Volume 5, Issue 12, December 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Survey on Image Encryption Techniques

Garima Tanwar, Nishchol Mishra
SoIT, RGPV University, Bhopal,
India

Abstract—Secure sharing of images in between the various users required phenomenon of image encryption. An efficient image encryption technique is always requisite, such that the users other than the sharing participant cannot recognize the image. Thus, here the technique is always required to keep data secured and resourceful. Cryptography provides indispensable techniques for defensive multimedia data. In the latest study, algorithms based on chaotic map shown proficient image encryption. The paper mainly focuses on the assortments of methods which have been introduced in this domain for providing a competent security for images and framing all these techniques as literature survey. This review also depicts the analysis of image encryption algorithms and confers a comparison among them on the basis of different parameters like imperceptibility, visual degradation, compression friendliness, speed etc.

Keywords—Security, Cryptosystem, Image Encryption Techniques, Chaotic Maps and Chaos.

I. INTRODUCTION

Owing to regular run of digital images in the world over the broadcast media, it has become necessary to secure them from unwanted access. Encryption is a widespread technique to sustain multimedia image security in transmission over the internet. It has used in a variety of fields including internet communication, medical imaging and military communication etc. Due to several inherent features of images like large data redundancy and mass data capacity, the encryption of images differs from that of texts. Therefore, techniques that are appropriate for text data may not be possibly good for multimedia (images, video etc) data.

In order to keep the confidentiality between the users, image encryption techniques endeavor to the conversion of original image into a difficult confused image. The image encryption method should be proposed in such a way that the image changes over into a confused structure (an encrypted image), which again changes back to justifiable structure utilizing decoding operation (an opposite operation of encryption called decryption) and therefore the message is passed on safely. It is noticeable that both these encryption and decryption (unscrambling operations) are guided by particular keys, where the keys may be same or one can be effortlessly achieved from the learning of the other. Such cryptographic strategies are gathered under private key cryptography. In another methodology keys may be different or computationally it may not be doable to assume one key despite the fact that the information of other key is accessible, and such cryptographic routines are known as public key cryptography. It is well known that encryption algorithm should be sensitive to the cipher keys, and the key space should be large enough [1, 2].

A. Features of an Image Cryptosystem

A good information security system should be in a position to not only solely defend a confidential message inside the text kind, meanwhile it should support image kind also. In general there are three basic pillars of any information security systems as follows-

1) Confidentiality-Unauthorized user cannot reveal the secret information.
2) Integrity-Unauthorized users cannot alter or distort the secret information.
3) Availability-Information is invariably offered to licensed users genuinely.

A great image cryptosystem protection mechanism should be flexible as well as it should have high overall performance. Moreover, apart from the above characteristics, the image security systems should also entail the subsequent features

1) The strategies for encryption and decryption should be simple to be completed.
2) The procedure of encryption and decryption of an image must be fast enough so that it cannot degrade system's overall performance.
3) The encryption method must be computationally protected. It requires an extremely lengthy computation time to break keys.
4) Mechanism under the system must be widespread; it should be broadly suitable to layout a cryptosystem like a business product.
5) Flexibility of an encryption and decryption method must be high.[21]

B. Challenges in Image Cryptography

The following challenges are taken into account while encrypting the images:

1) The foremost issue is that similar methods are used to encode image data as for the text. Images are generally represented in 2-Dimensions form. They should be first converted into 1-Dimension form before enciphering. Various encryption techniques can be used and applied on the 1-Dimension. Since the image is large, it is inconvenient to encrypt or decrypt the picture directly.
2) Due to the extraordinary features of an image it becomes tough to apply an encoding scheme on it. The chief feature of an image is that it allows a bit of distortion. A small distortion in the image compression turns the encryption in another way.
3) The size of compressed image is large enough. Thus they cannot be encrypted by the same method as for text. This is also inconvenient to decrease or reduce the size of image before enciphering.
4) The problem also depends on techniques or parameters that are considered as candidate for design of encryption techniques which are good for practical use [21].

