ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 2, Issue 5, May 2014

Multimedia Security Techniques

Reena J. Shah[1], Bhavna K. Pancholi[2]

PG Scholar, Electrical Engineering Department, Faculty Of Technology & Engineering, The M.S.University Of Baroda, Vadodara, India[1]

Assistant Professor, Electrical Engineering Department, Faculty Of Technology & Engineering, The M.S.University Of Baroda, Vadodara, India[2]

Abstract : Image, which covers the highest percentage of the multimedia data, its protection is very important. This can be achieved by cryptography. Image encryption plays an important role to ensure confidential transmission and storage of image over internet.It becomes an important issue that how to protect the confidentiality, integrity, and authenticity of image.A real–time image encryption faces a greater challenge due to large amount of data involved. This paper presents a review on image encryption techniques of both full encryption and partial encryption schemes in spatial, frequency & hybrid domains.

Keywords: Cryptography, Encryption, Decryption, Keys, Cipher text ,Plain text, Symmetric key cryptography, Asymmetric key cryptography

I. INTRODUCTION

In today's rapid growth of digital communication and electronic data exchange, many of us communicate in cyber space without thinking for the security of the same. We exchange a lot of our private information and secrets in cyberspace. In today's highly computerized and interconnected world, the security of digital images/video has become increasingly more significant in applications such as pay-per-view TV, confidential video conferencing, medical imaging and in industrial or military imaging systems, online transactions, passwords ,digital signatures legals etc. These applications need to control access to images and provide the means to verify integrity of images. In many cases, such information leakage seriously invades personal privacy, e.g.the malicious spread of photos in personal online albums or patients' medical diagnosis images, and further more it may cause uncountable losses for a company or a nation, e.g. a secret product design for a company or a governmental classified scanned document. However, such convenience could also be used by malicious/unauthorized users to rapidly spread the image information that it may cause uncountable losses for the owner.

II. CRYPTOGRAPHY

Image encryption algorithms attempt to convert original images to other images so that they are difficult to understand in order to keep the image confidentiality between users. The process of coding and transformation of plain text using a digital key into unreadable format is called encryption; while the process of decoding and converting the unreadable text to readable information using a special digital key is called decryption. Plain Text is an image that a sender wishes to transmit to a receiver, on which encryption process is applied. Cipher text is the result of encryption performed on plaintext using an algorithm, i.e encrypted image.

III. CLASSIFICATION BASED ON KEYS

A. Public key /Asymmetric key cryptography

The public digital key utilizes a pair of digital keys. The two-key system enables the parties to communicate more securely. Because the key pair is mathematically related, whatever is encrypted with a Public Key may only be decrypted by its corresponding Private Key and vice versa. The private key is known only to your computer, while the public key is given by your computer to any computer that wants to communicate securely with it. To decode an encrypted message, a computer must use the public key, provided by the originating computer, and its own private key. Although a message sent from one computer to another won't be secure since the public key used for encryption is published and available to anyone, but anyone who picks it up can't read it without the private key.

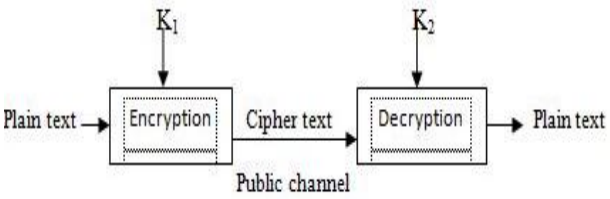

Fig.1. Public key cryptography

B. Private key / Symmetric key

The same digital key is used for encryption and decryption. Sender must send the key to receiver in such a way that no other person can hack it.For this, key sending media must be different than the related encrypted image. i.e.via telephone or mobile or other means.

