Literature Survey on Different Techniques of Image Encryption

Mohammad Ali Bani Younes

Abstract— Encryption is used to transmit data securely in open networks. Information contents may be textual data or image data. Encryption of text or images, which cover the highest percentage of the multimedia, is most important during secure transmission of information. There are so many different techniques that should be used to protect confidential image data from unauthorized access. In this paper, literature review of different image encryption and description techniques from 2013 to 2015 have been discussed from which researchers can efficient techniques to be used. Moreover, it provides the various aspects used for the image security.

Index Terms— Cryptography, Image encryption, Image decryption, Security, Ciphers, Symmetric, Blowfish.

1 Introduction

THE presence of communication networks has prompted new problems with security and privacy. Having secure and reliable means of communication with images and video is becoming a necessity, and its related issues must be carefully considered. Hence, network security and data encryption have become important. Images can now be considered one of the most usable forms of information. Image and video encryption have applications in various fields, including wireless communication, multimedia systems, medical imaging, telemedicine, and military communication [1].

As digital imaging plays an important role in multimedia technology, it becoming important to provide security and privacy to the user. Image encryption is very important to protect from any unauthorized user access [2].

Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient. While cryptography is the science of securing data, cryptanalysis is the science of analyzing and breaking secure communication. Encryption is the process of using an algorithm to transform information to make it unreadable for unauthorized users. This cryptographic method protects sensitive data such as credit card numbers by encoding and transforming information into unreadable cipher text. This encoded data may only be decrypted or made readable with a key. Symmetric-key encryption and asymmetric-key encryption are the two primary types of encryption.

Decryption is the process of transforming data that has been rendered unreadable through encryption back to its unencrypted form. In decryption, the system extracts and converts the garbled data and transforms it to texts and images that are easily understandable not only by the reader but also by the system. Decryption may be accomplished manually or automatically. It may also be performed with a set of keys or passwords [3].

Image encryption techniques are different from data encryption techniques. There are several security problems associated with digital image processing and transmission, so it is necessary to maintain the integrity and the confidentiality of the image [4]. Fig. 1 shows a general image encryption process using any image encryption algorithm and the resultant encrypted image.

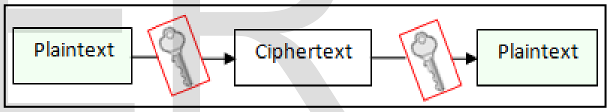

Fig1: Image encryption process

2 Cryptography Goals

This section clarifies the five main goals of Cryptography. These goals are as follows [5,8]:

a. **Authentication** : This process provides the assurance that the communicating entity is the one that it claims to be. It means that, a message has not been modified while in transit (data integrity) and that the receiving party can verify the source of the message.

b. **Secrecy or Confidentiality**: Confidentiality refers to the relationship between two or more persons in which the information communicated between them is to be kept in confidence. It means that, the authenticated users are able to interpret the message content and no one else.

c. **Integrity:** It is the method of ensuring that data is real, accurate and safeguarded from unauthorized user modification.

d. **Non-Repudiation**: It is a process of guaranteeing message transmission that provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.

e. **Availability and Service Reliability**: Availability refers to the ability of a user to access information or resources

Dr. Mohammad Ali Bani Younes, Ajloun National University, Faculty of Information Technology, Department of Computer Science, Jordan,
Email: mohammad_aliyounes@yahoo.com

in a specified location and in the correct format. Secured systems usually get attacked by intruders, which may affect their availability and type of service to their users. Such systems should provide a way to grant their users the quality of service they expect.

3 Block Cypher and Stream Cypher

One of the main categorization methods for encryption techniques commonly used is based on the form of the input data they operate on. The two common types are block ciphers and stream ciphers [6]:

3.1 Block Cypher

A block cipher is one in which a block of plaintext is treated as a whole and used to produce a ciphertext block of equal length. It is an encryption algorithm that encrypts a fixed size of n-bits of data known as a block at one time. The usual sizes of each block are 64 bits, 128 bits, and 256 bits. Ffor example, a 64-bit block cipher takes in 64 bits of plaintext and encrypt them into 64 bits of ciphertext. In cases where bits of plaintext are shorter than the block size, padding schemes are called into play. Majority of the symmetric ciphers used today are actually block ciphers. DES, Triple DES, AES, IDEA, and Blowfish are some of the commonly used encryption algorithms that fall under this group.