Chaos-based algorithms have shown some remarkably good properties in many concerned aspects on the subject of security, complexity, performance, speed etc. The possibility for self-synchronization of chaotic oscillation has sparked an inundation of works on application of chaos in cryptography.

C. Chaos and Cryptography

The shut affiliation among chaos and cryptography makes chaos based algorithm as an accepted candidate for secure transmission. The chaos encoding consider as a smart sensible mechanism because of their decent combination of security, complexity, speed, cheap process overheads and process power etc. The chaos theory is a field of study in mathematics which studies the behavior of dynamical systems. The chaotic maps evolve in time according to set of rules. The rules are generally nonlinear. There may be many interacting variables present in the map. The present condition determines the future continuously [3].

D. Features of Chaotic Maps

The fundamental features of the chaotic maps have engrossed the awareness of cryptographers, as it has many properties like ergodicity, sensitivity to initial condition, nonlinear, deterministic, complex behaviour etc. Most properties are related to some requirements such as mixing and diffusion in the sense of cryptography.
The following are the characteristics of chaotic maps:

1) They are deterministic i.e. they have several mathematical equations or formulation which ruling their behavior.
2) They are sensitive to initial conditions.
3) They are unpredictable and non-linear that is a small change can produce large or huge effects.
4) They appear to be random and disorderly.
5) They usually produce fractal patterns.

What make the encryption algorithms based on chaotic systems more robust and reliable than other algorithms is their complex properties and behaviors. Chaotic systems and cryptographic algorithms they both have some similar properties. Comparison shown in table1 [3-5].

Table 1 Comparison of Chaotic Systems V/S Cryptographic Algorithms.

Chaotic Systems	**Cryptographic Algorithms**
Phase space: set of real numbers	Phase space: finite set of integers
Iteration	Round
Parameters	Keys
Sensitivity to initial condition /control conditions parameter	Diffusion with small change in plain text /key
Mixing	Diffusion with a small change in one point block to whole point
Ergodicity	Confusion
Deterministic dynamics	Deterministic pseudo randomness
Structure complexity	Algorithm complexity

E. Motivation

Today more and more information is being transmitted over the internet. The information is not only text, but also audios, images and other multimedia. Due to the speedy use of images in internet, their security becomes an important factor. Several image encryption techniques have been introduced to secure the images when they travel. However, more extensively we exploit the images, more important their security will be. Image security has become an important topic in the current computer world. Application of image encryption lies under the area of medical, telemedicine, military, multimedia etc.

