Biosc.Biotech.Res.Comm. Special Issue Vol 13 No 13 (2020) Pp-58-66

BBRC
Bioscience Biotechnology Research Communications

Secured Image Transmission Using Color Transformation Fragmented Mosaic, Chaos Based Encryption and LSB – Mapping Steganography Technique

Y Manjula[1]* and K B Shivakumar[2]
[1]*Department of Electronics & Communication Engineering, Sri Siddhartha Institute of Technology, Tumakuru, Karnataka, India.*
[2]*Department of Electronics and Telecommunication Engineering, Sri Siddhartha Institute of Technology, Tumakuru, Karnataka, India*

ABSTRACT

In information technology environment most of the organizations are depending largely on digital services by cloud computing for data base resource management. This needs the transmission of sensitive data to the database servers present in cloud .Therefore the primary concern is for secure data transfer and control access. The proposed method mainly focus on secure network communication of image data base. The secret image is first encrypted in to a meaningful Mosaic encrypted image using fragmented tiles and selected target image. Applying the Color transform to mosaic encrypted image improves the quality of Mosaic image look like Target image. Discrete wavelet transform is then applied to this Mosaic encrypted image to decompose the image in to approximate and information components. The information components are then encrypted by using Chaos based encryption algorithm. The chaos Encrypted image along with approximate components combined and combined image is then hidden in a cover image by using Improved LSB-mapping Steganographic technique. The Mosaic encrypted image is meaningful cipher which camouflage the intruder and secondly the chaos encryption algorithm produces a cipher which gives good amount of confusion and diffusion. Also two bits of double encrypted cipher image is hidden in each pixel of cover image. The proposed algorithm is a combination of both cryptographic and steganography techniques becomes a comprehensive approach to critical data protection from discovering and monitoring.

KEY WORDS: CHAOS ENCRYPTION, FRAGMENTED MOSAIC IMAGES, LSB –MAPPING.

INTRODUCTION

Currently, large number of images are used as sources of confidential data which is communicated through internet. In most of the applications such as personal online photo graphs, military image data base, data storage systems, medical image etc., (Prabu, S et al. 2019)

Hiding techniques hide the existence of confidential message itself. This is possible if the secret data (audio, video, and image) is hided in cover media. Then the cover media is sent in transmission network. Existing methods mostly utilise substitution techniques listed by C. K. Chan and L. M. Cheng (2004), modifications in histograms defined by Z. Ni, Y. Q. Shi, N. Ansari, and W. Su,(2006) , prediction error expansion mentioned by J. Tian,(2003) et al., Y. Hu, et al., (2008) used Difference –Expansion , V. Sachnevet al., (2009) use predictive error improved adaptive predictive error used by X. Li, B. Yang, and T.

ARTICLE INFORMATION

*Corresponding Author: manjulayerva@ssit.edu.in
Received 28th Nov 2020 Accepted after revision 25th Jan 2021
Print ISSN: 0974-6455 Online ISSN: 2321-4007 CODEN: BBRCBA

Thomson Reuters ISI Web of Science Clarivate Analytics USA and Crossref Indexed Journal

NAAS Journal Score 2020 (4.31)

*Online Contents Available at: http//www.bbrc.in/
Doi: http://dx.doi.org/10.21786/bbrc/13.13/9*

Zeng (2011) and wavelet transforms used by W. Zhang, X. Hu et al., (2013) or J. Fridrich (2001) and W.-H. Lin et al., (2008) uses discrete cosine transforms. The main issue of hiding techniques is embedding the large amount of data in cover media without degrading the quality of cover media.

The encryption methods along with hiding techniques gives more security to image data. Encryption is implemented when user privacy is necessarily to be protected. Two main approaches used to develop encryption techniques are non-chaos methods and chaos methods. Also the encryption techniques can be implemented on complete payload image or selected part of payload image. In band width limitation applications encryption techniques can be either combined with compression techniques or non-compression techniques.

Chaotic encryption mainly depends on theory of chaos which describes the behaviour of some nonlinear dynamical systems. The nonlinear dynamical systems exhibits dynamics that are highly sensitive to initial conditions under certain restrictions. The behaviour of chaotic systems appears to be random as a result of this sensitivity. The change in initial conditions results in exponential growth of errors in chaotic systems. Even though the chaotic systems are deterministic, in the sense that their future dynamics are well defined by their initial parameters, the random behaviour occurs and there are no random factors involved. Sensitive dependence on its initial parameters, a chaotic dynamic system is a deterministic system that apparently reveal chaotic behaviour and can never be defined with infinite precision.

