Secure Data Embedding In Images from External Attacks

Vanita J. Dighe, Dr.Baisa L Gunjal

***Abstract*— Most of the times in the data hiding process in images least significant bits of the pixels are used to store the data. And many of the researches are done based on the serial placing of the data bits without estimating the data allocation size. Due to this an irregularity is raised and data may not be hidden properly in the image. So it is a need to estimate the data allocation bits before performing steganalysis by doing reverse engineering. So proposed methodology put forwards an idea of estimating the least significant bits before storing the textual data bits and then these bits are embed into the pixels bytes to perform steganalysis in proper manner. Proposed model exposes to many attacks like image encryption, Image compression and file segmentation. Even though all this proposed model efficiently recovers the hidden data from the image.**

Keywords— Steganography, Image encryption, Image compression and data Segmentation.

I. INTRODUCTION

Image Steganography - Steganography is the technique of concealing a secret message, file, image, video etc. inside another message, file, image, and video. It is a science and art of invisible communication. The term steganography contains two Greek words Steganos and Graphy. It is the method of hiding messages within another data. It is an encryption method that is combined with cryptography to give extra protection technique for hiding data. Cryptography and Steganography are two different techniques. Cryptography is used to make message contents invisible or secret, but Steganography is used to hide the message existence from unauthorized third party. Individually, both these techniques are not much effected or strong in maintaining secrecy of the information. Effectiveness of steganography increases by mixing it with cryptography.

Normally steganography is written in characters containing hash marking but it is also used in image. The steganography protects from unauthorized viewing and from pirating copyrighted materials. It is designed in this way that it is always hidden from unauthorized third party. The two other methods that are closely related to steganography are water marking and fingerprinting. In watermarking all the object instances are marked in a similar way. The information hidden using the watermarking method is normally a signature to signify origin for the copyright protection. In fingerprint technique distinct marks are embedded in different copies of the object carrier that are provided to distinct customers. In fingerprinting and watermarking techniques the secret information hidden in the file may be even visible or may be public knowledge, but in steganography the information imperceptibility is very difficult.

The Steganography contains three essential components: the carrier, message and key. The carrier is anything like mp3, digital image, TCP/IP packet etc. The hidden message is carried by the object. A key is in the form of a password, a pattern or black lights, apply to decipher the secret information.

In today's high tech world the image steganography uses in many applications. In the web world the privacy is the most important concern for many persons. Image steganography permit two users to conveying or send information secretly without any disturbance. Many countries' governments use image steganography technique for transformation of top secret documents between them.

Image Steganography method is divided into two domains: the transform and image. In image domain messages are embedded directly in pixels intensity, but in transform domain the image is first transformed and then the secret message is embedded in the image. Image domain techniques encircle bit-wise method and transform domain techniques involve algorithms manipulation and image transforms.

There are many methods or approaches used to conceal the secret information in images some of them are LSB substitution, Transform techniques and masking & filtering. LSB substitution method modifies the last significant bit of the cover image. Transform method embed the message in the image by modulating coefficients in a transform domain like DCT (Discrete Cosine Transform) utilize in JPEG compression. Masking and filtering methods are most commonly used in gray scale and 24 bit images. This technique hides message by marking an image.

Image Compression - Image compression is the technique to convert or encode an image files in such manner so that the converted files contain less space than the original one. It is the most commercially successful method in the field of digital image processing. The length of the image file becomes less than the original one without degrading or affecting its quality. The Data/ Image compression or codec algorithm is utilized to compress images. These algorithms used distinct method to lower image size like some of the algorithms used technique to split image into distinct and identify parts using fractal, some algorithms determine all same color pixels by color code, name and number of pixel. Algorithms use statistical and visual perception properties to provide the best results. The most standard image compression methods are wavelets, fractal, transform coding, run length coding and chroma sub sampling.