II. RELATED WORK

1) Xingyuan Wangn et al. [4] devised a chaotic technique which uses R, G, B system to change and encrypt the image. The basic idea is to use a chaotic algorithm which works on the color system. Authors mentioned that traditional cryptographic techniques such as DES, IDES and RSA are no longer suitable for image encryption as the algorithms neglected the correlation between the R, G, B component of images. The combined permutation and combined diffusion stages effectively reduce the correlations between R, G, B components and enhance the performance of encrypting. Proposed algorithm able to work against the resistant of the chosen plain- text/cipher text attack. Finally, the proposed work was performed effectively on color image which was the drawback of the previous technique as they performed simulation on gray scale images.
2) S. S. Askar et al. [5] Described the algorithm in which it creates a chaotic sequence by the CEM map to encrypt the image data. The elements in this sequence consist of decimal fractions numbers while the image consists of pixels. Therefore, a function is required to transfer the fraction decimals to integers. Then, the plain image can be encrypted using the new integer sequence. The work of this paper was first to convert color image to the grayscale image. Calculation of CEM coefficient has been done and then by using CEM values the encryption of image has been performed. They have performed the encryption on the Lena image which is the rough image for operating performance and histogram has been drawn for comparison. Finally, they have performed the simulation, concluded effectiveness and robustness of the proposed image algorithm.
3) A Mitra et al. [6] Described a scheme for the image encryption by utilizing a blend of distinctive permutation techniques. Basically the primary thought of an author is that an image can be seen as a course of action of bits, pixels and blocks. The correlation linking these bits, pixels and blocks presents a clear data of an image. Thus this recognizable data can be lessened by diminishing the relationship among the bits, pixels and blocks by using some permutation technique. A random permutation scheme is performed. They have demonstrated the outcomes with the blend of [block, bit, pixel] permutation individually. The decoded image can be acquired as the original image by having a converse permutation only, or else they get jumbled image. At last, they have finished up their system, the best case scenario and said that the further work will be possible with variable length.
4) H. H. Nien et al. [7] Proposed a fusion encryption procedure for the image security, taking into account the multi chaotic framework which joins Pixel-Chaotic-Shuffle (PCS) and Bit-Chaotic-Rearrangement (BCR).They proposed an encryption mechanism based on chaotic theory because of chaotic system's properties such as non-linear, dynamic and affectability to introductory conditions. Thus the illustrious elements of variables were applied to generate encryption codes for the image. They have worked on the image pixel and the distance between the images pixels. The paper also worked on the various attack methodologies. They provided methods to increase the key space of images, which completely eradicates the outlines of the encrypted images.
5) Chen Wei-bin et al. [8] Proposed a secure system for image encryption using Henon chaotic map. To shuffle the relationship between the original and encrypted image, they applied shuffling on the position of image pixels while changing the gray values of pixels. Former the Arnold map is used to shuffle the positions of the image pixels. Later, they shuffle image pixel by pixel and encryption has been done based on Henon's chaotic system. The proposed scheme significant advantages prevention of the brute force attack. They also mentioned that there is very less encryption time for the image encryption as compared to other.
6) Tiegang Gao et al. [9] Devised a method which work with the shuffle based technique for image encryption. In this work the image matrix is totally shuffled to change the position of pixels in original image. Then to confuse the connectivity of pixels of an encrypted image and original image the blend of two chaotic systems has been used. The algorithm worked with the shuffle generation. The experiment performed by them was on 200*200 dimensional images and histogram was drawn in order to prove their technique's efficiency.
7) Nidhi Sethi et al.[10] Proposed a novel encryption strategy which has two phases. In the former phase the input image is remolded by applying a new alteration method while in the later phase chirikov standard map and enhanced logistic map are used for shuffling the pixels value of an image and diffusion respectively. The aim of enhanced logistic map is to produce a arbitrary series of an image pixels. Numerous images are used to express the efficiency of proposed algorithm. The demonstration shows that the proposed strategy is good to hide the correlation between the original image and cipher image. The result is also compared with two different method, haar wavelet and fast haar wavelet. Finally they concluded it with the security of proposed work towards attacks.
8) Yashpal singh Rajput et al.[11] Projected an encryption technique which has an advanced and enhanced adaptation of existing technique called hill cipher. The grouping of encryption strategy and block based conversion are done to secure image. By accounting such idea to blocks of an image, the correlation between the image's pixels becomes low and to understand the original image becomes hard to cryptanalysis as the quantity of blocks are fixed. Therefore, they conclude that for secure image communication the block size of an image should be small. Utmost 8 blocks are used to separate an image in the proposed strategy.
9) C. X. Zhu et al. [12] Proposed an algorithm using the concept of encryption theory as the encryption is based on a third-order chaotic system in which the theory is defined for the RGB levels of image, because the high security is the character of a high-order chaotic system. They confused the relation between the encrypted image and the original image by means of shuffling the position and varying the RGB levels of each pixel. Finally, they have finished up their system, best case scenario.