The behaviour of chaotic system is random and so it look like noise. Using the chaotic system in cryptographic algorithms for encryption makes a chaos based encryption algorithm, a natural suitor for secure cryptographic communication. Chaotic maps and cryptographic algorithms have similar characteristics such as susceptibility when change in initial parameters and conditions, long periods with unstable periodic orbits, and pseudo random behaviour. The cryptographic algorithms uses permutation and substitution tables for repeated iterations of encryption which leads to sufficient amount of confusion and diffusion to raise the performance of the algorithm. Whereas iterations in chaotic maps cover entire phase space by initial conditions.

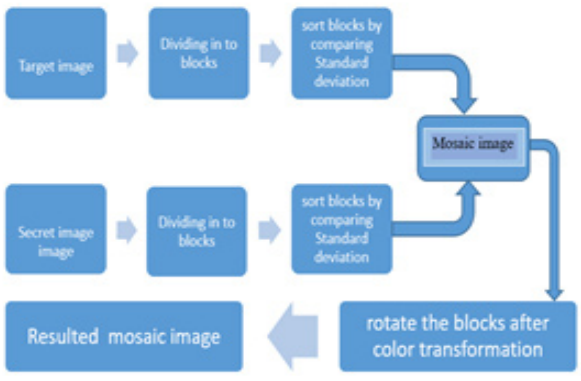
The initial conditions of chaotic maps are used to represent the key of encryption algorithms. The principle difference between the chaotic maps and cryptographic algorithms is that the chaotic maps are defined only for real numbers whereas encryption algorithms are defined for finite sets; The performance of cryptographic algorithms escalate with use of chaotic theory in cryptographic security mentioned by C.-H. Hsu (2004) in his book. In the proposed algorithm, a target and a pay load images are selected. Then both images are fragmented in to tiles for comparison. Threshold values are set for comparison in all directions. All the tiles of payload images are compared with target image tiles. Then encryption is performed based on similarity values.

The encrypted image is named mosaic encrypted image which again go through Color transformation to enhance the image quality. The mosaic encrypted image will be similar to target image. Discrete wavelet transform is applied to this mosaic encrypted image to decompose the image in to detailed and approximate components. The information component of the image is then encrypted by using Chaos based encryption algorithm. The Encrypted information are embedded in to a cover image by using Improved LSB-mapping Steganographic technique. The mosaic encrypted image is meaningful cipher which camouflage the intruder and secondly the chaos encryption algorithm produces a cipher image which gives good amount of confusion and diffusion. Also two bits of chaos encrypted cipher image is hidden in two LSBs bits each pixel of cover image.

2. Conceptual Knowledge Used For Proposed Method

Mosaic Technique: Choose an appropriate target image similar in background Color information with respect to secret information that needs to be communicated in a covert way. If the dimension of the target and payload image is not equal then resize the payload in accordance with host medium image by using simple arithmetic coding technique. The arithmetic encoding method is the most popular technique to reduce information of the payload secret images if the dimension of the secret images are large in size when compared to that of size of cover images stored in pre-existing data base.

Figure 2.1: Mosaic image creation



Both of these images are fragmented into divided blocks of similar dimension. The size of the fragmented blocks could be 4x4, 8x8, 16x16, 32x 32 etc. After fragmentation, mean and standard deviation feature of each of this fragmented block is calculated. Rearrange these fragmented blocks in their increasing order of mean and standard deviation. As a first step, fit the appropriate fragmented tile in payload within corresponding fragmented tile of host medium. Repeat the above said process with all other fragmented blocks. This results in marked fragmented visible mosaic image.

The resultant fragmented mosaic encrypted image looks similar to selected target image which does not emphasize the hacker attention regarding secret payload information being encrypted. Hence applying Color modification making use of standard Color modulation methodology would make the PSNR of resultant picture much better. Color modification is carried out using the standard Color modulation method. Let A and A' indicate pixel information of two different images they are

$$\{p_1, p_2, \ldots, p_n\} \text{ and } \{p'_1, p'_2, \ldots, p'_n\}$$

Consider an image in RGB format. P_i denoted by (r_i,g_i,b_i) and that of each P_i' by (r_i',g_i',b_i'). Mean of A and A' are computed in all three planes R, G, and B individually by using equations (2.1.1) and (2.1.2):

$$\mu_c = \frac{1}{n}\sum_{i=1}^{n} c_i \quad (2.1.1)$$

$$\mu_c' = \frac{1}{n}\sum_{i=1}^{n} c_i' \quad (2.1.2)$$

Standard deviation of A and A' are computed in all three planes R, G, and B individually by using equations (2.1.3) and (2.1.4).