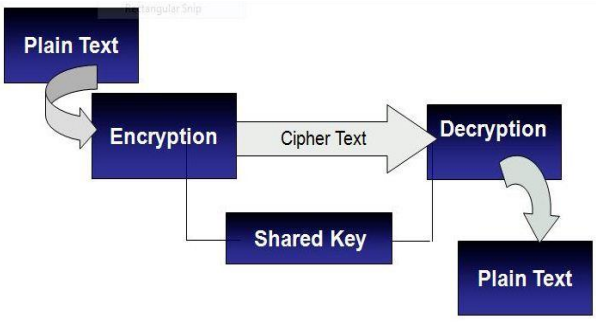

Fig 2.Private key cryptography

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 2, Issue 5, May 2014

C. Hash key

This type of cryptography does not require any digital key as it utilizes a fixed length hash value encrypted into the plain text. The purpose of the hash key is to make sure that the original information is not tampered with. This is a one-way encryption. It uses algorithms to facilitate communication. The hash key normally provides a digital fingerprint, making sure that the file is not corrupted or infected with virus. The hash key also helps computer administrators to encrypt passwords.

IV. ANOTHER CLASSIFICATION APPROACH

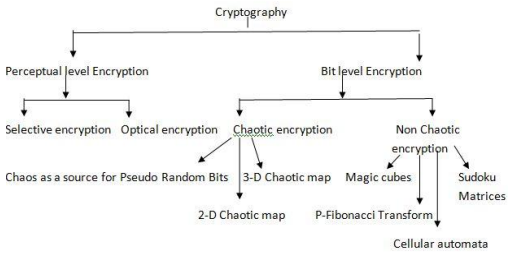

Fig.3. Classification of cryptography techniques

A. Optical Encryption

This group adopts opticsor optical instruments to build physical systems for image encryption,which commonly relies on optics to randomize frequency components in an image. Color Image Encryption Using Double Random PhaseEncoding: Shuqun Zhang and Mohammad A. Karim have proposed a new method to encrypt color images using existing optical encryption systems for gray-scale images. The color images are converted to their indexed image formats before they are encoded. In the encoding subsystem, image is encoded to stationary white noise with two random phase masks, one in the input plane and the other in the Fourier plane. At the decryption end, the color images are recovered by converting the decrypted indexed images back to their RGB (Red-Green-Blue) formats. The proposed single-channel color image encryption method is more compact and robust than the multichannel methods.

Huang Jinga,Zheng, Zhen-zhuc has developed an optical encryption technique for secure real time image transmission. Because any image hold a huge amount of data or information, which results in very less efficiency of the real time image encryption. The authors has proposed a new scheme for image encryption which is used in optical computing technologies that apparently focuses on images and large amounts of data simultaneously, as the result of this high speed is attained. Hence this scheme was implemented by using a stream cipher on the polarization encoder as the optical logic gates. The results states very good security for the images with histogram.

D. Selective Encryption

Selective encryption aims at avoiding the encryption of all bits of a digital image and yet ensuring a secure encryption. The key point is to encrypt only a small part of the bitstream to obtain a fast method.

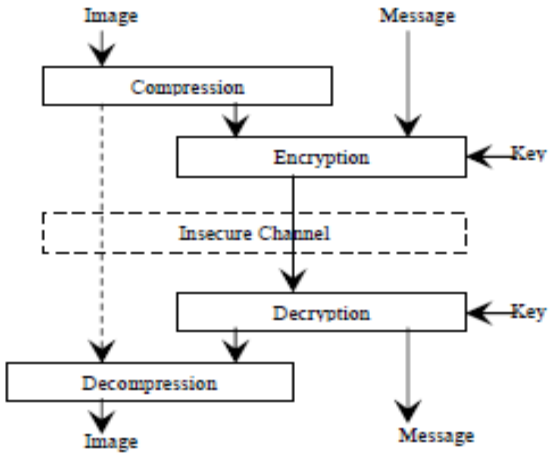

Fig 4.Selective Encryption

Methods for selective encryption proposed include DCT-based methods, Fourier-based methods, SCAN-based methods, chaos-based methods and quadtree-based methods. These methods have to be fast to meet the applications requirements and try to keep the compression ratio as good as without encryption. Several techniques have been proposed for the encryption of DCT based coded image. A method called zig-zag permutation was originated by Tang.Another algorithm, developed by Qiao and Nahrstedtis based on the frequency distribution of pairs of two adjacent bytes in an MPEG bitstream. C. Fonteneau, J. Motsch, M. Babel, and O.D´eforges introduce a hierarchical encryption technique using the compressed bitstream produced by a scalable lossless codec. Encryption is fast and provide a good trade-off between security, visual quality and distortion. Marc Van Droogenbroeckpropose a generalized scheme to selectively encrypt an image. The scheme offers several advantages: flexibility, multiplicity, spatial selectively and format compliance.