10) J. Scharinger et al. [13] In this paper author described a method of encryption based on chaotic Kolmogorov-flow. In this method, the entire image is treated as one block and then key controlled chaotic method is use to perform permutation. In order to confuse the data, a substitution based on a shift-registered pseudo-random number generator is applied, which alters the statistical property of the cipher image. It was advocated that the scheme is computationally secure and superior to contemporary bulk encryption systems when aiming at efficient image and video data encryption.
11) Sesha Pallavi Indrakanti et al. [14] proposed a scheme in which image encryption is based on random pixel permutation which also maintains the image quality. In the algorithm at the place of permutation, visual transformation and value transformation are used. The procedure completed in three different rounds. First, image is divided into blocks then permutation is applied on these blocks. This permutation is applied randomly to reinforce the algorithm. In the next round key is generated by the values which are used in previous encryption round. In last or third round numbering is done on shares which are generated by private image. Then key and shares are send to the receiver. Decryption can be done by using these key and shares at receiver site. Finally the author of this paper mentioned that the effective key generation process and less permutation process to make proposed algorithm more secured.
12) Hossam El-din H. Ahmed et al.[15] Anticipated an encryption technique called "efficient chaos based feedback stream cipher" (ECBFSC).The method consist of logistic map and an external key. Session key concept, dividing key in 8 block used in an encryption process. Their technique's sensitivity to the plain image is also a plus to the security of the proposed ECBFSC. They have performed analysis on feedback mechanism and on Lena image to prove their proposed technique as the best and can be used in real time scenario.
13) Rakesh S et al. [16] proposed an algorithm that breaks the correlation among the pixels position of an image so that the encrypted image can be so differ to recognize. Firstly, entropy of pixel position and pixel value is increased by applying block shuffling and chaotic series correspondingly. Then the original image is divided into blocks and by means of Arnold cat map block based shuffling is performed. Additionally a scrambled image is produced. That scrambled image is again shuffled as a whole. Lastly that image is encrypted by applying chaotic series on it. They concluded that the encrypted image has less correlation coefficient and high entropy by demonstration and analysis.
14) Ismail Amr Ismail et al. [17] introduced a composed mechanism of two chaotic maps and one exterior private key. The proposed method follows a chaos based stream cipher scheme. The original and encrypted image is discriminate on the basis of an external key and maps. Added the private key is enhanced after every pixel is encrypted of an image to maintain the robustness of proposed method.
15) Pratibha S. Ghode et al.[18] introduced a new 'keyless' (without any key) technique for encrypting lossless images. The aim of proposed work is to amplify the security level by arbitrarily distribute pixels bits over the whole image and to perk up the storage capacity of the system .The encryption and decryption algorithm is intended for lossless broadcast of an image. The author tested their technique on some other images which shows good outputs. Finally they conclude by discussing about the advantage of a keyless approach.
16) Lalita et al.[19] proposed a technique, which uses confusion and diffusion for encryption. The diffusion template is created by random number generator based on Gaussian distribution. The technique uses Bakers map and capable of providing the key length of 64 bits although it's length can be extended further.
17) Manish Mishra et al. [20] proposed a technique which uses Chaotic System, Wavelet Transform along with the fingerprint of the image is created by using Hash Function. All is to be transmitted to the receiver. An input image is taken on which encryption technique is applied. The method proceeds by applying the Wavelet Transform. Application of Wavelet Transform converts the image into frequency domain from where we can gather the minute details of the image. Then inverse Wavelet Transform is applied to get the image from frequency domain. Finally the image obtained is an encrypted image. Besides encryption the hash function is applied on the original image to get the fingerprint of the image. The fingerprint of the image is obtained which is used to maintain the integrity of the image.
18) T. Venkata Sainath Gupta et al. [21] proposed the image security technique along with compression. They have proposed an algorithm using chaos on EZW compression technique to provide security along with image compression. Their process of providing image security starts with compressing the image using EZW. The Embedded Zero Wavelet (EZW) is simple and remarkably effective algorithm for image compression which has a property of coding the bits in the order of their importance. The output sequence of EZW is converted to 2-D data and on this 2-D data we apply row and column scrambling algorithm based on chaos. They have chosen chaos logistic map along with EZW compression method for providing security to images. EZW compression is used not only for compression but also for providing the image security making chaos more robust.
19) Xiaojun Tong, et al. [22] proposed work a novel composite 2-D chaos method is introduced. Basically the method exploits two 1-D chaotic functions that switch randomly and this architecture is acclimating as a series generator. Encryption is done by choosing any one 1-D function arbitrarily and applying a permutation on image pixels. 3-D baker scheme is also explain by the authors. They tested the security of proposed encryption by accounting some analysis on method. From distinction of a new compound encryption technique with 2-D baker and DES algorithm they conclude the performance, security and speed of a new encryption technique is better than previous technique.