The two common methods of compression in images are lossless and lossy. A Lossy technique, form small image files by discarding surplus image data which are almost invisible to the human eye to detect from the authentic image. The resultant image is closer to the original image, but not the

Manuscript received July 30, 2018

Vanita J. Dighe, PG Scholar , Computer Engineering Amrutvahini College of Engineering, Sangamner, India

Dr.Baisa L Gunjal, Prof and Head, Department of I.T. Amrutvahini College of Engineering, Sangamner, India

duplicate. The JPEG uses a lossy compression technique. Lossless compression used mathematical formulas to compress image, so that the original image integrity is maintained. Techniques used in lossless image compression are Run-length coding, DPCM, Entropy Coding, DEFLATE, Are image compression etc. The GIF uses lossless technique. Compression is the deciding factor in selection of stenographic algorithm. Compression reduces the transmission time by a factor of around 2 to 10 or more.

Image Encryption **-** Encryption is the technique of encoding an information or message in such manner that it is accessed by only authorized parties. It follows a finite set of instruction in the form of the cipher algorithm to convert plain text to cipher text (encrypted form), which can be read again only when decrypted. The Encryption technique uses a pseudo-random encryption key provided by an encryption algorithm. This key is used by authorized users to decrypt encrypted message. There are two types of key uses in encryption technique private key and public key. In private or symmetric key the same keys are utilized for both encryption and decryption. In asymmetric or public key the encryption key is used by anyone but the decryption key access is only given to authorized parties.

Information security is one amongst the foremost necessary factors in data transmission and storage. Images are widely used in distinct process. The protection of image information from unauthorized access is also a vital part of information security. Image encryption is a vital role in data hiding. Image encryption techniques hide the image or secret information contain in the image in an unreadable form. Therefore an unauthorized user or a hacker which does not have encryption key does not read the image in encrypted form. There are many requirements for image encryption technique such as ability to acquire the pixels of encrypted image, encrypted image cannot be hacked easily, faster encryption time, perfected in the decrypted image etc.

In this paper, section 2 is dedicated for literature review of past works. Section 3 describes the proposed methodology and Section 4 discusses the results and evaluation of the proposed technique. Finally Section 5 concludes this paper with future extension possibilities.

II. Literature Review

This section of literature survey eventually reveals some facts based on thought analysis of many authors work as follows.

Ratnakirti Roy, Suvamoy Changder, Anirban Sarkar, & Narayan C Debnath [1] present evaluation of some of the maximum established algorithms for image steganography inside the distinct embedding domains based on the degree of capacity, security and factors which include the statistical belongings of image that they deviate resulting from their embedding mechanism. Based on the records collected through the evaluation, some vital traits of a best steganography system have been put forward and future opportunities of research within the field of image steganography were indexed.

Alvaro Martín, Guillermo Sapiro, and Gadiel Seroussi [2] introduced the impact of applying famous steganography Algorithms on specific statistical models of natural images. On One hand, they determined that a few popular steganography algorithms always bias these facts for a numeral of the most essential models. Then again, the intrinsic variability of these statistics is so high, for the class of images studied that this bias triggered by means of hiding "unnatural" records isn't always sufficient in general to transport the results outdoor of the "natural" variety, except knowledge of the embedding algorithm is to be accessible and exploited. The satisfactory type outcomes have been obtained in the latter case. They observed that these fundamental records of natural images are, in reality, commonly altered by way of the hidden "nonnatural" Information. Regularly, the alternate is always biased in a given direction. However, for the class of natural images taken into consideration, the trade normally falls within the intrinsic variability of the data, and, therefore, does not allow for dependable detection, unless awareness of the facts hiding process is taken into consideration. Within the latter case, tremendous levels of detection are revealing.