E. Chaotic Encryption

A chaotic system has high sensitivities to its initial values, high sensitivities to its parameter, the mixing property and the ergodicity , it is considered as a good candidate for cryptography. The core of digital chaos-based cryptography is the selection of a good chaotic map for a given encryption scheme.The chaotic map used for encryption should have following properties. Mixing property:It is connected with the property of diffusion in encryption algorithms. Suppose the set of possible plaintexts has an initial region in the phase space of the map (transformation), then it is the mixing property that implies scattering out of the influence of a single plaintext digit over many ciphers text digits.

Robust chaos: A good encryption algorithm should spread the influence of a single key digit over many digits of cipher text. The keys symbolize parameters of an encryption algorithm. Therefore, we should imagine about those transformations in which both parameters and variables are concerned in a sensitive way. Parameter set: Larger parameter space of the dynamical system implies that its discriminated version will have larger keys.

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 2, Issue 5, May 2014

Jiun-In Guo and Jui-Cheng Yen have presented an algorithm which was mirror like. In this algorithm there were 7 steps. In the first, 1-D chaotic system is determined and its initial point x (0) and sets k = 0. Then, the chaotic sequence is generated from the chaotic system. After that binary sequence is generated from chaotic system. And in last 4 stages image pixels are rearranged using swap function according to the binary sequence.

Yong-Hong Zhanghas designed and developed an image encryption using extended chaotic sequences. In this study, the chaotic cryptography technique is used which is called a key cryptography. Here, the extended chaotic processes are generated by using the *n* -rank rational Bezier curve. Results shows that the high key space and good security level. Jun Lang, Ran Tao, Yue Wang has proposed an image encryption technique which is based on the concept of multiple parameter discrete fractional Fourier transform and the chaos function. Deng Shaojiang completed an image encryption bya chaotic neural system and the cat map. In this, for making the technique chaos, the neural networks was used.

Huang-PeiXiao ,Guo-jiZang made an algorithm using two chaotic systems . One chaotic system generates achaotic sequence, which was changed into a binary stream using a threshold function. The other chaotic system wasused to construct a permutation matrix.Qais H. Alsafasfeh and Aouda A. Arfoa proposed a new algorithm by adding the Lorenz chaotic system and the Rössler chaotic system. Chong Fu, Jun-Bin Huang, Ning-Ning Wang, Qi-Bin Hou and Wei-Min Lei proposed an improved bit-level permutation approach for chaos-based image cipher with permutation-diffusion architecture. In the permutation stage, a significant diffusion effect is introduced through a 3D cat map-based spatial bit-level shuffling algorithm.

F. Nonchaotic Encryption

Yue Wu have presented image encryption using the Sudoku matrix. Sudoku matrix defines as no two digits in the same block can be aligned in the same row, column or box. Encryption of the image consists of three stages. In first stage, a reference Sudoku matrix is generated and it is used for scrambling process. The image pixels intensities are then changed by using the reference Sudoku matrix values, and then the pixels positions are shuffled using the Sudoku matrix as a mapping process. So using this matrix we can encrypt any digital images such as binary images, gray and RGB images. Logistic map is used to control the size of Sudoku matrix. Yue Wu has proposed a novel Latin square image cipher. It provides a 256 bit key length for generating Latin square and generates 256 x256 square image and it looks like Sudoku matrix, that is no two digit in the same block can be aligned in the same row, column or box .LSIC achieve many desired properties of a secure cipher including a large key space, high key sensitivities, uniformly distributed cipher text, excellent confusion and diffusion properties, semantically secure, and robustness against channelnoise . Yue Wu have presented Sudoku associated two dimensional bijections for image Scrambling.

Yicong Zhou, SosAgaian, Valencia M. Joyner & Karen Panetta present two new image scrambling algorithms based on Fibonacci p-code. One is working in spatial domain, the other is for frequency domain (including JPEG domain). The security keys of our image scrambling algorithms are parameters p and i, and the size of original image. There are many possible choices for security keys so that the scrambled image is difficult to decrypt by unauthorized users, and thus, greater security is guaranteed.