20) G.A.Sathish et al. [23] present a new encryption technique .They committed to give secured image encryption/decryption strategy by utilizing various circular maps which are based on chaos. Initially a couple of sub keys are generated by the use of chaotic maps. Later the image is encoded by those sub keys and in its change prompts diffusion process .Finally sub keys are created by four diverse chaotic maps. Based on initial/introductory conditions every single sub key will produce some random numbers from different circle of maps. Among those bitrary numbers, a specific number is chosen as a key for the encryption algorithm. Now the input image is first converted into 1-D form by utilizing two methods (raster and zigzag) and then partitioned into sub blocks. At this point, position and value permutation is applied on every binary matrix. At long the receiver uses the similar sub key to decrypt the images.

Table 2 Comparison of different encryption algorithms

Encryption Techniques	Imperceptibility	Visual Degradation	Compression Friendliness	Speed	Cryptographic Security
Image Encryption Algorithm Based on Henon Chaotic System[8]	High	Moderate	Yes	High	High
An Improved cryptographic technique to encrypt image using extended hill cipher[11]	High	High	Yes	Variable	Moderate
Image Encryption Technique Based on Chaotic System and Hash Function[20]	Medium	Moderate	No	Variable	Moderate
Image Security using Chaos and EZW(Embedded Zero Wavelet)Compression [21]	High	High	Yes	Variable	High
Image encryption scheme based on 3D baker with dynamical compound chaotic sequence cipher generator[22]	High	High	Yes	Moderate	High
Image Encryption Based on Diffusion and Multiple Chaotic Maps[23]	High	Moderate	No	Variable	High
Secure Image transmission using in-compression encryption technique[24]	High	High	Yes	Moderate	High
An Approach to Image Compression with Partial Encryption without sharing the Secret Key[25]	High	High	Yes	Fast	Moderate
Selective biplane encryption for secure transmission of image data in mobile environments[26]	High	High	No	Fast	Medium
Techniques for a selective encryption of uncompressed and compressed images[27]	High	High	Yes	Fast	low

III. SECURITY ANALYSIS

A good encryption scheme should resist known attacks. Also the secret key and key space should be larger enough to make attacks unfeasible. The security analysis of different encryption techniques can be done by analyzing techniques under the following parameters. It is based on ideas from the Refs. [28, 29]

A. Key Space

The key space of any security system is basically an augmentation between two procedures. Assuming that if one is diffusion D1 and the other is confusion D2 then the key space of such security system can be given as-

$$S = D1 * D2$$

If 'n' is an iteration time and different keys are used in different iteration then the key space is given as-

$$S = (D1 * D2)^n$$

Thus, the cryptosystem's key space S increases with the rise of parameter space D1, initial-value space D2, or iteration time n.

B. Key sensitivity Analysis

To protect encrypted images from brute-force attacks, a strengthen algorithm should be absolutely sensitive to both encryption and decryption keys. Even a change in single bit of a secret key will cause a completely different output in either the encrypted (ciphered) image or the decrypted (original) image. Key sensitivity analysis should be done in both the phases encryption and decryption.

C. Histogram Analysis

An allotment or distribution of every pixel of an image can be seen by histogram analysis. This analysis signifies the quantity of every pixel at different color intensity level. Histogram of an original image represents the color components of that image whereas histogram of cipher image represents the distribution of pixels uniformly.

D. Statistical Analysis

There are lots of ciphers which can be profitably analyzed by some statistical investigation. Many statistical attacks can be applied on them to recover the original one. Therefore, it is important to make the cipher strong against such attacks. Statistical analysis can be applied on any cipher by performing calculation on histograms, by finding correlation between pixels and by computing correlation coefficient of an encrypted image.

