International Journal of Engineering, Science and Mathematics
Vol. 6Issue 7, November 2017,
ISSN: 2320-0294 Impact Factor: 6.765
Journal Homepage: http://www.ijesm.co.in, Email: ijesmj@gmail.com Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

A Secure Chipped Image Encryption Technique for Image Transmission

Arun JB *
Reshu Choudhary**

Abstract

A major issue for computer networks is to prevent important information from being disclosed to illegal users. So to ensure the security of these multimedia data encryption technique is used. After analyzing several digital encryption and decryption algorithms this study designs a symmetric image encryption and decryption scheme based on image chipping method. Through number of experimental tests conducted with this detailed encryption algorithm, we demonstrate a high security algorithm of the new scheme. In this study, we propose a new algorithm to encrypt an image for secure transfer. At the start, we break up the original image using chipping algorithm, and find out the most appropriate optimum chipping point where encrypted and cover image quality are similar. This proposed method applied chipper and encryption both simultaneously.

Keywords:

Data securityt;
Encryption algorithms;
Cryptography;
Image chipping;
Image quality measurement.

Author correspondence:

First Author,
Lecturer, Government Polytechnic College
Ajmer, Rajasthan, India

1. Introduction

In the recent years, with the rapid development of communication and the computer technology, it has created an environment in which it became very easy to obtain, replicate and distribute digital media products such as digital text, image, video and audio without any loss in quality. In fact, an enormous number of digital products have been pirated. Protection of digital multimedia products has therefore become an increasingly important issue for products owners and service providers [1].

Processing and transmission of multimedia contents over insecure networks, possesses several security problems as a result, multimedia data security has become a serious and major issue in telemedicine, military, E-Commerce, financial transaction and mobile phone applications [2]. To provide security attributes to multimedia contents, one needs to protect communicated information (plaintext) from unauthorized users. Multimedia contents needs to be secured from

*Lecturer, Government Polytechnic College, Ajmer, Rajasthan, India
**Research Scholar, Bhagwant University, Ajmer, Rajasthan, India

different type of attacks; for example, interruption, interception, modification and fabrication [3]. Cryptography is basically scrambling of data for ensuring secrecy and authenticity of information. Cryptography enables us to transmit data across insecure networks so that it cannot be read by anyone except the authorized recipient. Cryptology and cryptanalysis are two main branches of cryptography. Cryptology is to keep plaintext secret from eavesdropper or simply the enemy while cryptanalysis deals with the defeating such techniques to recover information or forging information that will be accepted as authentic [4]. For secure transmission of multimedia data, information should be concealed from adversaries or attackers. Information is an asset like other assets. So as an asset, information is to be kept secret from intruders, interceptor, attackers or simply the enemy. Over global communication channels, people send sensitive personal information, corporate documents and financial transactions. In such scenarios; security, integrity, authenticity and confidentiality of digital data should be provided. For security of multimedia data, one of the obvious technology is encryption. Encryption is the process of disguising a message. In encryption, the content of multimedia data is protected and a key is required for proper decryption [5]. The encrypted message is called the cipher text and unencrypted message is called the plaintext. Obtaining the plaintext back from the cipher text is known as decryption. There are two types of algorithms used for encryption; symmetric-key algorithms and public key algorithms. In most of the symmetric algorithms, the encryption key and the decryption key are same. In public key algorithms, encryption and decryption keys are different. The encryption key is made public so that anyone can encrypt a message, however, only the person who has the correct private key can decrypt the message. It is believed that in a reasonable amount of time, it is infeasible to calculate the decryption key from the encryption key.

2. Literature Survey

In 2010, Kiran Kumar introduces that encryption is the process of transforming the original data in to a chipper data (the original data can be transferred to unreadable format) and converting the chipper data to original data in other side. With the enormous growth of computer networks and digital technologies, a huge amount of digital images are transferred through networks. Then in 2012, Abusukhon and Talib proposed that mostly the images from bank transaction and any money related digital images will be confidential or private, distinct security algorithm has been used to provide the required protection methods [6-8].

