AN OVERVIEW ON VARIOUS METHODS OF SECURE PICTURE TRANSMISSION

J. Shaik Dawood Ansari, P. Tamilselvan*

Abstract

Today people are associated with each other through the internet. Various formats of pictures transmitted through the Web for different applications. These pictures contain either secret or private information. To guarantee classification, trustworthiness, confirmation and non-renouncement of pictures during transmission is a significant issue. When transferring the picture over the internet, unauthorized individuals can control the classified information. It creates weakness for its sender. To face the issue as a challenge, enormous techniques are proposed and implemented in which information hiding and picture encryption are the two primary methods. In this paper, various picture security strategies were studied and summed up in an even structure. In this table we have secured different parameters, like fundamental ideas utilized by the creator, kinds of picture, execution assessment parameters, creator's comment about their work and finally our understanding on their work.

Keywords: Cryptography, Image Encryption, Image Decryption, Image Transformation, and Data Hiding

I. INTRODUCTION

The security of pictures is significant due to the huge number of pictures transmitted through the web for different uses, for instance, satellite pictures, clinical imaging frameworks, military databases and administrations, broadcasting, banking, private venture files, and so on. It is ultimate to ensure the privacy of pictures from gatecrashers. To accomplish this, the changing over the first picture to another non-editable structure before sending it by picture encryption or by utilizing information-concealing procedure eliminates the presence of the pictures from the unauthorized person.

At present, various picture encryption techniques are available for unauthorized persons to avoid contact over transmitted pictures. The vast majority of the current encryption algorithms used for content information, but may not be reasonable for picture as result of their huge size and continuous imperatives. Another method forgiving picture security is information covering up. A primary issue of the information covering strategy in pictures is the trouble in embedding a lot of information into a picture. Usually, mystery pictures and a spread picture are similar in size
Using picture change for giving security to a picture during transmission. The data presented in the digital picture happens due to the correlation of two adjoining picture pixels. The detectable data diminished when reducing the pixel correlation using certain change procedures. Various procedures and methods for pictures provide diverse percent of picture security.

To evaluate various assessment factors are available. In order to assess various picture security strategies, the standard assessment parameters like pixels relationship, entropy esteem, Pinnacle Sign to Commotion Proportion (PSNR), Mean Square Blunder (MSE), Histogram investigation, brought together

II. LITERATURE REVIEW

In this paper, we audited not many of the conspicuous existing exploration work to cover all the accessible picture security strategies like, picture change, picture encryption, and image steganography.

Department of CS,
Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu, India
*Corresponding Author

A. Picture Change

In picture change, digital pictures are used as information and produce another picture as a result to upgrade the security level of a picture. The principal picture encryption strategy we have examined in the beneath table is square based picture change [1], [2]. It isolates input pictures into squares, which adjust into a changed picture utilizing their particular change calculation. Their outcomes show that expanding the quantity of squares by isolating pictures into littler squares brings about a lower relationship and higher entropy. Another kind of picture change like Fragmentary Fourier Change (FRFT) and wavelet change [3], [4] shrouded in the accompanying table.

B. Picture Encryption

Picture encryption is the way toward changing over an information picture into another irregular picture that is difficult to comprehend. This should be possible by utilizing key or without key. There are various picture encryption techniques accessible to make transmission of pictures increasingly secure. Various kinds of picture encryption strategies examined beneath.