E. Correlation Coefficient Analysis

Sometimes the correlation between the adjacent pixels is high and the correlation between the neighbor's pixels is low corresponding to an encrypted image. It is well understood that the connection correlation between the neighboring pixels of a scrambled/encoded image is more sensible element to recognize the encryption viably of any cryptosystem. Any security system is said to be good, if all the elements of encrypted and original image are absolutely irregular and exceptionally uncorrelated. For highly correlated image the correlation coefficients are almost 1 and for encrypted image the correlation coefficients is almost 0.

F. Encryption Quality

To estimate the quality of the algorithm, the correlation is used. To analyze the strength of an image encryption technique towards differential attacks, time taken analysis is performed. Number of Pixel Change Rate (NPCR) and Unified Average Change in Intensity (UACI) are the methods to observe the result of small change in input image. From these methods consequential correlation among the pixels of original image and encrypted image can be found.

IV. CONCLUSION

In this paper various image encryption algorithms are analyzed. Some algorithms are working on grayscale image whereas other algorithms are working on R,G,B color system which is the latest trend and it is the requirement for image encryption. These encryption algorithms are studied and analyzed well under the different parameters to promote the performance of the encryption methods also to ensure the security proceedings. To sum up, all the techniques are useful for real-time encryption. Each technique is unique in its own way, which might be suitable for different applications. The further work can be done which resist some other attacks by analyzing the capabilities of algorithms.

ACKNOWLEDGEMENT

This research was supported by School of information Technology, RGPV university (State Technological Universities of Madhya Pradesh) Bhopal, India .Sincere thanks to all the faculty members who provided insight and expertise that greatly assisted the research. Thanks to Nitin Kumar Mishra [MTech] and Himadri Soni[MTech] for remarks that greatly enhanced the manuscript.

REFERENCES

[1] V. Bhatt; G. S. Chandel, *Implementation of NewAdvance Image Encryption Algorithm to enhance security of multimedia component*, International Journal of Advanced Technology & Engineering Research (IJATER), vol. 2, no. 4, 2012, pp. 13–20.

[2] A. B. Abugharsa; A. S. B. H. Basari; H. Almangush, A New Image Encryption Approach using The Integration of A Shifting Technique and The AES Algorithm, InternationalJournal of Computer Applications, vol. 42, no. 9, 2012, pp.38–4.

[3] Ljupco Kocarev, Chaos-Based Cryptography: A Brief Overview

[4] Xingyuan Wangn; LinTeng,XueQin, *A novel colour image encryption algorithm based on chaos*, Signal Processing 92 (2012) 1101–1108, 2011 Elsevier.

[5] S. S. Askar; A. A. Karawia; Ahmad Alshamrani, *Image Encryption Algorithm Based on Chaotic Economic Model* Volume 2015, Article ID341729,10pageshttp://dx.doi.org/10.1155/2015/341729.

[6] A Mitra; Y. V. Subba Rao; S. R. M. Prasanna,*A New Image Encryption Approach using Combinational Permutation Techniques*, International Journal of Electrical and Computer Engineering 1:2 2006.

[7] H. H. Nien; W. T. Huang; C. M. Hung, *Hybrid Image Encryption Using Multi- Chaos-System*, 2009 IEEE.

[8] Chen Wei-bin; Zhang Xin, *Image Encryption Algorithm Based on Henon Chaotic System*, 2009 IEEE.

[9] Tiegang Gao; Zengqiang Chen, *Image encryption based on a new total shuffling algorithm*, Elsevear.

[10] Nidhi Sethi; Sandip Vijay, Comparative *Image Encryption Method Analysis Using New Transformed - Mapped Technique*,Conference on Advances in Communication and Control Systems 2013 (CAC2S 2013).

[11] Yashpalsingh Rajput; A K. Gulve,*A Comparative Performance Analysis of an Image Encryption Technique using Extended Hill Cipher*, International Journal of Computer Applications (0975 – 8887) Volume 95– No.4, June 2014

[12] C. X. Zhu; Z. G. Chen; W. W. Ouyang, *A new image encryption algorithm based on general Chen's chaotic system*,Journal of Central South University (Science and Technology) 37 (2006) 1142.