Dilpreet Kaur, Harsh Kumar Verma, Ravindra Kumar Singh [3] proposed hybrid technique of steganography, cryptography and compression. The motivation behind their studies is too available a smart image steganography approach which have to be capable sufficient to provide a higher satisfactory stego-picture with an excessive statistic hiding capability. The proposed method is an LSB depended method and stimulated with the innovation of H. B. Kekre in the area of image steganography. Maximum records hiding functionality of proposed method may be evaluated from kekre's algorithm. The proposed technique hides information within the higher LSB bit exclusively when its adjoining LSB bit of all the pixel have frame a bit of secret information to improve stego-image standard. The LZW compression technique is utilizes to optimize the proportions of secret statistics, it's going to allow a private to hide approx 2 times the extra information in a cover-image. This technique is reliable against the RS detection attack and its stego-photograph is totally indistinguishable from the original photograph (cover-photo) via the human eye.

M. Mansour, H. Mouhadjer, A. Alipacha & K. Draoui [4] proposed a comparative evaluation of four images Compression techniques (JPEG, Wavelets, Bandelets and Ridgelets) relevant to images of chromosomes. The interest of this examine is to measure the sensitivity to the Noise of those techniques when coping with the contour and Texture of various types of items within the image. This Synthesis and from the outcomes, proves that the studied elements (compression ratio, processing period, coding error and Signal noise ratio) have an attribute effect on each other. This suggests that the choice of the end result converges to an optimal compromise. Promising outcomes are received.

Jianmin Jiang [5] presents new options for lossless photograph compression where the entropy coding is implemented to the wavelet transform coefficients as opposed to pixels. The Advantage of using wavelet remodel prior to entropy Coding is that the statistical properties of the resulting Coefficients can be analyzed and exploited before the model is installed for mathematics coding. Experiments display that the proposed set of rules achieves competitive performances to that of JPEG.

Yuhan Hai Ying [6] introduce the key to image data compression is extracting primary feature data consisting of aspect and mutation part of the image signal. To enhance the performance of image data compression based totally on

lifting wavelet, the 2 lifting levels, which include prediction and update can comprehend the information Separation from high frequency to low frequency. Biorthogonal wavelet transform is used for Image decomposition the wavelet coefficients are extracted with multi-scale in distinct frequency bands, the region, size and the corresponding relationship to mutations point for module most of wavelet coefficients are all decided. The Compression process is stopped till the image, sign can be about reconstructing from those feature fact, Image feature extraction and records compression are found out subsequently. The simulation suggests that the lifting wavelet is absolutely capable for image facts compression.

S.P.Raja, Dr. A. Suruliandi [7] presents the comparison between the results of exclusive wavelet-based totally image compression methods. The outcomes of distinct wavelet functions, quantity of Decompositions, filter orders, compression ratios and image contents are tested. The effects of the above methods EZW and WDR are as compared by way of using two parameters together with PSNR and MSE points from the recreated image. These Compression algorithms offer a better performance in image quality at low bit rates. These methods are efficaciously tested with lots of images. The EZW set of rules is coupled with the power of multiresolution analysis, yields good sized compression with little quality loss. Due to the Inherent multiresolution nature, wavelet-based coders facilitate revolutionary transmission of image thereby permitting variable bit quotes. The above algorithms may be utilized to compress the photo that is used in the net packages. WDR approach provides high PSNR and less MSE values whilst examines to EZW technique. The mathematics, coding with WDR algorithm might be added in the future.

XiHong [8] presents the DCT-based totally image compression standard in the subjective and the unbiased two evaluation techniques. The DCT quantization coefficients option is important to have an effect on the standard of static photograph compression, the more numbers of Coefficients are surrendered, the bigger quantity is compressed, however the image standard become worse. For the left coefficients quantity, the choice that mistakes threshold is 15 % is more perfect, and the rest of the 85 % plots may be not noted, it's not having an effect on the subjective standard of the image compression. Further Comparing the DCT compression image standard in objective Evaluation approach, with the image compression coding bit rate increasing, the MSE reduces, PSNR also progressively rises, the compression photograph quality becomes better gradually. When the bit rate is lower than 0.75bbp, the image quality is excellent from the subjective and the objective assessment, on the identical Time the image compression percentage and compression standard accomplished balance, it may meet considerable majority applications, so it's the most applicable.