• Private Key Picture Encryption: Symmetric key encryption and customary encryption are other names of this encryption. Works on resembling key sharing to encrypt the picture then restoring. Therefore, security depends on the length of the key. The sender uses a private key and sends. The receiver uses the resembled key shared to get the original. However, acceptance of the shared key before encryption is vital. Many private key encryption strategies are available. - [5][6] [7]

• Public Key Picture Encryption: It is also called deviated picture encryption. It has dual keys for picture encryption and picture decoding. Works on recipient's open key and when received works on its own private key to access the original image. This method is slower than private key encryption method and so used for huge information encryption. - [8][9]

• Chaos Based Cryptography: It is an investigation of a nonlinear unique framework where disorder indicates the haphazardly. These disorderly strategies are the touchiest parts to starting conditions and other framework factors. Due to affectability, the confused framework acts haphazardly, its high adaptability in the structure of encryption strategy and accessibility of huge number of riotous framework's variations, and various likely encryption keys are the advantages. [10][11]

• Selective Picture Encryption: It is also called fractional picture encryption. The strategy for encoding the segments of a picture alone. The encryption’s execution time is controlled in this method while it scrambles a part of the image simultaneously creating the execution. Constant applications require this sort of method. [12][13]

• Encryption of image along with compression technique: In this method, picture security is achieved using three ways. Compression after encryption, encryption after compression and compression and encryption at the same time. Both used to provide major measures of security and to reduce image size. Various creators have guaranteed various perspectives with respect to the methods of utilizing this consolidated methodology. A few creators did pressure followed by encryption, while others initially encoded the picture, at that point packed. For quick preparing and improved picture security, joint pressure and encryption utilized additionally. [14][15][16][17] [18]

• Visual Cryptography: This approach was proposed by M. Naor and A. Shamir in 1994. Most are utilized for biometric security, watermarking, remote electronic democratic, and so on. Visual cryptography encodes visual data into n straightforward pictures and individuals having all n offers can play out the unscrambling outwardly without

scientific figuring's and furthermore without the assistance of PCs. Any individual having n-1 offers negative uncover data about the first picture. [19][20]

• Keyless approach: This method is intended to beat the restrictions of key located procedures, an instance, calculation, to keep the key records. The keyless methodology of reversible shading picture encryption plotted in the table. [21]

• Image Steganography: It is an information concealing strategy used to ensure mixed media information. It shrouds data inside other data to make it outlandish for any unapproved client to recognize nearness of any mystery data. Steganography utilizes various sorts of hindrances like material, advanced image, or motion picture of digitized pictures are the most famous. It works similar to picture cryptography. The later keeps the cover of a message hidden while the former hides the content. We have broken down and classified different picture steganography approaches [22][23][24] utilized for making sure about pictures.

C. Other Techniques for Security of Images

These days, numerous new strategies for raising the security proposed and steadily new picture security procedure is proceeding. The following table shows the summary of some techniques. [25][26][27][28].

Table-I
Comparative Table Shows Multiple Security Techniques upon Images.

Authors of the proposed techniques: Mohammad and Jantan [1]			
Image utilized for the proposed techniques	***Concept utilized for the proposed techniques***	***Parameters used to evaluate the performance***	***Finding on the technique***
IMAGE TYPE: Bitmap Image IMAGE SIZE: 300x300 pixels IMAGE COLOR:256	CONCEPTS APPLIED: 1. Mixture of square based picture change 2. Blowfish encryption	Correlation and entropy	Table used for transformation seems to be complex.

****Remarks of the Author:***
1. High security level of the encoded pictures contrasted with utilizing the Blowfish alone and brings about lower connection and higher entropy esteem.

2. Upgrading the quantity of squares brought about better picture security

Table-II
Comparative Table Shows Multiple Security Techniques upon Images.

Authors of the proposed techniques: Rathod, Sisodia and Sharma [2]			
Image utilized for the proposed techniques	***Concept utilized for the proposed techniques***	***Parameters used to evaluate the performance***	***Finding on the technique***
IMAGE TYPE: BITMAP (BMP) and Joint Photographic Expert Group (JPEG) IMAGE SIZE: 300x300 IMAGE COLOR:256	1. Encryption method for images. 2. One or more of image permutation techniques. 3. Hyper Image Encryption.	Entropy evaluation, processor and Memory utilization.	Achieved higher entropy compared to [1], efficiency too is higher compared to [1] because of high entropy.