[13] J.Scharinger, *Fast encryption of image data using chaotic Kolmo- gorov flows*, J. Electron Imaging 7 (2) (1998) 318–325.

[14] Sesha Pallavi Indrakanti; P.S.Avadhani,*Permutation based Image Encryption Technique*, International Journal of Computer Applications (0975 – 8887) Volume 28– No.8, August 2011.

[15] Hossam El-din H. Ahmed; Hamdy M. Kalash; Osama S. Farag Allah, *An Efficient Chaos-Based Feedback Stream Cipher (ECBFSC) for Image Encryption and Decryption*, Informatica 31 (2007) 121–129.

[16] Rakesh S; Ajitkumar A Kaller; Shadakshari B C; Annappa B,*Image Encryption Using Block Based Uniform Scrambling and Chaotic Logistic Mapping*, International Journal on Cryptography and Information Security (IJCIS),Vol.2, No.1,March 2012.

[17] Ismail Amr Ismail; Mohammed Amin; HossamDiab,*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.

[18] Pratibha S. Ghode; Abha Gaikwad,*A Keyless approach to Lossless Image Encryption*,International Journal of Advanced Research in Computer Science and Software Engineering 4(5), May - 2014, pp. 1459-1467.

[19] Lalita Gupta1; Rahul Gupta; Manoj Sharma,*Low Complexity Efficient Image Encryption Technique Based on Chaotic Map*,International Journal of Information And Computation Technology.ISSN 0974-2239 Volume 4, Number 11(2014),pp1029-1034.

[20] Manish Mishra; Shraddha Fandi,*Image Encryption Technique Based on Chaotic System and Hash Function*,2014 IEEE International Conference on Computer Communication and Systems(ICCCS '14).

[21] T. Venkata Sainath Gupta; Ch. Naveen; V. R. Satpute; A.S. Gandhi, *Image Security using Chaos and EZW Compression Computation Technology*.ISSN 0974 -2239 Volume 4, Number 11 (2014).

[22] Xiaojun Tong; Minggen Cui, *Image encryption scheme based on 3D baker with dynamical compound chaotic sequence cipher generator*. Signal Processing 89 (2009) 480–491, Elsevier.

[23] G.A.Sathish kuma; Dr.K.Bhoopathy bagan; Dr.N.Sriraa, *Image Encryption Based On Diffusion And Multiple Chaotic Maps*,International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.2, March 2011.

[24] Shaimaa A. El-Said; Khalid F. A. Hussein; Mohammed M. Fouad, *Securing Image Transmission using In-compression Encryption Techniques*, International Journal of Computer Science and Security, Vol. 4, No. 5, 2010, pp. 466-481.

[25] Abdul Razzaque; Dr. Nilesh singh V.Thakur,*An Approach to Image Compression with Partial Encryption without sharing the Secret Key*,IJCSNS International Journal of Computer Science and Network Security, VOL.12 No.7, July 2012.

[26] Martina Podesser; Hans-Peter Schmidt; Andreas Uhl,*Selective bitplane encryption for secure transmission of image data in mobile environments*.

[27] Marc Van Droogenbroeck; Raphaël Benedett,*Techniques for a selective encryption of uncompressed and compressed images*,In Advanced Concepts for Intelligent Vision Systems (ACIVS), Ghent, Belgium, pages 90-97, September 2002.

[28] Shiguo Lian; Jinsheng Sun; Zhiquan Wang,*Security Analysis of A Chaos-based Image Encryption Algorithm*''Department of Automation, Nanjing University of Science and TechnologyNanjing, Jiangsu 210094, P.R China.

[29] Varsha Bhatt; Gajendra Singh Chandel,*Implementation Of New Advance Image Encryption Algorithm To Enhance Security Of Multimedia Component*,international journal of advanced technology & engineering research (ijater).