Guo, in 2010 proposed the security of bank or money oriented images become more and more emphasis due to the high evolution of e-banking in the network world today. The security of these kinds of images has attracted more and many different image encryption algorithms have been proposed by Liu in 1993, to enhance the security of checks and demand draft images. In 1998, Tao modified this image encryption algorithm try to convert to another one, that can be hard to understand and hard to rearrange. On the other hand in 2011, Zhang and Liu proposed that the encrypted image gets decrypted and bring original image. In recent years, we have various encryption and decryption algorithms and there is no single algorithm that satisfies different image types but can encrypt all type of images. Most of algorithms are designed to encryption and decryption of original images which are proposed in the middle of 1990s [9-12].

In 2002, Zhao and Chen proposed the encryption algorithm is classified in two ways one is non-chaos selective method and another is chaos based selective method. In 2011, Lakhtaria studied about protecting computer network with encryption technique with bit pixel and block permutations. In 2011, Chan in his study on security framework for privacy preserving data aggregation in wireless sensor networks showed shuffling image pixels which changed the value of gray color of image and confused the hacker to find out the chipper text. In 2010 Padma in their study on encoding and decoding of a message in the implementation of elliptic curve cryptography provided secret combinations combined with other encryption techniques to make highly encrypted chipper images. Kiran Kumar studied efficient digital encryption algorithm based on matrix scrambling technique, this image encryption based on the permutation of pixels combined with a new algorithm. In 2010, Abusukhon and Talib in their study used digital signature algorithm to create a complex digital algorithm for making encryption. Cryptography is referred as encipher or encoding used to convert the image or text to incomprehensible format. When the data are to be transmitting, it will be decrypted depending on what kind of data to be sent. More and more important images like checks and tenders transmit over the internet due to the enormous growth of internet and multimedia technology [13-16].

A new approach is recommended in this study for fast and secure image encryption. In this study, we propose a new encryption algorithm based on the image encryption using color scheme encryption. In 2010, Zaiden et al. give that the image values of blocks are strongly connected and the blocks are predicted by the values. They propose a coloring algorithm that divides the images by their colors, subdivide into blocks and shuffle their blocks position before it is transmitted by blowfish encryption algorithm. Before the encryption, they added the 128 bit public key for more encryption. Recently in 2013, Ganesh Kumar proposed the secret key of algorithm is used to encrypt the shuffled image and check the correlation value, the value is very high compared with other encryption algorithms [17-18].

2.1 Image Evaluation Techniques:

Some image encryption and decryption quality are measured by researches most commonly used parameters are:

2.1.1 Mean Squared Error (MSE)

One obvious way of measuring this similarity is to compute an error signal by subtracting the test signal from the reference, and then computing the average energy of the error signal [19-20]. The mean-squared-error is the simplest, and the most widely used .For good image quality its value is became low. This metric is frequently used in signal processing and is defined as follows:-

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left(x(i,j)-y(i,j)\right)^2 \qquad (1)$$

Where x (i, j) represents the original (reference) image and y (i, j) represents the distorted (modified) image and i and j are the pixel position of the M×N image. MSE is zero when x (i, j) = y (i, j).

2.1.2 Peak Signal to Noise Ratio (PSNR)

The PSNR is evaluated in decibels and is inversely proportional the Mean Squared Error. If PSNR value is high it shows good quality image.

$$PSNR = 10\log_{10}\frac{\left(2^n-1\right)^2}{\sqrt{MSE}} \qquad (2)$$

3. Proposed Method

The new algorithm of this paper handles hiding different images inside other images of various types. When an image is chosen to be used for hiding other image, it is called a cover image and the image which is to be hiding is called secret image [21-25]. By applying proposed image chipping algorithm find out the effect of image distortion in image cryptography. In this proposed technique unauthorized user is unable to recognize the encryption process on cover image, because encrypted image quality is very near to the cover image quality. So it is more secure and safe access.

In this proposed technique secret image is chipped by a chipping factor (N), and afterwards encrypted with cover image (key) as shown in Figure 1, and then encrypted image transmitted to user. The authorized user can decrypt image with the help of cover image (key) and then unchipped by unchipping factor (N), after this process user get the decrypted secret image as shown in Figure 2.