****Remarks of the Author:***
1.Entropy achieved around 70%.
2.Efficiency of image achieved around 80%.
3.Security of image achieved maximum.

Table-III
Comparative Table Shows Multiple Security Techniques upon Images.

Authors of the proposed techniques: Tao, Meng and Wang [3]			
Image utilized for the proposed techniques	***Concept utilized for the proposed techniques***	***Parameters used to evaluate the performance***	***Finding on the technique***
IMAGE TYPE: Grayscale image of Lena IMAGE SIZE: 256x256	1. Image encryption by multi orders of FRFT.	Mean Square Error	Has more security

****Remarks of the Author:***
1. Has a large key space and calculated the number of pixels of the image to double the quantity of keys.
2. Deviate when transforming image decryption due to sensitivity

Table-IV
Comparative Table Shows Multiple Security Techniques upon Images

Authors of the proposed techniques: Chan, and Fekri [4]			
Image utilized for the proposed techniques	***Concept utilized for the proposed techniques***	***Parameters used to evaluate the performance***	***Finding on the technique***
IMAGE TYPE: Grayscale image of Lena	1. Two-round private key wavelet cryptographic system.	Computational complexity	Developing characteristics scope leads to different attacks.

****Remarks of the Author:***
1. Very first application using finite-field wavelets for cryptography.
2. Advanced Encryption Standard gives Equal computational complexity
3. Data Encryption Standard gives Partial computational complexity.

Table-V
Comparative Table Shows Multiple Security Techniques upon Images

Authors of the proposed techniques: Dr. J. A. Jaleel and J. M. Thomas [5]			
Image utilized for the proposed techniques	***Concept utilized for the proposed techniques***	***Parameters used to evaluate the performance***	***Finding on the technique***
IMAGE: Lena – Grayscale Baby – color FORMAT: Portable graphic format (PNG) and Joint Photographic Experts Group (JPEG)	1. Blowfish algorithm – variable key size limits 448 bits	Pixel correlation	The algorithm used is strong and hacking resistant due to 16 rounds of data encryption using function iterating Feistel network.

****Remarks of the Author:***
Better than other algorithms due to variable keys starts from 32 to 448 bits.

Table-VI
Comparative Table Shows Multiple Security Techniques upon Images

Authors of the proposed techniques: N.Kaur and K.Saurabh [6]			
Image utilized for the proposed techniques	***Concept utilized for the proposed techniques***	***Parameters used to evaluate the performance***	***Finding on the technique***
IMAGE: Grayscale image	1. A new algorithm of symmetric image encryption used. 2. One or more chaotic maps and pseudorandom numbers.	Cross Correlation, Entropy, and Histogram Analysis.	Efficient to encrypt real time images in proposed approach.

****Remarks of the Author:***
The approach is capable of ciphering an image.

Table-VII
Comparative Table Shows Multiple Security Techniques upon Images

Authors of the proposed techniques: Nandeesh, Vijaya, and Sathya N [7]			
Image utilized for the proposed techniques	***Concept utilized for the proposed techniques***	***Parameters used to evaluate the performance***	***Finding on the technique***
IMAGE: Grayscale image	Image encryption approach follows on confusion-diffusion design.	Correlation, Histogram analysis, NPCR - Number of changing pixel rate, and UACI - Unified Averaged Changed Intensity.	Stands good against differential attack.

****Remarks of the Author:***
Extended security level using UACI -Unified Averaged Changed Intensity, NPCR - Number of changing pixel rate along with entropy.

Table-VIII
Comparative Table Shows Multiple Security Techniques upon Images

Authors of the proposed techniques: A. M. Jaafar and A.Samsudin [8]			
Image utilized for the proposed techniques	***Concept utilized for the proposed techniques***	***Parameters used to evaluate the performance***	***Finding on the technique***
IMAGE: black and white secret image	1. A low computational public-key image 2. Encryption. Non-expandable visual Cryptography. 3. Boolean operations.	Computational Complexity.	Less computation than other Schemes.