3.2 Stream Cipher

It is an encryption algorithm that encrypts 1 bit or byte of plaintext at a time. It uses an infinite stream of pseudorandom bits as the key. For a stream cipher implementation to remain secure, its pseudorandom generator should be unpredictable and the key should never be reused. Stream ciphers are designed to approximate an idealized cipher, known as the One-Time Pad. The One-Time Pad, which is supposed to employ a purely random key, can potentially achieve "perfect secrecy". That is, it's supposed to be fully immune to brute force attacks. The problem with the one-time pad is that, in order to create such a cipher, its key should be as long or even longer than the plaintext. In other words, if you have 500 Megabytes video file that you would like to encrypt, you would need a key that's at least 4 Gigabits long. Clearly, while Top Secret information or matters of national security may warrant the use of a one-time pad, such a cipher would just be too impractical for day-to-day public use. The key of a stream cipher is no longer as long as the original message. Hence, it can no longer guarantee "perfect secrecy". However, it can still achieve a strong level of security.

4 Mode of Operations

There are many different methods of block cipher, where they can be used to strengthen the security of a system. These methods are called the block cipher modes of operations; ECB (Electronic Codebook Mode), CBC (Chain Block Chaining Mode), and OFB (Output Feedback Mode. There are many other modes like CTR (counter), CFB (Cipher Feedback) modes.

5 Symmetric and Asymmetric encryptions

Data encryption procedures are mainly categorized into two categories depending on the type of security keys used to encrypt/decrypt the secured data. These two categories are: Asymmetric and Symmetric encryption techniques [7,8].

5.1 Symmetric Encryption

Symmetric encryption is a form of computerized cryptography using a singular encryption key to guise an electronic message. Its data conversion uses a mathematical algorithm along with a secret key, which results in the inability to make sense out of a message. Symmetric encryption is a two-way algorithm because the mathematical algorithm is reversed when decrypting the message along with using the same secret key. Symmetric encryption is also known as private-key encryption and secure-key encryption. For further clarification, in this type of encryption, the sender and the receiver agree on a secret (shared) key. Then they use this secret key to encrypt and decrypt their sent messages [8]. Fig. 2 shows the process of symmetric cryptography. Node A and B first agree on the encryption technique to be used in encryption and decryption of communicated data. Then they agree on the secret key that both of them will use in this connection. After the encryption setup finishes, node A starts sending its data encrypted with the shared key, on the other side node B uses the same key to decrypt the encrypted messages.

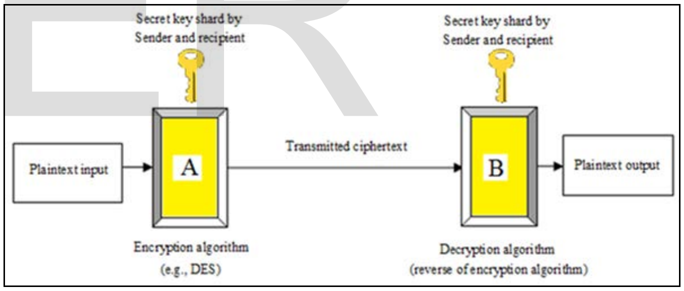

Fig. 2. A simple model of symmetric key encryption (Stallings, 2006).

The main concern behind symmetric encryption is how to share the secret key securely between the two peers. If the key gets known for any reason, the whole system collapses. The key management for this type of encryption is troublesome, especially if a unique secret key is used for each peer-to-peer connection, then the total number of secret keys to be saved and managed for n-nodes will be n(n-1)/2.

The symmetric encryption scheme has five ingredients [9]:

1. **Plaintext**: This is the original intelligible message or data that is fed to the algorithm as input.
2. **Encryption algorithm**: The encryption algorithm performs various substitutions and permutations on the plaintext.
3. **Secret Key**: The secret key is also input to the encryption algorithm. The exact substitutions and permutations performed depend on the key used, and the algorithm will

produce a different output depending on the specific key being used at the time.