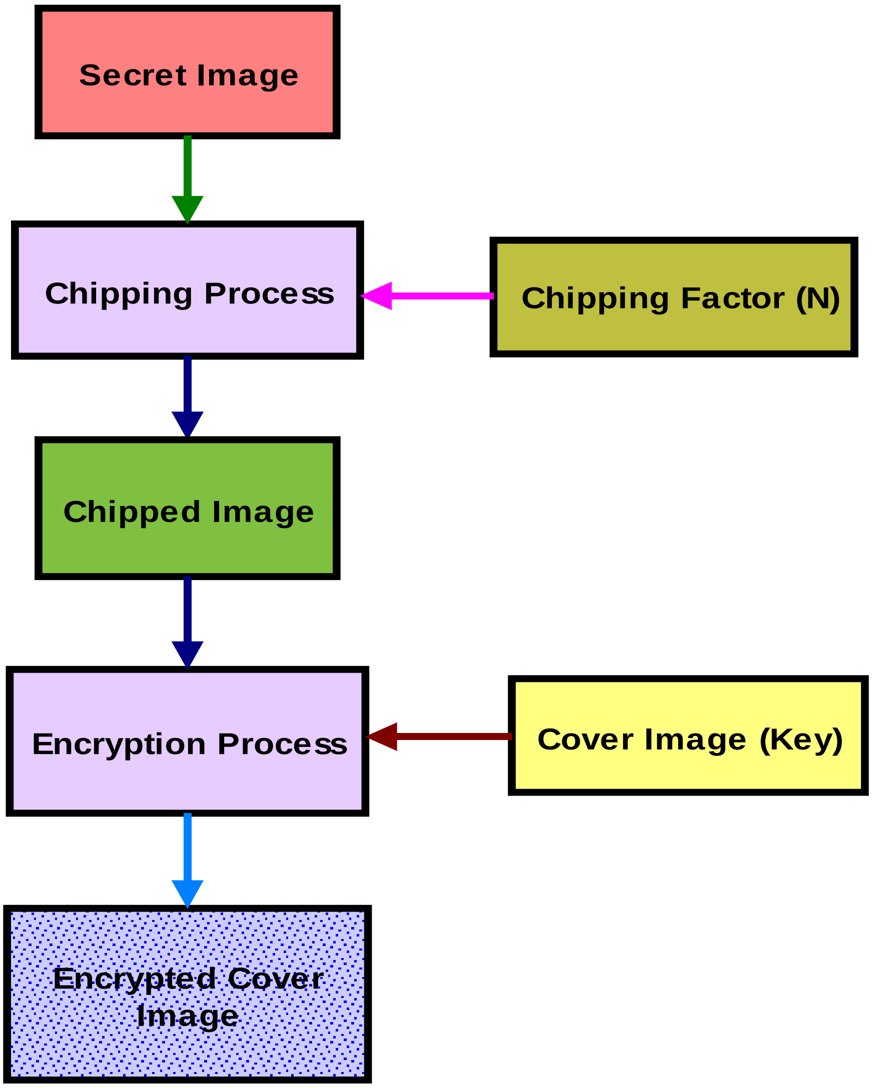

Figure 1. Proposed method for Chipping and Encryption Process.

3.1 Proposed Encryption algorithm is shown below:

i. Read the secret image.
ii. Read cover image database.
iii. Chip the secret image by chipping factor N.
iv. Encryption of chipped secret image with cover image.
v. Evaluate the $PSNR_2$.
vi. Transmit encrypted image over channel.

3.2 Proposed decryption algorithm is shown below:

i. Transfer image to user.
ii. Decrypt secret image with the use of cover image database.
iii. Multiplies the chipping factor for unchipping to the encrypted image.
iv. Evaluate the $PSNR_1$.
v. Displays the image to user.