****Remarks of the Author:***
Easy encryption and decryption without complexity in computation.

Table-IX
Comparative Table Shows Multiple Security Techniques upon Images

Authors of the proposed techniques: J.Kushwaha and B.N. Roy [9]			
Image utilized for the proposed techniques	***Concept utilized for the proposed techniques***	***Parameters used to evaluate the performance***	***Finding on the technique***
Every types of images used	1. A public key algorithm. 2. Joining pixel encryption and block encryption.	Correlation and Entropy.	Users are convenient when encrypting and decrypting.

****Remarks of the Author:***
Reduction occurs between image pixels correlation.
Increase in Entropy

Table-X
Comparative Table Shows Multiple Security Techniques upon Images

Authors of the proposed techniques: Jakimoski G and Kocarev L [10]			
Image utilized for the proposed techniques	***Concept utilized for the proposed techniques***	***Parameters used to evaluate the performance***	***Finding on the technique***
Details not available	1. Multiple block encryption. 2. Ciphers followed by chaos using exponential and Logistic maps.	Differential and linear cryptanalysis.	Brute force attack can crack the ciphers.

****Remarks of the Author:***
Ciphers are resistant to known attacks

Table-XI
Comparative Table Shows Multiple Security Techniques upon Images

Authors of the proposed techniques: M. Mishra, P. Singh, and C. Garg [11]			
Image utilized for the proposed techniques	***Concept utilized for the proposed techniques***	***Parameters used to evaluate the performance***	***Finding on the technique***
IMAGE TYPE: color image	1. An image encryption algorithm. 2. Multiple pixel scrambling. 3. Chaotic maps.	Correlation.	Efficient, Real Time technique. Real time transmission.

****Remarks of the Author:***
1. Saves statistical attacks.
2. Saves brute- Force attack.

Table-XII
Comparative Table Shows Multiple Security Techniques upon Images

Authors of the proposed techniques: Sasidharan, Jithin [12]			
Image utilized for the proposed techniques	***Concept utilized for the proposed techniques***	***Parameters used to evaluate the performance***	***Finding on the technique***
IMAGE TYPE: Grayscale	1. Selective encryption. 2. DCT - Discrete Cosine Transform and RC4 - Rivest Cipher 4.	PSNR - Peak Signal to Noise Ratio, Entropy and Histogram analysis.	Image security well provided.

****Remarks of the Author:***
Encrypted images have low PSNR - Peak Signal to Noise Ratio value. Statistical attacks are restricted.

Table-XIII
Comparative Table Shows Multiple Security Techniques upon Images

Authors of the proposed techniques: Bisht & Goswami [13]			
Image utilized for the proposed techniques	***Concept utilized for the proposed techniques***	***Parameters used to evaluate the performance***	***Finding on the technique***
IMAGE TYPE: Red Green Blue (RGB) image	In MATLAB using selective encryption to do easy and fast partial encryption.	Histogram analysis.	Image Security level is average.

****Remarks of the Author:***
1.Implementation is easy using MATLAB.
2.Easy to understand

Table-XIV
Comparative Table Shows Multiple Security Techniques upon Images

Authors of the proposed techniques: Zhou, Liu, Au & Tang [14]			
Image utilized for the proposed techniques	***Concept utilized for the proposed techniques***	***Parameters used to evaluate the performance***	***Finding on the technique***
IMAGE TYPE: Grayscale images Lena: Grayscale Along with multiple images.	ETC system using permutation.	PSNR - Peak Signal to Noise Ratio	Compression efficiency in the approach is slightly worse.