Tao Wang, Dongmei Li, Chunkuang Tao, Haiquan Shi [9] introduced the idea of optical wavelet transform and the light path method. They found out by way of the use of 4f optical record processing technique. Optical wavelet transforms Features high conversion rate because it used the parallel evaluation of optical elements. And it's used extensively in Imaginative structures like image feature extraction, pattern recognition, etc. They examined the necessities of optical methods in image compression depend on optical wavelet transform. The necessities are specifically about the performance of the light-path method, light source, filter and Optical elements. And some advanced measurements are put forward according to present issues. First, the method of figuring out focuses of lens and a way to use Talbot impact to discover the object plane and spectrum plane are given. To reduce chromatic aberration and noise in optical wavelet transform use of reflecting 4f system is recommended. The spatial light modulator and Liquid crystal light valve is adopted to give strength to flexibility and practicability. They examine the merits of the use of white light information processing technique for image Compression.

Hemlata Agrawal, Dimple Kalot, Ankita Jain, Narendra Khatri [10] presents the comparative analysis of the gray scale image Encryption method and greater awareness of safety control of the majority information (i.e. image) switch in the most secure manner. This will provide authentication for person ethical code, accuracy and protection of images that's travelling over the net at the same moment as image based information require greater effort in the course of encryption & decryption. The maximum proposed structure for encryption and decryption is advanced with the same objective of an image the usage of appropriate user described key. There are numerous techniques with the aid of which image can be encrypted and decrypted to confirm the security. They use the Discrete Linear Canonical and Discrete Fractional Transform for image encryption and decryption.

Huiben Zhang, Sm Min Liu, Min Gao, Mengmeng Zhang [11] introduces the chaotic image encryption set of rules studies based totally on Contourlet transformation. Firstly, they introduce the idea of the CT Transformation. Secondly, they introduce the designated Experimental steps of the set of rules. Finally, they experiment the proposed algorithm using Matlab Simulation. They analyzed the experimental results of the algorithm depend on the histogram, adjacent pixels Correlation, and key sensitive its security indexes. As compared with regular chaotic image encryption set of rules, this Algorithm is combining CT transformation and hyper-chaos structural upgrade the security of the encrypted image.

M. Amr Mokhtar, Sameh N. Gobran and El Sayed A M El Badawy [12] proposed an algorithm for color image encryption and decryption. They implement the proposed algorithm using the chaos method and vernam cipher OTP implemented using strings of DNA. Encryptions of the two phases are done in two manners. The first stage is encrypted by utilizing two functions logistic maps to convert the statistical quality, pixels image value and location. The second phase uses one time pad encryption to change the significance of the pixels image to take over the prior stage to find the encrypted algorithm.

Liu Bo, Liu Na,Li Jianxia, Liang Wei [13] proposed the improved image encryption algorithm depend on chaotic sequences using the best qualities of chaotic signals, merge with pixel position scrambling technique and grey value alternative. The proposed algorithm has the big key space and it is hard to decipher.

Shengan Zhou [14] proposed the structure of the digital image encryption depend on the framework of cellular neural network and depend on the attributes of the alternative image grouping size. They introduce the group encryption algorithm depend on the feistel structure. In every round, the cell of

neural network blocks one encrypted image data using a block encryption algorithm.

III PROPOSED METHODOLOGY

The proposed methodology of secure data embedding in the images which is unaltered by the external attacks can be narrated with the following description as mentioned with the below steps.

Step 1: This is the primitive step of the proposed model where Proposed model accepts the image of any format and a textual data to hide in the image. The Textual data is converted into the byte array to hide into the image. In this step the input image pixels are read into the form of byte array and this process yields an image byte array.