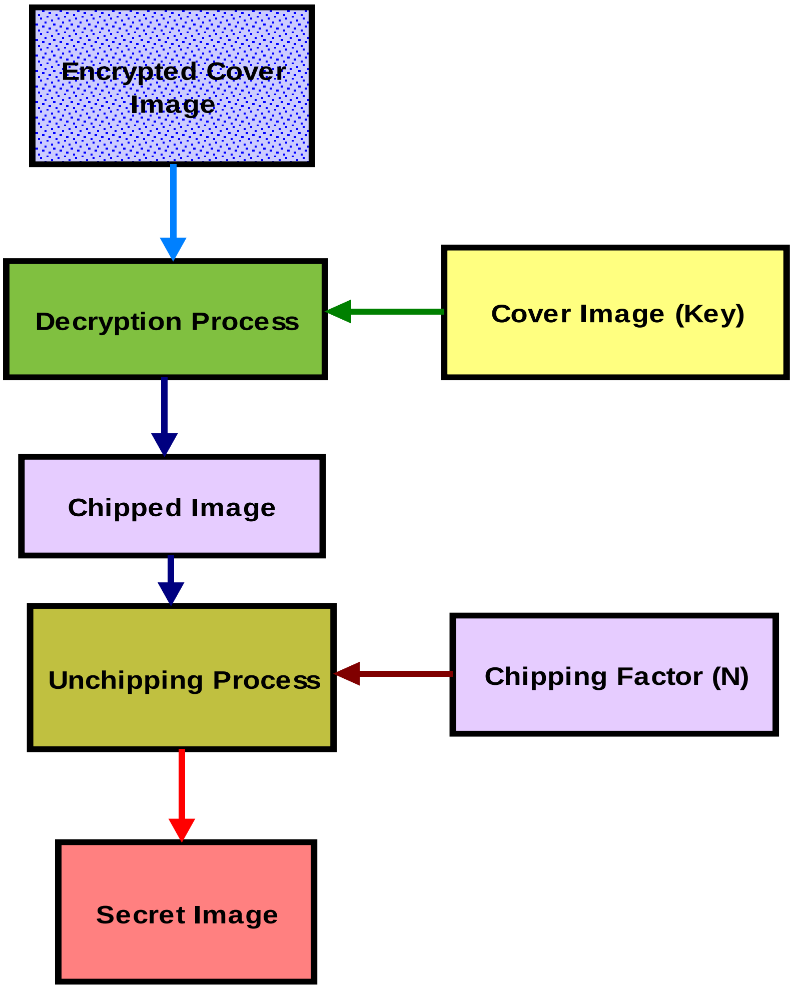

Figure 2. Proposed method for Decryption and Unchipping Process.

4. Results

In this proposed technique we chipped secret image up to N number of times so we get the effect of image quality after image encryption. The proposed algorithm is tested on some of the images from wang database [21], with size of 128×96 (w×h) pixels; total number of pixels are 12288. The Fig. 3 and Fig. 4 shows the forest and bear images respectively.