****Remarks of the Author:***
Semantic meaning are destroyed effectively

Table-XV
Comparative Table Shows Multiple Security Techniques upon Images

Authors of the proposed techniques: Razzaque & Nileshsingh [15]			
Image utilized for the proposed techniques	***Concept utilized for the proposed techniques***	***Parameters used to evaluate the performance***	***Finding on the technique***
IMAGE TYPE: multiple standards gray level images FORMAT: BITMAP (BMP), Tag Image File Format (TIFF) & Graphical Interchangeable Format (gif)	Image encryption - Private key. Image compression – Discrete Cosine Technique (DCT).	Peak Signal to Noise Ratio (PSNR) & Coding/decoding time.	Security achieved. Bandwidth fulfilled.

****Remarks of the Author:***
DCT has an 8-compression ratio.

Table-XVI
Comparative Table Shows Multiple Security Techniques upon Images

Authors of the proposed techniques: Kang, Peng, Xu & Cao [16]			
Image utilized for the proposed techniques	***Concept utilized for the proposed techniques***	***Parameters used to evaluate the performance***	***Finding on the technique***
IMAGE TYPE: 8-bit grayscale images	Scalable lossy Compression method.	Peak Signal to Noise Ratio (PSNR).	Encrypted video compression not achieved.

****Remarks of the Author:***
Achieved better performance.

Table-XVII
Comparative Table Shows Multiple Security Techniques upon Images

Authors of the proposed techniques: Dang & Chau [17]			
Image utilized for the proposed techniques	***Concept utilized for the proposed techniques***	***Parameters used to evaluate the performance***	***Finding on the technique***
IMAGE TYPE: Grayscale image	DWT - Discrete Wavelet Transform and DES - Data Encryption Standard.	PSNR - Peak Signal to Noise Ratio and MSE - Mean-Squared Error.	Improved results using Discrete Wavelets Transforms (DWT) with other compression techniques.

****Remarks of the Author:***
Image security enhanced during transmission.
Transmission rate improved

Table-XVIII
Comparative Table Shows Multiple Security Techniques upon Images

Authors of the proposed techniques: Razzaque & Dr. Thakur [18]			
Image utilized for the proposed techniques	***Concept utilized for the proposed techniques***	***Parameters used to evaluate the performance***	***Finding on the technique***
IMAGE TYPE: gray images SIZE: 512×512 IMAGE FORMAT: BITMAP (BMP), Tag Image File Format (TIFF) & Graphical Interchangeable Format (gif)	Image compression. Partial encryption by no sharing secret key.	PSNR - Peak Signal to Noise Ratio & Compression ratio.	Balancing of transmission time.

****Remarks of the Author: Encryption and decryption happened with no sharing secret key.***

Table-XIX
Comparative Table Shows Multiple Security Techniques upon Images

Authors of the proposed techniques: Arce, & Lee [19]			
Image utilized for the proposed techniques	***Concept utilized for the proposed techniques***	***Parameters used to evaluate the performance***	***Finding on the technique***
IMAGE TYPE: Original images Lena and Baboon	VIP - A visual information pixel Sync. Color visual Cryptography Proceeds with Error diffusion.	PSNR - Peak Signal to Noise Ratio	Quality improved.

****Remarks of the Author:***
1.Stores the pixels positions making visual data of original images completely in the color channels.
2.Error diffusion shares pleasant feel.

Table-XX
Comparative Table Shows Multiple Security Techniques upon Images

Authors of the proposed techniques: Wang, Pei, & Li [20]			
Image utilized for the proposed techniques	***Concept utilized for the proposed techniques***	***Parameters used to evaluate the performance***	***Finding on the technique***
IMAGE TYPE: Binary images	An extended tagged visual cryptography (TVC) named LTVC.	Decoded image quality.	Provides better performance.

****Remarks of the Author:***
Semantic meaning are destroyed effectively

Table-XXI
Comparative Table Shows Multiple Security Techniques upon Images

Authors of the proposed techniques: Patil, Nayyar & Ghode [21]			
Image utilized for the proposed techniques	***Concept utilized for the proposed techniques***	***Parameters used to evaluate the performance***	***Finding on the technique***
IMAGE TYPE: Red Green Blue bitmap	Extended no key method for image encryption in lossless RGB images.	Peak Signal to Noise Ratio (PSNR).	No need to maintain the key record decreases high Calculation cost.