Xiaoyan Zhang, Chao Wang, Sheng Zhong, and Qian Yao, proposed a new image encryption/decryption scheme based on balanced two-dimensional cellular automata.

G. Reversible Cellular Automata Based Encryption

Marcin Seredynski, Krzysztof Pienkoszand Pascal Bouvry presented a new block cipher based on one dimensional, uniform and reversible Cellular Automata is proposed. A class of CA (Cellular Automata) with rules specifically constructed to be reversible is used. The algorithm uses 224 bit key. It is shown that the algorithm satisfies safety criterion called Strict Avalanche Criterion. Due to a huge key space a brute-force attack appears practically impossible.

V. VARIOUS METHODS

A . JPEG Encryption

Osamu Watanabe has jointly developed a scalable encryption method which comprises of backward compatibility with the JPEG2000 Images. This encryption technique tells the encrypted images to hold the multilevel encryption method also decreases the computational complexity of the encryption process. In this paper the standard JPEG 2000 decoder is used to decode the encrypted images and some parameters of JPEG 2000 were saved after the encryption process. As the result of this, the duration of the encryption process is controlled by selective encryption algorithms to promote faster processing.

Analysis on encryption techniques with JPEG Images was done by W. Puech, and J.M. Rodrigues. This paper mainly focuses on the draw backs of both the selective encryption (SE) and the image compression. The SE (selective encryption) can be made by Advanced Encryption Standard *(AES)* algorithm incorporate with the Cipher Feedback (CFB) mode. And for the compression, the JPEG algorithm has been used. Here the SE was done in the stage of Huffman coding in JPEG algorithm which does not affects the size of the compressed image. The results show the application of SE in JPEG compressed images.

B. SCAN

Lossless Image Compression and Encryption Using SCAN : S.S. Maniccam and N.G. Bourbakis have presented anew algorithm which does two works: lossless compression and encryption of binary and gray-scale images. The compression and encryption schemes are based on SCAN patterns generated by the SCAN

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 2, Issue 5, May 2014

methodology. The SCAN is a formal language based 2D spatial-accessing method generate a wide range of scanning paths or space filling curves.

C. Hash Function

Seyed Mohammad Seyedzade, Reza Ebrahimi Ataniand Sattar Mirzakuchaki proposed an algorithm based on SHA-512 hash function, which was novel algorithm. It had 2 sections. Firstly does pre-processing operation to shuffle one half of image and then hash function to generate a random number mask. The mask is then XORed with the other part of the image which is going to be encrypted.

D. Visual Cryptography

Visual cryptography uses the characteristics of human vision to decrypt encrypted images. It needs neither cryptography knowledge nor complex computation. For security concerns, it also ensures that hackers cannot perceive any clues about a secret image from individual cover images. Sen-Jen Lin, Ja-Chen Lin ,Wen-Pinn Fang had introduced Visual cryptography by using Hilbert-curve and two queues. This scheme can generate non-expanded shadows. The Hilbert curve was used to reduce the problem from 2-dimensional image to 1-dimensional binary string, whereas the white queue was use to accumulate enough white pixels (mwhite pixels) so that these m white pixels together could just use one matrix (rather than m matrices) grabbed from C0. The black queue was used for similar purpose in an analogous manner. Stacking our shadows yield image of competitive quality.

C.C. Chang, C.S. Tsai, T.S. Chen suggested that visual cryptography scheme should support wide image format like color and gray scale. Author also argued that random looking shares appear to be suspicious and thus are vulnerable to attacks by attackers in the middle, to fill in this security gap, meaningful shares should be produced.
Y.C. Hou, F. Lin, C.Y. Chang used the binary encoding to represent the subpixels selected for each block and applied the AND/OR operation randomly to compute the binary code for the stacking subpixels of every block in the coverimages. The code ranges from 0 to 255, but it can be even larger depending on the expanding factor. Consequently, a secret image can be a 256 color or true-color one. Analysis on encryption techniques with JPEG Images was done by W. Puech, and J.M. Rodrigues. This paper mainly focuses on the draw backs of both the selective encryption (SE) and the image compression. The SE can be made by Advanced Encryption Standard (AES) algorithm incorporate with the Cipher Feedback (CFB) mode. And for the compression, the JPEG algorithm has been used. Here the SE was done in the stage of Huffman coding in JPEG algorithm which does not affects the size of the compressed image.