$$\sigma_c = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(c_i - \mu_c)^2} \quad (2.1.3)$$

$$\sigma_c' = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(c_i' - \mu_c')^2} \quad (2.1.4)$$

In which C_i and C_i' denote the intensity information of pixels, with C= r, g, or b values. In next step new Color values (r_i", g_i",b_i") are computed for each P_i in A by equation (2.1.5).

$$c_i'' = q_c(c_i - \mu_c) + \mu_c' \quad (2.1.5)$$

In which $q_c = \frac{\sigma_c'}{\sigma_c}$ is the quotient of standard deviation and C= r,g,or b .It can be easily verified that new Color mean and variance of the tiles of image A is almost very nearer to those of A' respectively. In order to calculate the original Color values (ri,gi,bi) of P_i from the new Color values,(r_i", g_i ",b_i"), inverse of equation (2.1.5) is computed by the following equation (2.1.6).

$$c'' = \left(\frac{1}{q_c}\right)(c_i'' - \mu_c') + \mu_c \quad (2.1.6)$$

Each Mosaic Tile Angular Movement: The required tile is chosen and rotate them angularly considering different angles such as angular rotation by 0°, 90 °, 180 °, or 270 °. The appropriate angular rotation angle is chosen which could give lesser mean square error values.To retrieve the sensitive image information from target image, it is very important to hide the relevant information required to get back the pay load secret image. The information needed to retrieve back the payload secret image fragment A ,which is mapped to cover image block A' includes _ Index of segment A', appropriate angular rotation angle , standard deviation and mean values of marked segments of mosaic encrypted image and target image. All these four parameters are combined as four component streams and is hidden in LSB bits of marked image pixels.

Retrieval Method For Secret Pay Load Image: Post retrieval of hidden confidential data from each segmented division of the fragmented mosaic picture, angular movement of each fragmented division in the opposite angular movement by the same amount of angular rotation as done at the transmitter facet and retrieval of the concerned index, accommodate the incoming sub division into original tile of a vacant picture with no information. As a next step making use of features like mean along with standard deviation to obtain back authentic block of payload picture. Continue this method for rest of the segments. As a last stage integrate all the resultant retrieved fragmented tile picture information to obtain the required sensitive picture data. In the receiver side the embedded information is extracted from mosaic image then secret image is recovered using the extracted information.

Chaos Encryption: A Dynamic discrete time system is considered for cryptographic algorithm. A dynamic system is said to be chaotic if all curves are bounded by nearby curves which diverge exponentially at every point of the phase space. A chaotic system is defined by an iterated function (map) 'f' of a state space 'X'. The iterated function transforms the present state of the system to next state with an equation.

$$X_{n+1} = f(X_n) \quad (2.2.1)$$

Where $X_n \varepsilon X$, which denotes the system state at the discrete time. In chaos based cryptography the state space is typically on finite binary space,

$$X=P=C\ \{0, 1\}^n \quad ; n=1, 2 \quad (2.2.2)$$

Where P is plain text and C is cipher text. The initial condition is a vector $x_0 \epsilon X$, and it is assigned to an internal state variable before the first iteration. The vector $C \epsilon K = \{0, 1\}^n$ contains parameters of the dynamic system. The parameters are kept constant throughout all iterations as mentioned by F. Belkhouche and U. Qidwai (2003).I D chaotic maps are generated and used in proposed method. A dynamical system is a couple (I, Φ), where I is a Real interval and Φ is a transformation from I to I .A nonlinear transformation used as iterative scalar map mentioned by Mohammad Obaidur Rahman, and Muhammad Kamal Hossen (2018), which is defined as

$$X_{n+1} = F(X_n, \alpha) \quad (2.2.3)$$

$X_n=0=X_0$ Where α is real set of real parameters. The use of equation (2.2.3) for image encoding means that the image is taken as a dynamical system. The image is represented in integer values and they are mapped in to real values of equation (2.2.3).Logistic map is one of the known chaotic maps defined in the equation (2.2.4)

$$X_{n+1} = \alpha X_n(1 - X_n),\ X_n = 0 = X_0 \qquad (2.2.4)$$

In order to enhance security, Chaos usage for encoding images gives rise to three types of keys which may be used together or separately. The three keys are control parameter 'α', initial state x0 and number of iterations used by F. Belkhouche and U. Qidwai (2003), the number of iterations is kept constant and equal to size of the image, which is to be encrypted. Three types of approaches are followed based on three keys of encryption. The approaches used in the proposed method are explained as following. In first approach one external encryption key is used .The chaotic map will generate a threshold vector of two values:0 and 1.