Remarks of the Author:
Ensures the Image transmission on lossless.

Table-XXII
Comparative Table Shows Multiple Security Techniques upon Images

Authors of the proposed techniques: Lou & Sung [22]			
Image utilized for the proposed techniques	***Concept utilized for the proposed techniques***	***Parameters used to evaluate the performance***	***Finding on the technique***
IMAGE TYPE: Grayscale	Chaotic asymmetric steganography (CAS). Followed by a chaotic dynamic system & Euler theorem.	Peak Signal to Noise Ratio (PSNR)., and Computational cost.	Protracted to images with color.

****Remarks of the Author:***
No visual artifacts produced.

Table-XXIII
Comparative Table Shows Multiple Security Techniques upon Images

Authors of the proposed techniques: Satish et al., [23]			
Image utilized for the proposed techniques	***Concept utilized for the proposed techniques***	***Parameters used to evaluate the performance***	***Finding on the technique***
IMAGE TYPE: Barbara and multiple images. IMAGE SIZE: 256x256	CSSIS method.	Stego Signal Power. Steganography SNR Embedded. Signal BER Message Payload.	Using 3 keys gets good security.

****Remarks of the Author:***
1. Implementation becomes poor
2. Robustness happens.

Table-XXIV
Comparative Table Shows Multiple Security Techniques upon Images

Authors of the proposed techniques: Feng, Lu, & Sun [24]			
Image utilized for the proposed techniques	***Concept utilized for the proposed techniques***	***Parameters used to evaluate the performance***	***Finding on the technique***
IMAGE TYPE: Bitmap images, few more images	Image steganography method using spatial domain- based binary to minimize distortion occurs when embedding over the texture.	Eld Distortion & Distance-Reciprocal Distortion.	Bitmap images alone are protected well.

****Remarks of the Author:***
Cover images with better qualities even the resembled data length bits embedded.

Table-XXV
Comparative Table Shows Multiple Security Techniques upon Images

Authors of the proposed techniques: Lai & Tsai [25]			
Image utilized for the proposed techniques	***Concept utilized for the proposed techniques***	***Parameters used to evaluate the performance***	***Finding on the technique***
Color images. Document images of Text-type in grayscale.	Secret-fragment-visible mosaic image.	Root Mean Square Error.	To reduce the space complexity target image database needed.

****Remarks of the Author:***
Good for hidden and secret communication.

Table-XXVI
Comparative Table Shows Multiple Security Techniques upon Images

Authors of the proposed techniques: Bouslimi, Coatrieux, Cozic & Roux [26]			
Image utilized for the proposed techniques	***Concept utilized for the proposed techniques***	***Parameters used to evaluate the performance***	***Finding on the technique***
IMAGE TYPE: 100 ultrasound images 200 PET images	Multiple image watermarking. Medical image protection using image encryption.	PSNR - Peak Signal to Noise Ratio and Entropy.	High unpredictability and less strong pressure assault to a lossy picture.

Remarks of the Author:
1.Secures starting and ending images of clinical pictures.
2.Low twisting and high limit accomplished in recovered images.

Table-XXVII
Comparative Table Shows Multiple Security Techniques upon Images

Authors of the proposed techniques: Yang Wu, Lin, & Kim [27]			
Image utilized for the proposed techniques	***Concept utilized for the proposed techniques***	***Parameters used to evaluate the performance***	***Finding on the technique***
IMAGE TYPE: Black & white	Multiple images can be shared using binary matrix functions.	HA – Histogram analysis.	Increased security.