VI. SECURITY ANALYSIS

A. Exhaustive Key Search

A secure encryption algorithm should have a large key space. The larger the keyspace, the lesser the attacks on encryption design are . If an algorithm has *k*-bit key, then the exhaustive keysearch needs 2^k trials to break the key. If *k* is 128 bit, then 2^{128} operations are required to discover the correct key.

B. Key Sensitivity Analysis:

A secure cipher should be sensitive to the encryption key. An ideal image encryption procedure should be sensitive with the secret key. It means that the change of a single bit in the secret key should produce a completely different cipher-image. Such sensitivity is commonly addressed with respect to two aspects: Encryption: how different are two ciphertext image C1 and C2 with respect to the same plaintext image using two encryption key K1 and K2, which are different only in one bit. Decryption: how different are two decrypted image D1 and D2 with respect to the same ciphertext image using two encryption key K1 and K2, which are different only in one bit .

H. Histogram Analysis

The ciphertext image histogram analysis is one of the most straight-forward methods of illustrating the image encryption quality. Since a good image encryption method tends to encrypt a plaintext image to random-like, it is desired to see a uniformly-distributed histogram for a ciphertext image.

I. Information Entropy Tests

Although the histogram is very straight-forward to show how uniformly the ciphertext image pixels distribute, one common problem is to tell how good or bad the histogram distributions. Information entropy is a kind of quantitative measurement of how random a signal source is.

$$H(X) = -\sum_{i=1}^{n} \Pr(x_i) \log_2 \Pr(x_i)$$

$$\Pr(X = x_i) = 1/F$$

In other words, the information entropy can be used to measure the randomness of the image as above eq. shows, where X denotes the test image, xi denotes the ith possible value in X, and Pr(x_i) is the probability of X = xi, i.e. the probability of pulling a random pixel in X and its value is x_i. The maximum of H(X) is achieved when X is uniformly distributed as shown in eq.i.e. X has a complete at histogram. Again, symbol F denotes the number of allowed intensity scales associated with the image format.

$$H(X) = -\sum_{i=1}^{n} \Pr(x_i) \log_2 \Pr(x_i)$$

$$\Pr(X = x_i) = 1/F$$

E. UACI and NPCR tests

$$\mathcal{N}(C^1, C^2) = \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{D(i,j)}{T} \times 100\%$$

$$\mathcal{U}(C^1, C^2) = \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{|C^1(i,j) - C^2(i,j)|}{L \cdot T} \times 100\%$$

$$D(i,j) = \begin{cases} 0, \text{ if } C^1(i,j) = C^2(i,j) \\ 1, \text{ if } C^1(i,j) \neq C^2(i,j) \end{cases}$$

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 2, Issue 5, May 2014

The number of changing pixel rate (NPCR) and the unified averaged changed intensity (UACI) are two most common quantities used for evaluating the resistance of differential attacks for an image encryption method/algorithm/cipher. Mathematically ciphertext images C1 and C2, whose plaintext images are slightly different, can be defined as per above two eqs. . The difference function D (i; j) is defined in eq. and denotes whether two pixels located at the image grid (i; j) of C1 and C2 are equal. The symbols T and L denote the number of pixels in the ciphertext image and the largest allowed pixel intensity, respectively. It is noticeable that NPCR concentrates on the absolute number of pixels which changes values in differential attacks, while the UACI focuses on the averaged difference between the paired ciphertext images.

J. Correlation Coefficient Analysis

Correlation is a factor that determines how much two variables are similar to each other. This is commonly used to measure the encryption quality of any cryptography scheme. The correlation coefficient (r_{xy}) is computed as follows:

$$r_{xy} = \frac{Cov(x,y)}{\sigma_x \sigma_y} \quad (1)$$

$$\sigma_x = \sqrt{VAR(x)} \quad (2)$$

$$\sigma_y = \sqrt{VAR(y)} \quad (3)$$

$$VAR(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \quad (4)$$

$$VAR(y) = \frac{1}{N}\sum_{i=1}^{N}(y_i - E(y))^2 \quad (5)$$

$$Cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \quad (6)$$

Where, *x* and *y* are the values of two pixels in the same location in the original and ciphered images, respectively. *Cov(x, y)* is covariance at these pixels. *VAR(x)*and *VAR(y)*are variance values at pixel values *x* and *y* in both the original and the cipher images respectively. $X\sigma$ and $y\sigma$ are standard deviations of both *x* and *y* pixelvalues, *E[.]*is the expectation operator and $N \times N$ is the image dimension.