The pixels vectors of the image that are corresponding to Zeros of the threshold vector will be encrypted by single key and other pixels will be normalised such that image vectors are hided. Second, using two encryption keys. Chaotic map will generate a threshold vector of two values: 0 and 1. The pixels of the image vector corresponding to zeros will be encrypted by first key and other pixels corresponding to the ones will be encrypted by second key. In order to increase the security further three keys are used. Chaotic map will generate threshold vector of three different values: 0, 0.5 and 1. The pixels corresponding to zeros will be encrypted by first key, the pixels corresponding to 0.5 values will be encrypted by second key and finally pixels corresponding to one will be encrypted by third key. The chaotic map defined in the equation (2.2.4) will implement the three encryption scheme. The reverse operation of the encryption process is the decryption process.

Improved Lsb-Mapping Steganographic Technique: In this technique, payload secret image and a carrier image are the inputs to the Steganographic algorithm which is also mentioned by Afrakhteh, Met al., (2010), Chang, C et al., (2010) , C. Sumathi, et al., (2013). The pay load secret image pixel values are taken as vector of binary values which are to be hidden the carrier pixel Least significant bits .In one iteration, one block (two bit size) of payload secret image vector of binary values is considered for substitution and compared with pixel byte information of carrier image. Since two bits of payload is considered for hiding all the combinations for two bits are considered as the conditions for substitution mentioned by N. Akhtar(2015). The combinations and their substitutions are shown in table 2.3.1. The substitution is based on LSB –mapping with simple addition function.

The method of mapping is as follows

a. Select the cover image with pixel values denoted by C (i, j).
b. Select the Payload secret data with pixel values denoted by PL (i, j).
c. Select the cover image pixel looking up to the mapping table shown in table 2.3.1 for hiding the payload data.
d. Changes in cipher pixels are made simply by addition on comparing with payload bits.
e. Two bits of payload data are selected for substitution in two LSBs of Carrier image pixel.
f. Repeat steps until all the payload bits are substituted in the carrier image.
g. The embedded image called Stego image pixels denoted by SI (i.j) is then transmitted in the network.

Proposed Method: The proposed method is a combination of both cryptographic technique and Steganographic technique. In sender side, Mosaic encryption technique is implemented on the selected pay load secret image choosing the target image. Then discrete wavelet transform is applied to mosaic encrypted image. DWT results Information part and approximate parts .The information part is then encrypted by using chaos based encryption. The chaos encrypted information part is then combined with approximate parts to get a combined image. Combined image is then hided using Improved LSB mapping technique in selected cover image to get a stego image. Stego image is then transferred in the network.The Receiver receives the stego image, de-embed stego image to get chaos encrypted image.

Table 2.3.1. LSB addition used for data hiding

Carrier Image pixel value CI	Payload image pixel value PL	Stego image pixel value SI	Change in cover image pixels
CI_1=10110000	01	$SI_1=CI_1$ (10110000)	No change
CI_2=11001101	11	$SI_2=CI_2+1$ (11001110)	One bit change
CI_3=11110011	10	$SI_3=CI_3+2$ (11110101)	One bit change
CI_4=11001101	01	$SI_4=CI_4+3$ (11010000)	One bit change
CI_5=10101010	00	$SI_5=CI_5+1$ (10101011)	One bit change

Chaos encrypted image is then decrypted to get mosaic encrypted information part. This information part is then combined with approximate components to get combined image. Apply Inverse DWT to combined image to get Mosaic encrypted image. Mosaic encrypted image is then decrypted to get back the payload secret image. Figure 3.1 and figure 3.2 depicts the proposed method both from sender and receiver side respectively.

The proposed method – Sender side: explained in following steps.

Step 1: Target image of 512*512 is selected and then Pay load image of size 256*256 is selected.