After converting the input text and the image into byte array, then image byte array is analyzed for each and every bytes to check the least significant bits (LSB) . Generally in the image based on the different color channels different byte formations are existed. For example , RGB color channel takes 3 bytes, Alpha,RGB takes 4 Bytes per pixel, HSV takes 3 bytes per pixels . After the evaluation of the number of the least significant bits in the image each bits are being labelled in the byte array to estimate the amount of bytes can be set into the image.

Once the amount bytes are within the estimated bytes of the given textual data, then the data is adding into the image byte array to get the enhanced byte array for the given respective image. And then the image is stored in the .png format as this format is efficiently holds the enhanced byte array of the image easily unlike JPEG and other format. These steps are following in the reversed order to get the textual data from the encoded image in the end. The proposed model can be shown in the below algorithm 1.

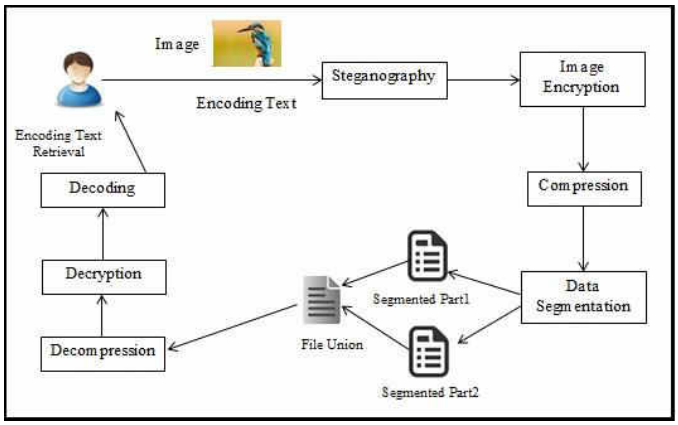

Figure 1: Proposed Sytem Overview

ALGORITHM 1: STEGANOGRAPHY

//Input : Image I and text T
//Output: Steganographed image I_S
1: Start
2: Read I into Byte Array B_A
3: **For** i=0 to size of B_A
4: **IF** $B_A[i] \neq 8$
5: $T_{set[0]} = i$, $T_{set[1]} = 1$
6: add T_{Set} to C_L
[C_L = Labeled cluster]
7: **End For**
8: Read T into Byte Array T_A
9: k=0
10: **For** i=0 to size of C_L
11: $T_{set} = C_{L[i]}$
12 : **IF** $T_{set[1]} == 1$
13: IN= $T_{set[0]}$
14: $B_{A[IND]} = B_{A[IND]+} T_{A[k++]}$
15: END IF
16: END FOR
17: Write B_A into I_s
18: **return** I_s

Step 2: Here in this step Steganographed image is accepted as the input and then it is subjected to image encryption process where the bytes of the image is tend to apply exclusive operations. And this operation is supported with the bytes of the key that is being used to encrypt the image.and this process can efficiently shown in the below algorithm 2. and the reversal of this process yields the decrypted image without any loss of data.

ALGORITHM 2: IMAGE ENCRYPTION

//Input : Image I_S and key K
//Output: Encrypted image E_I
1: Start
2: $R_K \rightarrow fK(SHA1)$
[Generate Random key]
3 : Read I into Byte Array B_A
4: **For** i=0 to size of B_A
5: $B_{A[i]} = B_{A[i]} \wedge R_K$
6: IF $B_{A[i]R} > 255$
7: $B_{A[i]R} = 255$
8: IF $B_{A[i]G} > 255$
9: $B_{A[i]G} = 255$
10: IF $B_{A[i]B} > 255$
11: $B_{A[i]B} = 255$
12: **End For**
13: Write B_A into E_I
14: **return** E_I

Step 3: Compression - Once the image is encrypted then it is subjected to the compression process, Where compression is done based on the Huffman encoding structure to create a symmetric tree of the file bytes. Once the symmetric tree is created, then they are conjugated to form in a single tree format to reduce the size of the file. Then these bytes which are in the tree data structure are alligned in the linear array to write in desired extension to compress the file. The reversal of this process eventually yields the decompresion of the data in losseless form.