****Remarks of the Author:***
Picture recuperation gets less computational unpredictability.

Table-XXVIII
Comparative Table Shows Multiple Security Techniques upon Images

Authors of the proposed techniques: Sudharsanan [28]			
Image utilized for the proposed techniques	***Concept utilized for the proposed techniques***	***Parameters used to evaluate the performance***	***Finding on the technique***
IMAGE TYPE: Color and monochrome images IMAGE FORMAT: Joint Photographic Experts Group (JPEG)	Shared encryption method for images is a new method. [2]	Computational complexity.	Comes out to a {n, k} imparting plan to less complex extra advance.

Remarks of the Author:
Comes out to some other change or wavelet area strategies for picture coding.

III. CONCLUSION

Acquiring the security of the picture mostly has major issues due to transmission of pictures on the Web. We have reviewed distinctive picture security processes and techniques, which includes basic picture encryption methods. A handful of picture encryption processes and techniques were introduced in the mid-1990s and every strategy is interesting with a particular goal in mind. Certain picture encryption process and technique gives great quality of picture for recipient while other gives degraded pictures, counting that certain picture encryption methods get less handling speed and others have high preparing speed. In this paper, we reviewed various picture encryption strategies in even structure. Various procedures of picture security studied in this paper.

REFERENCES

[1] Mohammad Ali Bani Younes and Aman Jantan, "Image Encryption Using Block-Based Transformation Algorithm", IAENG International Journal of Computer Science, vol. 35, no. 1, pp. 15-23, Feb. 2008.

[2] Hiral Rathod, Mahendra Singh Sisodia, Sanjay Kumar Sharma, "Design and Implementation of Image Encryption Algorithm by using Block Based Symmetric Transformation Algorithm (Hyper Image Encryption Algorithm)", International Journal of Computer Technology and Electronics Engineering, vol. 1, no. 3, pp. 7–13, Dec. 2011.

[3] Ran Tao, Xiang-Yi Meng, and Yue Wang, "Image Encryption with Multiorders of Fractional Fourier Transforms", IEEE Transactions on Information Forensics and Security, vol. 5, no. 4, pp. 734–738, Dec. 2010.

[4] Kevin Sean Chan, and Faramarz Fekri, "A Block Cipher Cryptosystem Using Wavelet Transforms Over Finite Fields", IEEE Transactions on Signal Processing, vol. 52, no. 10, pp. 2975–2991, Oct. 2004.

[5] Dr. J. Abdul Jaleel and Jisha Mary Thomas, "Guarding Images using a Symmetric key Cryptographic Technique: Blowfish Algorithm", International Journal of Engineering and Innovative Technology, vol. 3, no. 2, pp. 196–201, Aug. 2013.

[6] Narinder Kaur and Kumar Saurabh, "An Efficient Image Encryption System", International Journal of Engineering Science and Innovative Technology, vol. 3, no. 4, pp. 139–142, Jul. 2014.

[7] Nandeesh G S, Vijaya P A, and Sathyanarayana M V, "Image Encryption Using Bit-Level Sub Image Blocks Confusion and Circular Diffusion", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 5, pp. 185–193, May 2013.

[8] Abdullah M. Jaafar and Azman Samsudin, "A New Public-Key Encryption Scheme Based on Non-Expansion Visual Cryptography and Boolean Operation", International Journal of Computer Science, vol. 7, no. 2, pp. 1–10, Jul. 2010.

[9] Jayant Kushwaha and Bhola Nath Roy, "Secure Image Data by Double encryption", International Journal of Computer Applications, vol. 5, no. 10, pp. 0975–8887, Aug. 2010.

[10] Jakimoski G and Kocarev L, "Chaos and cryptography: block encryption ciphers based on chaotic maps", IEEE Transactions on Circuits and Systems, vol. 48, no. 2, pp. 163–169, Feb. 2001.

[11] Mayank Mishra, Prashant Singh, and Chinmay Garg, "A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping", International Journal of Information & Computation Technology, vol. 4, no. 7, pp. 741–746, 2014.

[12]Sapna Sasidharan and Jithin R, "Selective Image Encryption Using DCT with Stream Cipher", International Journal of Computer Science and Information Security, vol. 8, no. 4, pp. 268 – 274, Jul. 2010.