4. **Ciphertext**: This is the scrambled message produced as output. It depends on the plaintext and the key. The ciphertext is an apparently random stream of data and, as it stands, is unintelligible.
5. **Decryption Algorithm**: This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext. There are two requirements for a symmetric key cryptosystem
   a. they assume it is impractical to decrypt a message on the basis of the ciphertext plus knowledge of the encryption/decryption algorithm. In other words, they do not need to keep the algorithm secret; they need to keep only the key secret.
   b. Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure. If someone can discover the key and knows the algorithm, all communications using this key is readable.

5.2 ASymmetric Encryption

Asymmetric encryption is the other type of encryption where two keys are used. To explain more, what Key1 can encrypt only Key2 can decrypt, and vice versa. It is also known as Public Key Cryptography (PKC), because users tend to use two keys: public key, which is known to the public, and private key which is known only to the user. Fig. 3 illustrates the use of the two keys between node A and node B. After agreeing on the type of encryption to be used in the connection, node B sends its public key to node A. Node A uses the received public key to encrypt its messages. Then when the encrypted messages arrives, node B uses its private key to decrypt them.

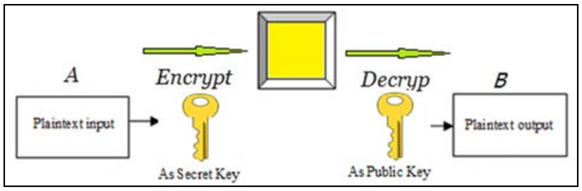

Fig. 3. Asymmetric Encryption

This capability surmounts the symmetric encryption problem of managing secret keys. But on the other hand, this unique feature of public key encryption makes it mathematically more prone to attacks. Moreover, asymmetric encryption techniques are almost 1000 times slower than symmetric techniques, because they require more computational processing power. To get the benefits of both methods, a hybrid technique is usually used. In this technique, asymmetric encryption is used to exchange the secret key, symmetric encryption is then used to transfer data between sender and receiver [8].

6 Literature Survey

1. **Image Encryption based on the RGB PIXEL Transposition and Shuffling** 2013. This paper [10] proposed a technique of transposition and reshuffling of the RGB values of the image in steps, which has proven to be really effective in terms of security analysis. The extra swapping of RGB values in the image file after RGB component shifting has increased the security of the image against all possible attacks that are currently available.
2. **New Image Encryption Technique Based On Combination of Block Displacement and Block Cipher Technique** 2013. In this paper [11], a new image encryption algorithm is proposed. It is already known that security of an algorithm depends on the length of the key. this means that longer keys will always support good security features. The proposed algorithm uses 128- bit key which provided too much security for the proposed algorithm. To access original key or crypto analysis of the proposed key is required 2^{128} time to break the key which is almost impossible for any hacker. There is no chance to generate floating point error because no such types of mathematical formulas have been applied on the proposed algorithm. The correlation co-efficient as well as their entropy values for the proposed algorithm were calculated.
3. **A New Combined Symmetric Key Cryptography CRDDBT Using – Relative Displacement (RDC) and Dynamic Base Transformation (DBTC)** 2013. This paper [12] focused on a new technique of encryption without a predefined key. The input string is fragmented into several parts, with each part encrypted using a different algorithm. Three unique algorithms have been applied to encrypt the fragmented string on the basis of its orientation. For higher security levels, the key is derived from the two differently determined keys. The salient feature of this algorithm is that, a part of string being manipulated using base conversion, the second part of the string is deformed by interchanging position and increasing number of repetitions, and in the remaining elements, they perform simple operations. So, this algorithm was a complex combination without involving any complex calculation.
4. **A Review on Image Encryption Technique based on Hyper Image Encryption Algorithm** 2013. This paper [13] presented a method for image security using block based image transformation and Hyper Image encryption techniques. The original image was divided into blocks, which were rearranged into a transformed image using a transformation algorithm, and then the transformed image was encrypted using the Blowfish algorithm i.e. Hyper Image encryption techniques. Finely, the result showed the correlation between image elements was significantly reduced . Their result also showed that increasing the number of blocks by using smaller block sizes resulted in a lower correlation and higher entropy. In this algorithm there is no key generator. A Hyper Image encryption algorithm was used, which divide the image into a number of blocks. Due to large data size and real time constrains,

algorithms that are good for textual data may not be suitable for multimedia data. In this algorithm the correlation between image elements was significantly decreased.