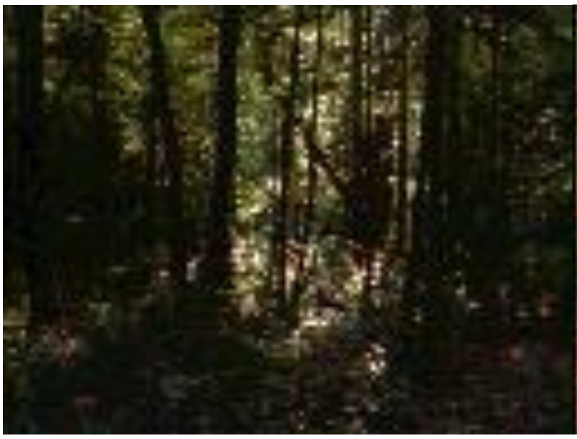

Figure 3. Forest Image

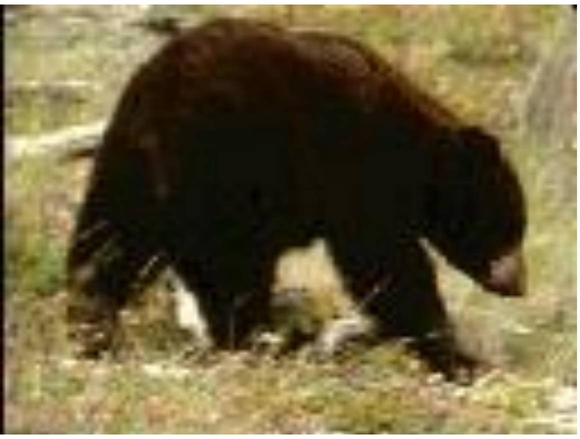

Figure 4. Bear Image

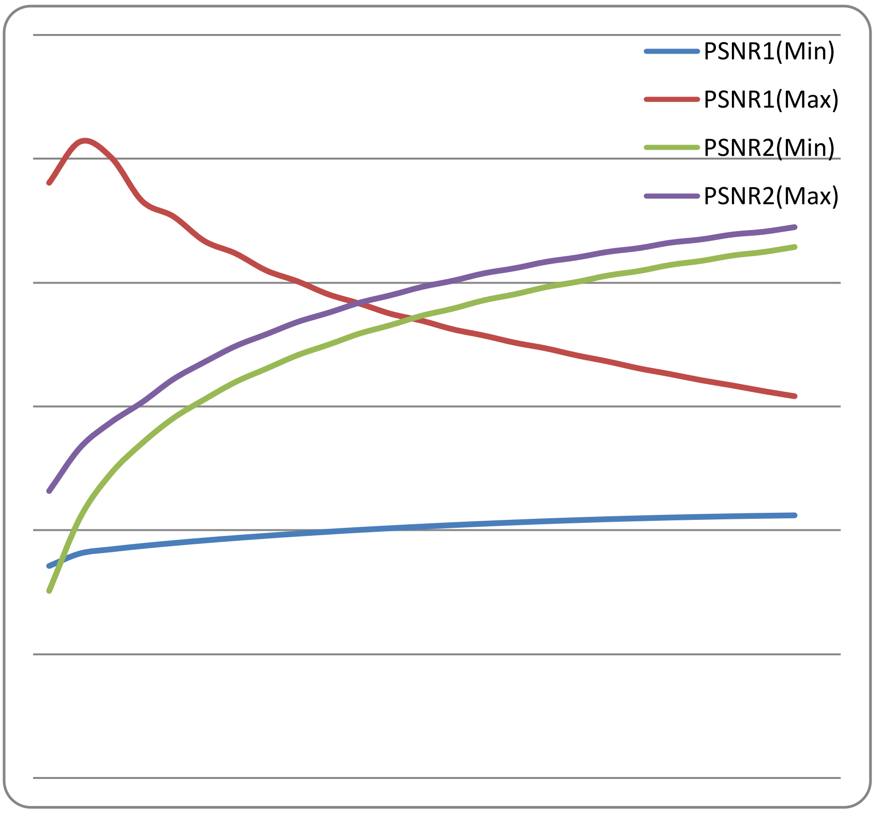

Figure 5. PSNR Plot for Forest Image

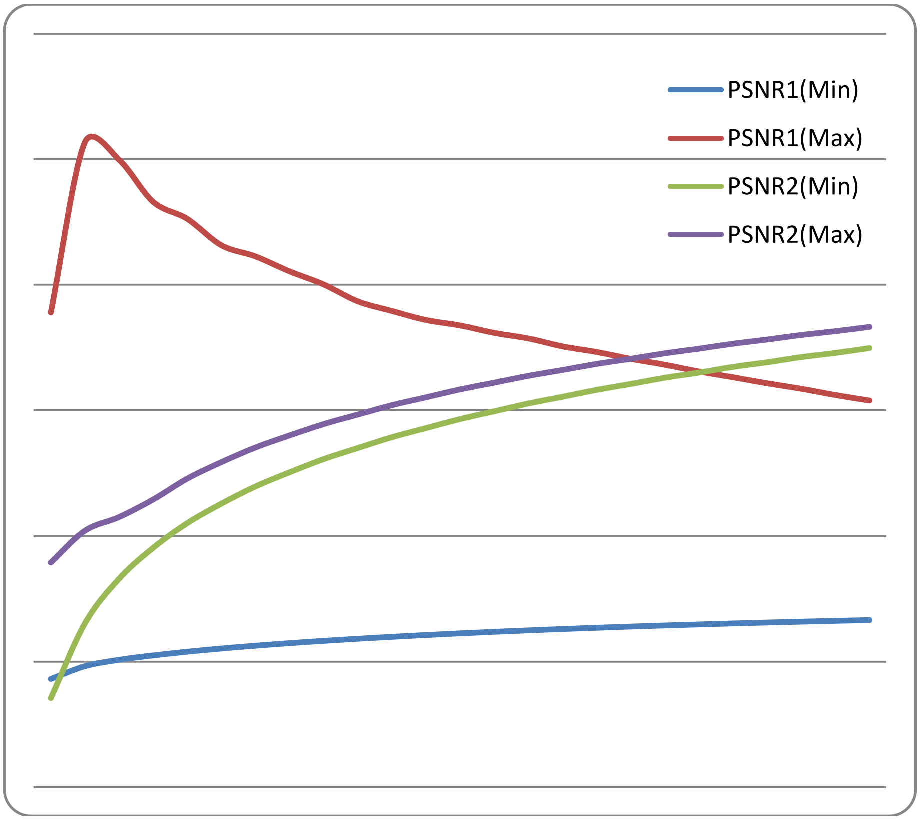

Figure 6. PSNR Plot for Bear Image

5. Discussion

PSNR$_1$ is noise ratio between the secret image and decrypted image. It represents the reproduced quality of the image. It so high in nature and indicate the quality of image but it reduces the visual effect on the encrypted image. So quality of encryption is not so good.

PSNR$_2$ is noise ratio between the cover image and the encrypted image. It is low in nature and indicates that the encryption is good for cover image but the decryption is poor in nature for secret image.

The plots for PSNR$_1$ (Min, Max) and PSNR$_2$ (Min, Max) are shown in Fig. 5 and Fig. 6. There is a gradual improvement in PSNR$_1$ (Min) and PSNR$_2$ (Min, Max), their values increases with increase in chipper effect while PSNR$_1$ (Max) is initially increases and then gradually decreases for chipping and it shows that we need a chipper for better encryption and finally crossover PSNR$_1$ (Min, Max) at different points. They provide as the flexibility for selecting of the values of 'N' for chipper where N varies from 1, 2, 3, 4, …, m. 'm' is integer number. In our method we are tested for N = 1 to 25. It crosses at point which are taken as optimum points where the encrypted and cover image has the equal PSNR ratio.

6. Conclusion

