entropy. It is found that the number of blocks and the correlation are inversely proportional to each other. Also, number of blocks and the entropy are directly proportional to each other.

Shesha P. *et al.* introduces an image encryption technique [8] which is based on the three classifications but the major task in image encryption technique is related to shifting process. The procedure is executed in three fundamental steps, the first phase is image encryption where the image is divide into blocks and these blocks are then permutated. Furthermore, the permutation is useful based on a random number to strengthen the encryption. The second phase is the generation of key, where the standards used in the encryption process are used to assemble a key. The third phase is the recognition process which involves the numbering of the chunks that are generated from the secret image. These chunks and the key are then transferred to the receiver. The receiver uses the key to build a secret image in the decryption process. The method projected is a exceptional one from others in a way that the generated key with valid information about the values used in the encryption process.

Abbas, *et al.* presented a novel technique for digital images encryption with password security using 1D SHA-2 algorithms attached with a compound forward transform [14]. A spatial masquerade is generated from the frequency domain by taking advantage of the Fourier Transform i.e. conjugate symmetry of the complex imagery part. This masquerade is then XORed with the bit stream of the original image. Both the exclusive OR (XOR) and a logical symmetric operation yields 0 if both the binary pixels are zeros or ones otherwise it yields 1.

Sang-Su proposed a method for a visual cryptography format that uses phase masquerade and an interferometer [15]. A binary image is to be encrypted only when the image is divided into an arbitrary amount of slides and encrypted them using an XOR process with a random key. The phase masquerade for each encrypted image was fictitious under the proposed phase obligation guideline. For decryption, phase masquerade were placed on any path of the Mach-Zehnder interferometer. Through optical experiments, it was inveterate that a covert binary image that was sliced could be improved by the proposed technique.

Ismail *et al.* projected a chaos-based stream code, which includes two chaotic logistic maps and peripheral secret key for encryption of image [16]. In this, an peripheral secret key of 104 bit and two chaotic logistic maps are used to discriminate between the encrypted image and the plain image. Further, the secret key is personalized after encrypting of every pixel of plain image which create the encrypted image more robust. There is a feedback system which increases the sturdiness of the projected system.

Recent research on image encryption calculations has been progressively in light of disorganized frameworks, however the disadvantages of little key space and feeble security in disordered cryptosystems are self-evident [17]. A new raucous maps in light of beta capacity were created.The era of various pseudo arbitrary successions was done to shuffle the position of the picture pixels and to confound the connection between the scrambled picture and the first picture, accordingly significantly expanding the imperviousness to assaults. The proposed framework has the benefit of high security investigation, for example, key space, measurable and affectability examination.

Mitra A, *et al.* has proposed an image encryption algorithm in which the order of the bit, pixel and block permutations is random [6]. The image encryption mechanism using the combination of different permutation techniques. They coeval an approach for random combination of abovementioned permutations for image encryption. By checking the results, it is pragmatic that the permutation of bits is efficient in appreciably dropping the correlation thereby decreasing the confidential information. Further they uses three different permutations methods i.e, bit level permutation, pixel permutation and then block permutation.

Kwok-W. *et al.* presented a more well-organized diffusion method using simple table lookup and swapping procedure as a light-weight replacement of the 1D chaotic map iteration [18]. In the substitution stage, this approach makes use of a static 2D table and a dynamic 2D lookup table formed in the diffusion process. The value and the position of each permuted image pixel are used to lookup the tables so as to obtain a novel 8-bit value pair to masquerade the permuted pixel value.

Zhu *et al.* have exhibited a image cryptosystem utilizing the Arnold cat map for bit-level stage and the logistic map for diffusion [19]. In this cryptosystem, the pixel-level stage is supplanted by somewhat level change. At the point when a bit in one pixel is traded with a bit in another pixel, the data in the two pixels is traded and their esteems are adjusted. Subsequently, the bit-level change has the impacts of both confusion and diffusion. In the confusion period of this cryptosystem, the higher 4 bits are permuted separately, while the lower 4 bits are moved overall. The impact of this stage is that not just the areas of the pixels are traded, additionally the estimation of every pixel is altered. In the diffusion stage, every one of the pixels are examined on a level plane from the upper left corner to the lower right corner to shape an arrangement. Every pixel esteem is changed successively at the pixel-level by the yield of the logistic map.