5. **Image Encryption And Decryption Using Blowfish Algorithm In Matlab** 2013. This paper [14] proposed encryption and decryption of images using a secret-key block cipher called 64-bits Blowfish designed to increase security and to improve performance. This algorithm is used as a variable key size up to 448 bits. It employs Feistel network which iterates simple function 16 times. The blowfish algorithm is safe against unauthorized attack and runs faster than the popular existing algorithms. The proposed algorithm is designed and realized using MATLAB. Hence if the number of rounds are increased then the blowfish algorithm becomes stronger. Since Blowfish does not have any known security weak points so far it can be considered as an excellent standard encryption algorithm.
6. **Comparative performance analysis of Cryptographic Algorithms** 2013. This paper [15] provides a fair comparison between five most common and used symmetric and asymmetric key algorithms: Two fish & Blowfish, IB_mRSA, RSA, RC. A comparison has been made on the basis of these parameters: rounds block size, key size, encryption/decryption time, and CPU process time in the form of throughput. These results show that IB_mRSA is more suitable than other algorithms. Simulation program is implemented using C#.NET programming.
7. **A Study of Encryption Algorithms AES, DES and RSA for Security** 2013. This paper [16] has implemented experiments for three encryption techniques: AES, DES and RSA algorithms and compared their performance based on the analysis of their stimulated time at the time of encryption and decryption. Results of the experiments were used to analyze the effectiveness of each algorithm.
8. **A Review: Image Encryption with RSA and RGB randomized Histograms** 2013. This paper [17] surveyed and analyzed several image encryption and decryption techniques. On the basis of their study the authors were able find the problem formulation as well as analysis, which enabled them to provide future enhancement directions. Based on the above study they provided the following future directions which can be helpful in better detection: 1) Use Powerful encryption technique like DES and RSA. 2) Increase RGB randomization and security key randomization for improving image security. 3) Improve the block size or bit encryption standard like 128 bit and 256 bit. 4) Chaos-based ciphers should not be susceptible to traditional differential and linear cryptanalysis attacks so the use of hybridization is the better possibility.
9. **A Survey On Different Image Encryption and Decryption Techniques** 2013. This paper [18] presented a survey of over 25 research papers dealing with image encryption techniques that scrambled the pixels of the image and decrease the correlation among the pixels, which lowers correlation among the pixel and produces the encrypted image. A survey of different existnig image encryption and decryption techniques was given. Additionally, the paper focused on the functionality of Image encryption and decryption techniques.
10. **Text and Image Encryption / Decryption Using Advanced Encryption Standard** 2014. This paper [19] implemented text and image encryption and decryption using AES. Features of data are depends on its types. Therefore same encryption technique cannot be used used for all types of data. If the Images have large data size and also have problems with real time constrain hence similar method cannot be used to protect images as well as text from unauthorized access. Few variations in method AES can be used to protect image as well as text.
11. **A Secure Symmetric Image Encryption Based on Bit-wise Operation** 2014. This paper [20] proposed a secured encryption technique for digital images; it is equally applicable for any digital file (e.g. text, image and audio etc.). The bit-wise XORing and shifting operation were used to cipher a block of secret bytes and then ciphered bytes were shuffled within N places (N is the size of secret key). This is the combination of substitution and transposition technique performed using dynamic SBOX and TBOX. The key for the proposed cryptosystem is very large which provides better security against brute-force attack. Moreover, key sensitivity analysis, statistical analysis and differential attack analysis prove the high acceptability of the proposed algorithm.
12. **Use of Symmetric Algorithm for Image Encryption** 2014. This paper [21] presented image encryption with DES algorithm which provides more security during the transmission. The proposed idea reproduces the original image with no information loss. They used three different steps: First, the image converted into byte array and then byte array is converted to string, which gets passed for encryption in DES. The resultant final ecrypted image is same as input image. they have discussed the compared study of DES with AES. Their future work involves encryption of text data embedded in image.
13. **A Keyless approach to Lossless Image Encryption** 2014. This paper [22] proposed an improved Keyless approach for image Encryption in lossless RGB images. There are three different approaches being followed in image encryption; key oriented encryption. Image splitting and multiple share. The objective of this work was to increase the security level and to improve the storage capacity with SST techniques. The security level was increased by randomly distributing the pixel bit over the entire image. Using keyless approach, to reversible encryption would be done and to maintain the originality of an image without any loss of quality.
14. **Review: Image Encryption Using Chaos Based algorithms** 2014. This paper [23] introduced different chaotic maps such as Arnold cat map, sine map, logistic map, tent map. Chaotic systems have many applications in image processing such as image compression and image encryp-