Step 4: This is the step where the compressed image file is taken into the account, then all the file bytes are stored in an array. Then this array is segregated into two halves to split and store in two different split files.

To union the same split files are considered and then the bytes are joined to form a single byte array to get the unioned file.

Finally, this unioned file is decompressed , Decrypted and then it is decoded to get the original text that was encoded before the attack is being done.

IV RESULTS AND DISCUSSIONS

The proposed model of secure data embedding in the images is deployed in windows machine. Machines are Java enabled, which uses JDK above version 8.0. Proposed model uses Netbeans 8.0 as IDE and MYSQL as database.

The Proposed model is subjected to different performance evaluation process which are discussed as below.

4.1 Encryption Time performance:

Proposed model is subjected to encryption performance time evaluation and it is compared with the Error Clustering and Random permutation (ECRP) [15] System with our model of Byte Replacement Approach. So as a result of this we get the following results which is plotted in the below graph.

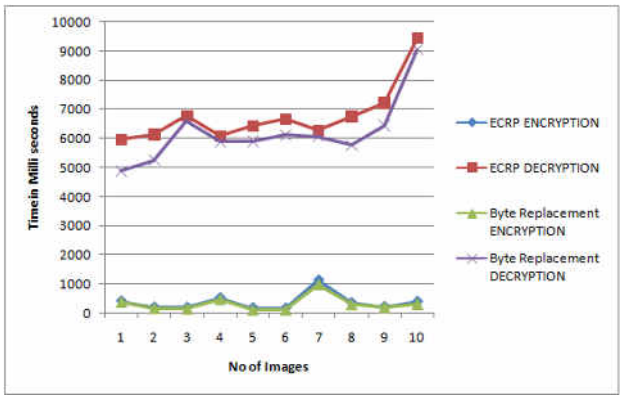

Figure 2:Encryption and Decryption performance Time

The above plot clearly indicates that our approach of Byte replacement technique clearly over performs in the encryption performance time .

4.2 Compression Time performance:

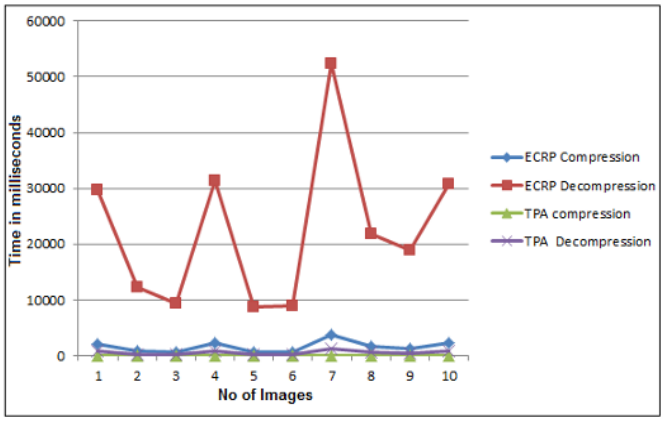

Figure 3: Compression and Decompression time Ratio Comparisons

The above plot clearly indicates that our approach of Tree pattern Access (TPA) compression scheme clearly over performs in the compression and decompression performance time .

V. CONCLUSION AND FUTUREWORK

The proposed model of enhancing the data embedding technique in the images measures the least significant bits and then these bits are analyzed to keep the textual data. Once these textual data is kept then the bytes are normalized as they were earlier to make the whole data invisible. The proposed model embed the data so finely that even it cannot be break by many of the attacks like Encryption at bit level, Compression and even the segmentation of the image in byte format.

This shows the firmness of the embedding data into the image and its stability to retrieve the same on performing of different attacks.