VII. CONCLUSION

There are various cryptography techniques & sub techniques. Some techniques do partial encryption & the others do full encryption. Some of the methods do image compressions & others do not. Depending on the type of application , speed, bandwidth, confidentiality , security & authenticity extent, one may select type of encryption method. Each & every method has its own merits & demerits. One must think in selecting a proper cipher ,because now cryptanalysis techniques research is under focus. Once a cipher is developed , one must do various security analysis mentioned in the paper.

ACKNOWLEDGMENT

The author would like to acknowledge the support, encouragement & valuable guidance provided by Dr.Sorum Kotia(Associate Professor) & Dr.DharmishthaVishwakarma.

REFERENCES

[1] Lahieb Mohammed Jawad,and Ghazali Bin SulongS.RamaMohan,"A REVIEW OF COLOR IMAGE ENCRYPTION TECHNIQUES"International Journal of Computer Science Issues, Vol. 10, Issue 6, No 1, November 2013.

[2] Abhishek Misra, Ashutosh Gupta, DamodarRai," Analysing the Parameters of Chaos Based ImageEncryption Schemes",World Applied Programming, Vol 1, No 5, December 2011.

[3] BorkoFurht and DarkoKirovski," Multimedia Security Handbook", December 2004.

[4] Y. Wu, J. P. Noonan, and S. Agaian,"Design of Image Cipher Using Latin Squares" Information Sciences ,2014.

[5] John Justin M, Manimurugan S," A Survey on Various Encryption Techniques" International Journal of Soft Computing and Engineering , Vol-2, Issue-1, 2012.

[6] AbhinavSrivastava,"A survey report on Different Techniques of Image Encryption", International Journal of Emerging Technology and Advanced Engineering",Vol 2, Issue 6, June 2012

[7] A. Alfalou1, C. Brosseau2," Optical image compression and encryption methods", Advances in Optics and Photonics 1, 589–636 (2009).

[8] PrakashHongal, Dr.SantoshL.Deshpande," Policy Based Chaotic Cryptography:A Hybrid Approach",International Journal of Emerging Trends and Technology in Computer Science, Vol.1, Issue 3, 2012

[9] Young-Chang Hou," Visual cryptography for color images", Pattern Recognition 36 (2003) 1619 – 1629.

[10] G.S.Nandeesh,P.A. Vijaya, M.V. Sathyanarayana," AN IMAGE ENCRYPTION USING BIT LEVEL PERMUTATION AND DEPENDENT DIFFUSION" International Journal of Computer Science and Mobile Computing, Vol. 2, Issue. 5, May 2013, pg.145 – 154.

[11] MarcinSeredynski, Krzysztof Pienkosz and Pascal Bouvry," Reversible Cellular Automata Based Encryption",International Federation for Information Processing, LNCS 3222, pp. 411-418 2004.

[12] ShiguoLian ,Jinsheng Sun, Zhiquan Wang," A block cipher based on a suitable use of the chaotic standard map", Chaos, Solitons and Fractals, 26 (2005) ,117–129.

[13] AlirezaJolfaei, AbdolrasoulMirghadri , "Image Encryption Using Chaos and Block Cipher", Computer and Information Science Vol. 4, No. 1; 2011

[14] SalehSaraireh, Yazeed Al-Sbou, Ja'afer Al-Saraireh, Othman Alsmadi," Image Encryption Scheme Based on Filter Bankand Lifting",Int. J. Communications, Network and System Sciences, 2014, 7, 43-52

[15] 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 , Vol. 2, Issue 4,2012.

[16] C. Fonteneaua, J. Motschab, M. Babela, and O. D´eforgesa," A Hierarchical Selective Encryption Technique in a Scalable Image Codec",International Conference in Communications, Bucharest : Romania,2008.