tion. Combination of chaos theory with cryptography may provide security of high level. Chaotic are used in image encryption. Two or more maps can also be used in combination. Arnold cat map cannot be efficient alone for image encryption so it must be used with other maps for efficient encryption.

15. **Image Encryption using CAT Mapping and Chaos Approach** 2014. This paper [24] proposed an innovative method which uses Cat mapping to realize the image discretization. The proposed approach uses the periodic changes to achieve the encryption of images. Images with different sizes may use different cycles to encrypt. The experiments show that the encryption approach is able to fulfill the image encryption effectively through drawing the best parameters to achieve the best image encryption effect. The sensitivity analysis implies that, this method is capable of performing well on the image pixel scrambling and replacement. For encrypted security, this proposed method has strong sensitivity to the plaintext which may attribute to handle the plaintext attack under difference situations.

16. **An Ethical Approach of Block Based Image Encryption Using Chaotic Map** 2015. This paper [25] proposed an image encryption algorithm by using chaotic map as it is well known for its Dynamic nature, Randomness and very sensitive towards initial condition. In the proposed algorithm two dimensional chaotic map and the two secrets keys for encryption of an image were used in which first the image was divided into four blocks and then each block of the image was encrypted individually in *n* times, after that the keys are inverted for each block and the process was repeated up to *m* times. The proposed work has been rigorously examined over the prevalent standard test and has encouragingly succeeded to pass most of them like key sensitivity analysis, statistical analysis, differential analysis, entropy analysis, which make the proposed algorithm good enough for real time secure communication.

17. **Image Encryption Algorithm Based on Chaotic Economic Model** 2015. This paper [26] presented a new algorithm of encryption and decryption of images based on a chaotic economic map. this work is the first attempt to apply a chaotic economic map in the construction of chaotic cryptography. All of the simulations and experimental results have shown that the proposed image encryption and decryption algorithm has (1) a very large key space 10^{84}, (2) high sensitivity to all secret keys, (3) information entropy that is close to the ideal value of 8, and (4) low correlation coefficients that are close to the ideal value of 0. Therefore, these results lead to the effectiveness and robustness of the proposed image algorithm. In addition, the results lead to suggest application of other well-known chaotic economic systems such as duopoly and tripoly economic systems.

18. **A new image encryption algorithm based on non-adjacent coupled map lattices** 2015. This paper [27] proposed a new image encryption algorithm which is based on the spatiotemporal non-adjacent coupled map lattices. The system of non-adjacent coupled map lattices has more outstanding cryptography features in dynamics than the logistic map or coupled map lattices does. In the proposed image encryption, they employed a bit-level pixel permutation strategy which enables bit planes of pixels permute mutually without any extra storage space. Simulations have been carried out and the results demonstrate the superior security and high efficiency of the proposed algorithm compared to other algorithms.