As the future scope proposed model can be enhanced to work in efficient web paradigm and in mobile applications. Proposed model can be used to provide live password authentication schemes to ensure the more security of the passwords and OTPs.Proposed model can be develop as the readymade API which helps the other developers too to build their system of steganalysis.

ACKNOWLEDGMENT

It gives me great pleasure in expressing thanks and profound gratitude to my project guide Dr.B.L.Gunjal and project coordinator Prof.S.K.Sonkar for her valuable guidance and continual encouragement throughout the project work. I am heartily thankful both for her time to time suggestion and the clarity of the concepts of the topic that helped me a lot during this work. It gives me immense pleasure to thank Dr.M.A.Venkatesh, principal, Amrutvahini College of Engineering and Prof. R.L.Paikrao, Head of the Computer Engineering Department, Amrutvahini College of Engineering for his co-operation and suggestions throughout the work.

I would like to thank my teachers for their encouragement, Guidance, Understanding and Support.

REFERENCES

[1] Ratnakirti Roy, Suvamoy Changder, Anirban Sarkar, & Narayan C Debnath, Evaluating Image Steganography Techniques: Future Research Challenges, DOI:978-1-4673-2088-7/13, IEEE, 2013.

[2] Alvaro Martín, Guillermo Sapiro, and Gadiel Seroussi, Is Image Steganography Natural, IEEE Transactions, DOI: 057-7149, Dec, 2005.

[3] Dilpreet Kaur, Harsh Kumar Verma, Ravindra Kumar Singh, "A Hybrid Approach of Image Steganography". ICCCA, ISBN: 978-1-5090-1666-2, IEEE, 2016.

[4] M. Mansour, H. Mouhadjer, A. Alipacha & K. Draoui, Comparative analysis on image compression techniques for chromosome images, Journal of Applied Social Psychology, DOI: 978-1-4799-0251-4/13, IEEE, 2013.

[5] Jianmin Jiang, "Lossless Image Compression with Wavelet Transform", Department of Computer Studies, Loughborough University.

[6] Yuhan Hai Ying, "The Image Compression Research on the Preprocessing Technology of Lifting Wavelet Transform", DOI: 978-1-4244-8845-2/10, IEEE, 2010.

[7] S.P.Raja, Dr. A. Suruliandi, "Performance Evaluation on EZW & WDR Image Compression Techniques",, DOI: 978-1-4244-7770-8, IEEE, 2010.

[8] XiHong, "Research on DCT -based Image Compression Quality", DOI: 978-1-4244-9793-5/11, IEEE, 2011.

[9] Tao Wang, Dongmei Li, Chunkuang Tao, Haiquan Shi, "Research of Image Compression Based on Optical Wavelet Transform", DOI: 1-4244-0342-1/06, IEEE, 2006.

[10] Hemlata Agrawal, Dimple Kalot, Ankita Jain, Narendra Khatri, "Image Encryption using Various Transforms-A Brief Comparative Analysis", DOI: 978-1-4799-5202-1, IEEE, 2014.

[11] Huiben Zhang, Sm Min Liu, Min Gao, Mengmeng Zhang, "Chaotic Image Encryption Algorithm Research Based On Contourlet Transformation", DOI: 978-1-4673-8266-3, IEEE, 2015.

[12] M. Amr Mokhtar, Sameh N. Gobran and El Sayed A M El Badawy, " Colored Image Encryption Algorithm using DNA Code and Chaos Theory ", DOI:10.1109,ICCCE, 2014.

[13] Liu Bo, Liu Na, Li Jianxia, Liang Wei, "Research of Image Encryption Algorithm Base on Chaos Theory", DOI: 978-1-4577-0399-7, IEEE, 2011.

[14] Shengan Zhou, "Image Encryption Technology Research based on Neural Network", DOI: 10.1109/ICITBS.2015.119, IEEE, 2016.

[15] [12] Jiantao Zhou, Xianming Liu, Oscar C. Au, 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, JANUARY 2014 39