Zhang Yun *et al*. explores on the chaotic encryption, DES encryption and a mix of image encryption calculation [20]. Initially, this method involves a new encryption conspire utilizes the calculated logistic chaos sequencer to make the pseudo-arbitrary succession, carries on the RGB with this grouping to the picture turbulently, at that point makes twofold time encryptions with change DES. Their outcome indicate high beginning quality sensitivity, and high security and the encryption speed.

The creators [21] utilize a non-symmetric divide to produce N-stage pseudorandom successions utilizing the calculated maps. The hypothetical examination demonstrates that this N-stage strategic succession is with uniform dissemination, also, free and indistinctly passed on. Numerical analyses demonstrate that these N-stage strategic groupings have high multifaceted nature and are with great irregularity. Moreover, they propose another image encryption calculation in view of the N-stage strategic succession, which is consolidated with both rearranging and substitution calculations. A few security tests

are done to exhibit that the creators' new calculation is with a high security level, and can oppose different assaults, which can be focused with some other as of late proposed image encryption calculations.

An adaptable optical encryption structure in light of different lighting up and disproportionate encoding is proposed [22].The info picture is encoded by consumption of two self-assertive shroud situated at the information and the conjugate plane in a veering circular wave field. Contrasted and the partners utilizing planar brightening and symmetric keys, a critical distinction is that consistent change of places of optical components connected for encryption is permitted, bringing about unscrambling keys not the same as the encryption keys and variable size show of encoded/decoded pictures. A quick and dull numerical portrayal and estimation comes about with various data transmissions of the structure reinforce our recommendation.

Most of papers on image encryption give a few measures to bear witness to that the introduced works fulfill the required criteria in the field [23]. Some others propose a near review and choose whether one work is superior to anything another continually utilizing these measures. These last are of different sorts where the association coefficient is one among them. It is a factual measure used to examine the likeness between neighboring pixels in a figure. Its significance is constrained to have a thought regarding the subsequent de-correlation. Notwithstanding, its utilization to choose about the nature of the calculation, or to contrast it with another is impractical. We demonstrate that any computed esteem is encompassed by arbitrariness.

Akkasaligar, P. T. et al. proposed a secure medical image encryption based on intensity level using chao's theory and DNA cryptography. In this specific circumstance, a safe picture encryption calculation is proposed [24] that utilize both AES and Visual Cryptographic systems to ensure the picture. The picture is scrambled utilizing AES and an encoding mapping has been proposed to change over the key into offers in view of Visual Secret Sharing. The cryptanalysis of the calculation is then performed and is ended up being secure. The proposed calculation is then actualized utilizing python and the outcomes are examined alongside the conceivable future alterations.

Panduranga et al proposed [25] a secure method by hybridizing the SCAN pattern and the carrier image for image encryption to get extremely distorted image. The encryption method involves the foloowing three steps; first pace is constructing a size extended binary image using original image. In second pace, pertain the existing SCAN patterns to reorganize the pixels of extended binary image and ultimately in third pace, rebuild the gray scale image to obtain the encrypted story. They also developed the perception of generating the carrier image with the help of distinctive code called as 4 out of 8-code. The proposed hybrid approach for image encryption gives very superior results as compared to entity encryption process.

III. ENCRYPTION MEASURES

A good encryption algorithm should always resist the known attacks. The security analysis of various encryption techniques can be done by using following image parameters.

A. Mean Square Error

Mean Square Error (MSE) is a parameter used to quantify distinction amongst original and encrypted image in which pixels are spoken in the vicinity of 0 and 255. MSE is explained as the measure of degree of similarity or it's the extent of error/distortion between two signals. MSE could also be thought of a measure of signal quality [26]. It is given as:

$$MSE(S, S') = \frac{1}{M}\frac{1}{N}\sum_{i=1}^{M}\sum_{i=1}^{N}(S - S')^2$$

Where S depicts original image and S' represents the encrypted image and M and N symbolizes total number of rows and columns respectively $(S\text{-}S')^2$ stands for squared error image i.e. squared difference between original and encrypted image.