19. **A robust image encryption algorithm resistant to attacks using DNA and chaotic logistic maps** 2015. This paper [28] proposed an image encryption technique using DNA (Deoxyribonucleic acid) operations and chaotic maps. Firstly, the input image is DNA encoded and a mask is generated by using 1D chaotic map. Secondl, this mask is added with the DNA encoded image using DNA addition. The intermediate result is DNA complemented with the help of a complement matrix produced by two 1D chaotic maps. Finally, the resultant matrix is permuted using 2D chaotic maps followed by DNA decoding to get the cipher image. The proposed technique is totally invertible and it can resist known plain text attacks, statistical attacks and differential attacks.

20. **A Review on DES, AES and Blowfish for Image Encryption & Decryption** 2015. In this paper [29] the authors discussed and surveyed DES, AES and Blowfish for Image Encryption and Decryption. In today's world it is a crucial concern that while transferring image from one network to another over the internet, the proper encryption and decryption should be applied so that unauthorized access can be prevented. The authors also surveyed related research and did some problem identification and provided suggestions that can be useful for image encryption. This is to enhance the performance and encryption and decryption times of the image.

7 Conclusions

Robust security scheme is essential to store and convey digital images such as important medical images. therefore, Cryptography is very important to provide secrecy and security against statistical attacks and other types of attacks when images are exchanged between two parties on the network. This paper presents a review of survey literature published from 2013 to 2015 in addition to different image encryption/decryption techniques. Each technique is unique in its own way and this makes it suitable for many applications. Everyday new techniques are evolving hence fast and secure conventional encryption techniques sould work with high security rate. This survey provides a way to realize the different aspects that are used for image encryption..

References

[1] E. Fathi et al, "Image Encryption: A Communication Perspective," by CRC Press, Reference - 418 Pages - 232 B/W Illustrations, ISBN

9781466576988 - CAT# K16760, December 14, 2013.

[2] P. K. Das, Mr. P. Kumar and M. Sreenivasulu, "Image Cryptography: A Survey towards its Growth," Advance in Electronic and Electric Engineering, vol. 4, no. 2, pp. 179-184, 2014.

[3] Ayushi, "A Symmetric Key Cryptographic Algorithm," International Journal of Computer Applications," (0975 - 8887) vol. 1, no. 15, pp. 1-4, http://www.ijcaonline.org/, 2010.

[4] M. Bani Younes and A. Jantan, "Image Encryption and Decryption Process Using Block-Based Transformation Algorithm," LAMBERT, October 9, 2011.

[5] J. Katz, Y. Lindell, "Introduction to Modern Cryptography," 2nd edition, Boca Raton : CRC Press/Taylor & Francis, pages 583, 2015.

[6] T. Cusick, Ding, and A. Renvall, "Stream Ciphers and Number Theory Revised edition," Amsterdam : Elsevier, 2004.

[7] M. Ebrahim, S. Khan and U. Bin Khalid, "Symmetric Algorithm Survey: A Comparative Analysis, "International Journal of Computer Applications (0975 – 8887) vol. 61, no.20, January 2013.

[8] S. B. Sasi, D. Dixon, and J. Wilson, "A General Comparison of Symmetric and Asymmetric Cryptosystems for WSNs and an Overview of Location Based Encryption Technique for Improving Security," IOSR Journal of Engineering (IOSRJEN) www.iosrjen.org ISSN (e): 2250-3021, ISSN (p): 2278-8719, vol. 04, Issue. 03, PP. 01-04, (March. 2014.

[9] W. Stallings, "Network Security Essentials: Applications and Standards," Prentice Hall, 2007.

[10] Q. A. Keste, "Image Encryption based on the RGB PIXEL Transposition and Shuffling," I. J. Computer Network and Information Security, 7, in MECS (http://www.mecs-press.org/), DOI: 10.5815/ijcnis.2013.07.05, pp.43-50, Published Online June 2013

[11] K. Kushwah, S. Shibu, "New Image Encryption Technique Based On Combination of Block Displacement and Block Cipher Technique," International Journal of Computer Science and Information Technologies, vol. 4, no. 1, pp. 61 – 65, 2013.