Step 2: Using the concept explained in the sec 2.1 , Target image and Pay load images are divided into tiles .Then those tiles are compared by calculating the standard deviations. Suitable tiles of payload image are then substituted in Target image such that a mosaic encrypted image is formed. Color Transformation is then applied to mosaic image tiles for matching the target image pixels.

Step 3: The parameters such as Index of image segment 'A', appropriate angular rotation of A standard deviation and mean of marked segments of payload image and target image should be known to the receiver for retrieval of pay load. So this information is hided in the LSBs of Mosaic image.

Step 4: The Discrete Wavelet transform is the applied to Mosaic image which divides the image into detailed part and approximate part .Detail part is then compressed and approximate part is encrypted by chaos encryption. The procedure is shown in the figure 3.2.

Step 5: The Chaos encryption technique which is explained in section 2.2 is used to encrypt the information part. The 1600 bit length key is generated by pseudorandom generator. Chaos encrypted cipher is formed.

Step 6: This Chaos encrypted cipher is then combined to form combined information image as shown in figure 3.2.

Step 7: The Chaos encrypted cipher of size 128*128 is then embedded in to a selected cover image of size 512 *512 using the concept improved mapping LSB hiding technique.

Step 8: The Stego image along with the detailed parts are transferred in the channel.

The stego image is then transferred in the communication channel. The receiver receives the stego image and follows the steps explained in the receiver side proposed method.

The proposed method – Receiver's side: Explained in following steps:

Step 1: The Detail components along with the stego image is taken as input in the Receiver Side.

Step 2: The stego image is de embedded to get the chaos encrypted cipher. This cipher is then Decrypted to get chaos decrypted Information part.

Step 3: The chaos decrypted Information part the combined with decompressed detailed parts to get combined image.

Step 4: Inverse DWT is then applied to this combined image and get back the mosaic encrypted cipher.

Step 5: Mosaic decryption algorithm is then applied to get back pay load image.

Experimental Results: The proposed method is implemented in mat lab software. The evaluation of proposed method is done by calculating Peak signal to noise ratio (PSNR), Root Mean Square and correlation values. One set images considered to implement the proposed method are shown in figure 4.1.

The output images resulted after implementing the proposed method in the senders side are shown in the figure 4.2. The values of PSNR, RMSE and Correlation calculated at sender side are listed in the table 4.1. The values of PSNR, RMSE and Correlation calculated at Receiver side are listed in the table 4.2.

Figure 3.1: Model for proposed method - Senders side

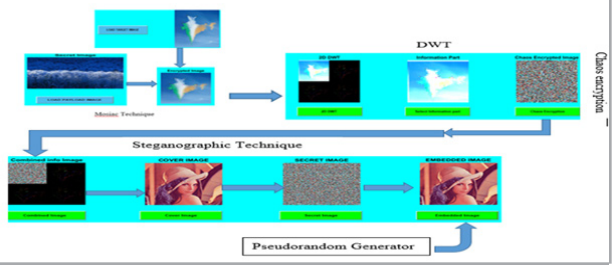


Figure 3.2 The Procedure of DWT and chaos encryption.

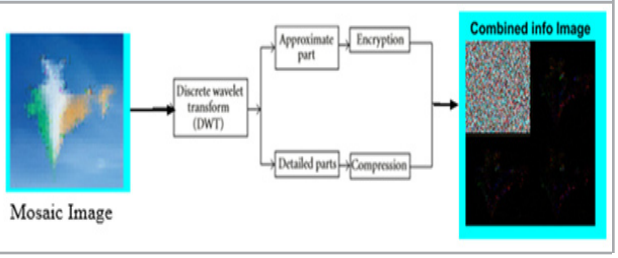
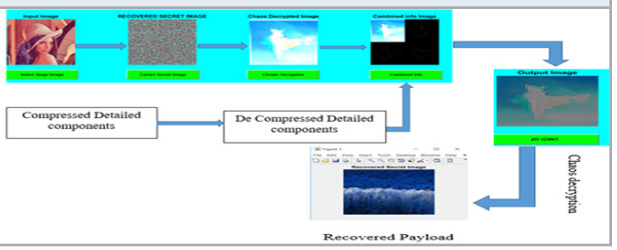


Figure 3.3: Model for proposed method – Receiver's side



Sensitive Analysis: The resistance of the crypto-steganography algorithms against the differential attacks is made by Sensitivity measures. Generally the desired property of encryption algorithm is to be sensitive to small change in key can cause large change in the cipher, then differential attack losses its efficiency and becomes practically useless. The cryptosystems efficiency is measured by sensitivity analysis. To test the influence of one byte chance in the key on the whole encrypted algorithm by the proposed algorithm, two common measures Number of Changing Pixel Rate (NPCR) and

Unified Average Changed Intensity (UACI) were used. NPCR, UACI and MSE between.