B. Peak signal to Noise Ratio

Peak signal-to-noise ratio is the ratio between the maximum possible power of pixel value and the power of noise. It is general expressed in logarithmic scale [27]. It is given as:

$$PSNR = 20*\log_{10}(MAX) - 10*\log_{10}(MSE)$$

Where MAX = maximum value of pixel in the original image and MSE is the mean squared error. Greater the PSNR value and better will be the quality of the image.

C. Entropy Analysis

The mathematical determination of randomness in an image and that can be utilized to describe the texture of the input image quantity [28]. It gives an idea about the amount of information which is to be coded by an algorithm. It is defined as:

$$H= -\sum_{k=0}^{M-1} p(k) * log_2 p(k)$$

Where H represents entropy, M is the range of gray levels and p(k) is the probability related to gray level k.

D. Correlation Analysis

The effect of the image decomposition is related to the correlation of adjacent pixels. A best decomposition level will always have a low correlation value. In order to calculate the correlation between the plain image and the original image then different levels of decomposition are analysed for both the original and the plain image. Following are the formulae which are used to calculate the correlation coefficients in the horizontal, vertical and diagonal directions.

$$\gamma = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x)\right)^2$$

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x)\right)\left(y_i - E(y)\right)$$

Where x and y are the gray scale values of two-adjacent pixels in the image and N is the number of duplets (x,y) obtained from the image.Correlation is the determination of strength. A correlation value greater than 0.8 is usually robust correlation, whereas a correlation value less than 0.5 are delineate as weak [29]. A practical measure to evaluate the encryption quality of any image cryptosystem is the correlation coefficient between pixels at the same indices in the original and the encrypted images.

IV. Conclusion

The Study of Literature survey is always a benchmark for any research work. Nowadays, it is more important to secure the digital images in an open network. A brief literature survey regarding image encryption on various techniques is revived in this paper. We conclude that in real time applications, all the image encryption techniques are useful. The techniques discussed in this paper provide better security functions. Always choose fast and secure algorithm which provides superior security. So, no one can access data or image in the open network.

V. Acknowledgement

I would like to express my sincerest appreciation to **Dr. Butta Singh**, Department of Electronics and Communication Engineering, who providing me valuable and countless resources; insight and intuition, but also continuously gave me support, reassurance and encouragement.

VI. References

[1] Xingyuan Wang, Ying-Qian Zhang and Xue-Mei Bao, "A novel chaotic image encryption scheme using DNA sequence operations," Opt Lasers Eng, vol. 73, pp. 53-61, October 2015.

[2] William stallings, "Cryptography and Network Security: Principles & Practices ‖, " Second edition.

[3] Fathi E. Abd El-Samie, Hossam Eldin H. Ahmed, Ibrahim F. Elashry, Mai H. Shahieen, Osama S. Faragallah, El-Sayed M. El-Rabaie and Saleh A. Alshebeili, "Image Encryption-A communication Perspective," CRC Press, Taylor and Francis Group, 2014.

[4] Bruce Schneier, "Applied cryptography: protocols algorithms and source code in C," New York (USA): Wiley, January 1996.

[5] Yen Juicheng and *Guo Jiunin*, "A *New* Chaotic *Mirror-Like Image Encryption Algorithm* and *Its VLSI Architecture*," Pattern Recognition and Image Analysis, vol. 10, no. 2, pp. 236-247, 2000.

[6] A Mitra, Y.V. Subba Rao and S.R.M. Prasanna, "A new image encryption approach using combinational permutation techniques," Journal of computer Science, vol. 1, no. 1, pp. 127-131, January 2006.

[7] Shuqun Zhang and Mohammad A. Karim, "Color image encryption using double random phase encoding," Microwave and Optical Technology Letters, vol. 21, no. 5, pp. 318-322, April 1999.

[8] Shesha Pallavi Indrakanti and P.S.Avadhani, "Permutation based image encryption technique," Journal of Computer Applications, vol. 28, no. 8, pp. 45-47, August 2011.

[9] Jui-Cheng and Jiun-In Guo, "A new chaotic key-based design for image encryption and decryption," IEEE International Symposium on Circuits and Systems, vol. 4, pp. 49-52, August 2002.

[10] Maniccam S. and N.G. Bourbakis, "Image and video encryption using SCAN patterns," Pattern Recognition, vol. 37, no. 4, pp. 725-737, April 2004.