Proposed algorithm is simple and effective. It performs real time fast access. It repels the hacker's attention because of visual image quality similarity. This proposed method is come in symmetric key cryptography in which same key is used by both parties, in this algorithm same cover image is work as key for both sender and receiver.

Limitations of this method is that both parties have same encryption key that is cover image otherwise secret image will not be retrieved. As future work this method is extended over videos.

References

[1] D. Song, D. Wagner and A. Perrig, "Practical Techniques for Searches in Encrypted Data", IEEE Symp. on Research in Security and Privacy, pp. 44-55, 2000.

[2] D. Boneh, G. Crescenzo, R. Ostrovsky and G. Persiano,"Public-key Encryption with Keyword Search", Proc. of Eurocrypt, pp. 506-522, 2004.

[3] A. Swaminathan, Y. Mao, G-M. Su, H. Gou, A. L. Varna, S. He, M.Wu and D.W. Oard, "Confidentiality Preserving Rankordered Search", Proc. of the ACM Workshop on Storage, Security and Survivability, pp. 7-12, Oct. 2007.

[4] R. Datta, D. Joshi, J. Li and J. Z. Wang, "Image Retrieval: Ideas, Influences, and Trends of the new age", ACM Computing Surveys, 2008.

[5] W. Lu, A. Swaminathan, A. L. Varna and M. Wu, "Enabling Search over Encrypted Multimedia Databases", SPIE Media Forensics and Security XI, Jan. 2009.

[6] Abusukhon, A. and Talib, "A novel network security algorithm based on private key encryption", In Proc. Int. Conf. on Cyber Security, Cyber Warfare and Digital Forensic, pp.1119-1224.,March ,2012.