[12] N. Kandele, S. Tiwari, "A New Combined Symmetric Key Cryptography CRDDBT Using - Relative Displacement (RDC) and Dynamic Base Transformation (DBTC)," International Journal of Engineering Research & Technology, vol. 2, Issue. 10, www.ijert.org , October - 2013.

[13] P. Junwale, R. M. Annapurna, and G. Sobha, "A Review on Image Encryption Technique based on Hyper Image Encryption Algorithm," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 11, pp. 614-618, November – 2013.

[14] Pia Singh, Prof. Karamjeet Singh, "Image Encryption And Decryption Using Blowfish Algorithm In Matlab," International Journal of Scientific & Engineering Research, vol. 4, Issue. 7, July-2013.

[15] L. Singh, Dr. R.K. Bharti, "Comparative performance analysis of Cryptographic Algorithms," International Journal of Advanced Research and Computer Science and Software Engineering (IJARCSSE), vol. 3, issue. 11, November 2013.

[16] Dr. P. Mahajan, A. Sachdeva, “A Study of Encryption Algorithms AES, DES and RSA for Security”, Global Journal of Computer Science and Technology Network, Web & Security (GJCSTNWS), vo. 13 Issue. 15 Version 1.0 Year 2013.

[17] G. S. Chandel, P. Patel, "A Review: Image Encryption with RSA and RGB randomized Histograms," International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), vol. 2, Issue 11, November 2013.

[18] R. Pakshwar, V. K. Trivedi, and V. Richhariya, "A Survey on Different Image encryption & Decryption Techniques," International Journal of Computer Science and Information Technology, vol. 4, no. 1, pp. 113-116, 2013.

[19] K. k. R. Saraf, V. P. Jagtap, and A. K. Mishra, "Text and Image Encryption Decryption Using Advanced Encryption Standard," International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), vol. 3, Issue 3, pp. 118-126, May – June 2014.

[20] S. Kaur et al , "A Review of ImageEncryption Schemes Based on the Chaotic Map," International Journal of Computer Technology & Applications,vol. 5, Issue. 1, PP. 144-149, 2014.

[21] K.Brindha, R. Sharma, and S. Saini, "Use of Symmetric Algorithm for Image Encryption," International Journal of Innovative Research in Computer and Communication Engineering, vol. 2, Issue 5, pp. 4401-4407, May 2014.

[22] P. S. Ghode, et al. " A Keyless approach to Lossless Image Encryption, "International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE.), vol. 4, Issue. 5, pp. 1459-1467, May 2014.

[23] A. Gaur et al , "Image Encryption Using Chaos Based algorithms," Int. Journal of Engineering Research and Applications, vol. 4, Issue. 3, ver. 1, pp.904-907, March 2014.

[24] W. Zhu, "Image Encryption using CAT Mapping and Chaos Approach," International Journal of Signal Processing, Image Processing and Pattern Recognition, vol. 7, no. 3, pp.1-8, 2014.

[25] K. Gupta, R. Gupta, R. Agrawal, and S. Khan, "An Ethical Approach of Block Based Image Encryption Using Chaotic Map," International Journal of Security and Its Applications vol. 9, no. 9, pp.105-122, 2015.

[26] S. S. Askar, A. A. Karawia, and A. Alshamrani, "Image Encryption Algorithm Based on Chaotic Economic Model," Hindawi Publishing Corporation, Mathematical Problems in Engineering, vol. 2015, Article ID 341729, 10 pages, 2015.

[27] Y.-Q. Zhang, X.-Y. Wang, "A new image encryption algorithm based on non-adjacent coupled map lattices, "Applied Soft Computing, vol. 26, pp. 10–20, 2015.

[28] A. Jain, N. Rajpal, "A robust image encryption algorithm resistant to attacks using DNA and chaotic logistic maps," Multimedia Tools and Applications, An International Journal, Springer Science + Business Media Ne Yourk, pp. 1-18, February 2015.

[29] A. Devi , A. Sharma, and A. Rangra, "A Review on DES, AES and Blowfish for Image Encryption & Decryption," Aarti Devi et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, vol. 6, Issue. 3, pp. 3034-3036. http://www.ijcsit.com/, 2015.