[11] Jiancheng Zou, R. K. Ward and Dongxu Qi, "A new digital image scrambling method based on fibonacci number," Proceeding of the IEEE Inter Symposium On Circuits and Systems, vol. 3, pp. 965-968, September 2004.

[12] Nabil Ben Slimane, Kais Bouallegue and Mohsen Machhout, "Nested chaotic image encryption scheme using two-diffusion process and the secure hash algorithm," Proceedings of 2016 4th International Conference on Control Engg. and Information Technology, no. 1, pp. 16–18, December 2016.

[13] Bani Younes, Mohammad Ali, Jantan and Aman, "Image encryption using block-based transformation algorithm," IAENG International Journal of Computer Science, vol. 35, no. 1, pp. 15-23, 2008.

[14] Seyed Mohammad Seyedzade, Sattar Mirzakuchaki and Reza Ebrahimi Atani, "A novel image encryption algorithm based on hash function," Optics Communications, vol. 283 pp. 879– 893, October 2010.

[15] Sang-Su Lee , Jung-Chan Na , Sung-Won Sohn , Cheehang Park , Dong-Hoan Seo , and Soo-Joong Kim, "Visual cryptography based on an interferometric encryption technique," ETRI Journal, vol. 24, no. 5, pp. 373-380, October 2002.

[16] Ismail Amr Ismail , Mohammed Amin, and Hossam Diab, "A Digital Image Encryption Algorithm Based a Composition of Two Chaotic Logistic Maps," International Journal of Network Security, vol. 11, no. 1, pp. 1 -10, July 2010.

[17] Weibin Zhong, Yu Hui Deng, and Kai-Tai Fang, "Image encryption by using magic squares," International Congress on Image and Signal Processing, BioMedical Engineering and Informatics, pp. 771–775, October 2016.

[18] KW Wong, BSH Kwok, and CH Yuen, "An efficient diffusion approach for chaos-based image encryption," Chaos Soliton Fract, vol. 41, no. 5, pp. 2652–63, September 2009.

[19] Z Zhu, W Zhang, K Wong and H Yu, "A chaos-based symmetric image encryption scheme using a bit-level permutation," Inform Sci., vol. 181, no. 6, pp. 1171–86, March 2011.

[20] Z Yun-Peng, L Wei, C Shui-ping, "Digital image encryption algorithm based on chaos and improved DES," IEEE International Conference on Systems, Man and Cybernetics, pp. 474-479, October 2009.

[21] L Liu, S Miao, H Hu, M Cheng, "N-phase logistic chaotic sequence and its application for image encryption," IET Signal Processing, vol. 10, no. 9, pp. 1096–1104, December 2016.

[22] X Wang, G Zhou, C Dai, J Chen, "Optical image encryption with divergent illumination and asymmetric keys," IEEE Photonics Journal, vol. 9, no. 2, pp. 1-8, April 2017.

[23] S Arul Thileeban, "Encryption of images using XOR cipher," IEEE International Conference on Computational Intelligence and Computing Research, pp. 1–3, December 2016.

[24] PT Akkasaligar and S Biradar, "Secure medical image encryption based on intensity level using chao's theory and DNA cryptography," IEEE International Conference on Computational Intelligence and Computing Research, pp. 1-6, December 2016.

[25] Panduranga H.T and Naveen Kumar S.K, "Hybrid approach for image encryption using SCAN patterns and carrier images," International Journal on Computer Science and Engineering, vol. 2, no. 2, pp. 297-300, 2010.

[26] SRM Prasanna, YVS Rao and A. Mitra, "An image encryption method with magnitude and phase manipulation using carrier images," World Academy of Science, Engineering and Technology, vol. 2, pp. 817-822, 2006.

[27] Chao-shen Chen and Rong-jian Chen, "Image encryption and decryption using SCAN methodology," PDCAT '06. Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies, pp. 61 – 66, December 2006.

[28] Quist-Aphetsi Kester, "Image encryption based on the RGB pixel transposition and shuffling," International Journal Computer Network and Information Security, vol. 7, pp. 43-50, June 2013.

[29] P Mishra, B Thankachan, "Highly Secure Method for Image Transmission Using Partition and Multi Encryption Technique," International Journal of Science and Research, vol. 2, no. 7, pp. 347-350, July 2013.