[7] Chan, " A security framework for privacy-preserving data aggregation in wireless sensor networks", ACM Trans. Sensor Networks. 7(5): 1-5, April, 2011.

[8] Chen, G., Mao, Y. and Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps", Chaos Solitons Fractals. 21(3): 749-761, 2004.

[9] Ganeshkumar, K., Arivazhagan, D. and Sundaram, "Strategies of cybercrime: Viruses and security sphere", J. Acad. Indus. Res. 2(7): 397-401, September, 2013.

[10] Guo, Q., Liu, Z. and Liu, "Color image encryption by using Arnold and discrete fractional random transforms in IHS space", Optics Lasers Engg. 48(12):1174-1181, 2010.

[11] Huang, C.K. and Nien, "Multi chaotic systems based pixel shuffle for image encryption", Optics Commun. 282(11): 2123-2127.2009.

[12] Kiran Kumar, M., Mukthyar Azam, S. and Rasool, "Efficient digital encryption algorithm based on matrix scrambling technique", Int. J. Network Security Appl. 2(4): 30-36, 2010.

[13] Lakhtaria, "Protecting computer network with encryption technique: A Study", Int. J. U-E-Serv. Sci. Technol. 4(4): 44-51, 2011.

[14] Liu, Z., Chen, H. and Liu, "Image encryption by using gyrator transform and Arnold transform", J. Elec. Imag. 2(4): 345-351, 1993.

[15] Zaidan, B., Zaidan, A., Al-Frajat, A. and Jalab, "On the differences between hiding information and cryptography techniques: An overview", J. Appl. Sci. 10:1650-1655, 2010.

[16] Zhang, G. and Liu, "A novel image encryption method based on total shuffling scheme", Optics Commun., 284(12): 2775-2780, 2011.

[17] Zhao, X.Y. and Chen, “Ergodic matrix in image encryption”, In Proc. of the 2nd Int. Conf. Image Graphics. 4875: 394-401, 2002.

[18] Zhu, Z.L., Zhang, W., Wong, K.W. and Yu, “A chaos-based symmetric image encryption scheme using a bit-level permutation”, Inform. Sci. 181(6): 1171-1186, 2011.

[19] G. Zhai, W. Zhang, X. Yang and Y. Xu, “Image Quality Assessment Metrics based on Multi-Scale Edge Presentation”, Proceedings of IEEE Workshop Signal Processing System Design and Implementation, Athens, Greece, pp. 331−336, 2005.

[20] C.-L. Yang, W.-R. Gao and L.-M. Po, “Discrete Wavelet Transform-Based Structural Similarity for Image Quality Assessment”, Proceedings of IEEE International Conference on Image Processing, San Diego, pp. 377−380, 2008.

[21] www-db.stanford.edu/~wangz/image.vary.jpg.tar.

[22] Abdelfatah A.Tamini and Ayman M.Abdalla, “Hiding an Image inside another Image using Variable-Rate Steganography”, In Proc. International Journal of Advanced Computer Science and Applications, Vol. 4, No. 10, 2013.

[23] Reshu Choudhary and Arun JB, “Image Encryption for Secure Data Transfer and Image based Cryptography”, In Proc. International Conference on Emerging Trends of Research in applied Sciences and Computational Techniques (ETRASCT’14), 21-22 February, 2014, pp. 173-176.

[24] Reshu Choudhary and Arun JB, “A Secure Image Transmission with Improved Encryption Technique”, National Conference on Recent Advances in Wireless Communication and Artificial Intelligence (RAWCAI’14), 14-15 March, 2014.

[25] Reshu Choudhary and Arun JB, “ Multimedia Content Security using Image Encryption”, In Proc. National Conference on Advances in Technology and Applied Sciences (NCATAS’14), 28-29 March, 2014, pp.79-82 .

[26] Reshu Choudhary and Arun JB, “Secure Image Transmission and Evaluation of Image Encryption”, In Proc. International Journal of Innovative Science Engineering and Technology (IJISET), Vol. 1, Issue 2, April 2014, pp. 65-69.