[13] Upendra Bisht and Shubhashish Goswami, "Analysis and Implementation of Selective Image Encryption Technique Using Matlab", Journal of Computer Engineering, vol. 16, no. 3, pp.108–111, Jun. 2014.

[14] Jiantao Zhou, Xianming Liu, Oscar C. Au and Yuan Yan Tang, "Designing an Efficient Image Encryption- Then-Compression System via Prediction Error Clustering and Random Permutation", IEEE Transactions on Information Forensics and Security, vol. 9, no. 1, pp. 39–50, Jan. 2014.

[15] Abdul Razzaque & Nileshsingh V. Thakur, "An Approach to Image Compression and Encryption", International Journal of Image Processing and Vision Sciences, vol. 1, no. 2, 2012.

[16]Xiangui Kang, Anjie Peng, Xianyu Xu, and Xiaochun Cao, "Performing scalable lossy compression on pixel encrypted images", EURASIP Journal on Image and Video Processing, 2013.

[17] Philip P. Dang and P. M. Chau, "Image Encryption for Secure Internet Multimedia Applications", IEEE Transactions on Consumer Electronics, vol. 46, no .3, pp. 395–403, Aug. 2000.

[18] Abdul Razzaque and Dr. Nileshsingh 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, Jul. 2012.

[19] In Koo Kang, Gonzalo R. Arce, and Heung-Kyu Lee, "Color Extended Visual Cryptography Using Error Diffusion", IEEE Transactions on Image Processing, vol. 20, no. 1, pp. 132–145, Jan. 2011.

[20] Xiang Wang, Qingqi Pei, and Hui Li, "A Lossless Tagged Visual Cryptography Scheme", IEEE Signal Processing Letters, vol. 21, no. 7, pp. 853–856, Jul. 2014.

[21] Prof. Pragati Patil, Prof.Vinod Nayyar, and Pratibha S. Ghode, "A Keyless approach to Lossless Image Encryption", vol. 4, no. 5, pp. 1459–1467, May 2014.

[22] Der-Chyuan Lou and Chia-Hung Sung, "A Steganographic Scheme for Secure Communications

Based on the Chaos and Euler Theorem", IEEE Transactions on Multimedia, vol. 6, no. 3, pp. 501–509, Jun. 2004.

[23] K. Satish, T. Jayakar, Charles Tobin, and K. Madhavi and K. Murali, "Chaos Based Spread Spectrum Image Steganography", IEEE Transactions on Consumer Electronics, vol. 50, no. 2, pp. 587–590, May 2004.

[24] Bingwen Feng, Wei Lu, and Wei Sun, "Secure Binary Image Steganography Based on Minimizing the Distortion on the Texture", IEEE Transactions on Information Forensics and Security, vol. 10, no. 2, pp. 243–255, Feb. 2015.

[25] I. J. Lai and W. H. Tsai, "Secret-fragment-visible mosaic image—A new computer art and its application to information hiding", IEEE Transactions on Information Forensics and Security, vol. 6, no. 3, pp. 936– 945, Sep. 2011.

[26] Dalel Bouslimi, Gouenou Coatrieux, Michel Cozic, and Christian Roux, "A Joint Encryption/Watermarking System for Verifying the Reliability of Medical Images", IEEE Transactions on Information Technology in Biomedicine, vol. 16, no. 5, pp. 891–899, Sep. 2012.

[27] Ching-Nung Yang, Chih-Cheng Wu, Yi-Chin Lin, and Cheonshik Kim, "Enhanced Matrix-Based Secret Image Sharing Scheme", IEEE Signal Processing Letters, vol. 19, no. 12, pp. 789–792, Dec. 2012.

[28] Subramania Sudharsanan, "Shared Key Encryption of JPEG Color Images", IEEE Transactions on Consumer Electronics, vol. 51, no. 4, pp. 1204–1211, Nov. 2005.