Figure 4.1: Selected input images for evaluating the proposed method

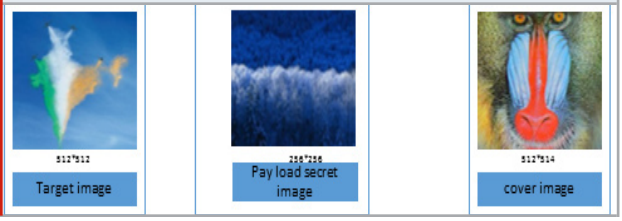


Figure 4.2: Output images of the proposed method- sender side

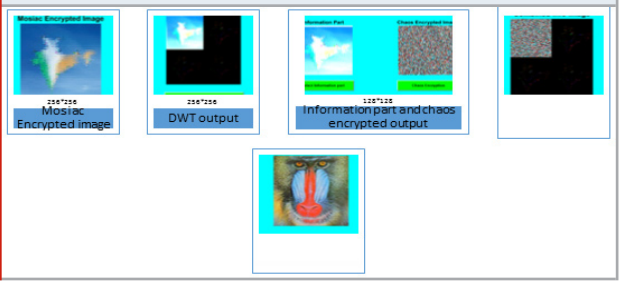


Table 4.1. List of PSNR, RMSE and correlation values – Sender side

Values between the Images	PSNR	RMSE	Correlation
Mosaic encrypted and target image	25.6824	13.0694	0.9564
Mosaic encrypted and chaos encrypted image	49.2055	0.8676	-0.004374
Stego and cover image	68.0435	0.012432	

To approach the performance of an ideal image encryption scheme, NPCR values must be as large as possible UACI should be close to 33% mentioned by the authors like Y. Hu et al., (2008) and Z. Ni al., (2006).High percentage of NPCR measure indicates that pixels positions have been randomly changed. Sensitive analysis has been done between the payload secret images and retrieved secret image shown in figure 4.3 .The figure indicates less UACI value and so the proposed method is highly effective to retrieve back the original play load image with high correlation and NPCR values. the two Images [Q_1 (i, j)] and [Q2 (i, j)] are defined as

$$D(i.j) = \begin{cases} 0 & :Q1(i,j)=Q2(i.j) \\ 1 & :Q1(i,j)=Q2(i,j) \end{cases} \quad (4.1.1)$$

$$\text{UACI} = \frac{1}{M*N}\sum_{i=0}^{N}\sum_{j=0}^{M}\left|\frac{Q1(i,j)-Q2(i,j)}{255}\right| * 100\% \quad (4.1.2)$$

Table 4.2. List of PSNR, RMSE and correlation values – Receiver side

Values between the Images	PSNR	RMSE	Correlation
Stego and Retrieved stego	51.192	0.494171	
Mosaic encrypted and chaos decrypted image	56.229	0.380703	0.734673

$$\text{NPCR} = \frac{1}{M*N}\sum_{i=0}^{N}\sum_{j=0}^{M} D(i,j) * 100\% \quad (4.1.3)$$

$$\text{MSE} = \frac{1}{M*N}\sum_{i=0}^{N}\sum_{i=0}^{M}[Q1(i.j) - Q2(i,j)]^2 \quad (4.1.4)$$

Tests have been conducted on proposed scheme for a small change in key presented in table 4.3. High UACI show almost all the pixel intensity values of encrypted image have been changed from their values in original image making original and encrypted image pixels more dissimilar.

Observations To Evaluate The Efficiency of the Proposed Algorithm: Figure 4.4 shows the PSNR, RMSE and Correlation between the Target image and Mosaic encrypted image. PSNR value 25.6824 indicates that the Mosaic encrypted image is meaningful cipher which camouflage the intruder since mosaic encrypted image is similar to target image. Figure 4.5 shows the PSNR, RMSE and Correlation between the Mosaic encrypted image and chaos encrypted image. PSNR value 49.255 and correlation value -0.0004371 indicates the strength of encryption algorithm since the Randomness is increased sufficiently in chaos cipher. Figure 4.5 shows the PSNR, RMSE between the Lena Stego image and cover image .PSNR value indicates 69.8924 indicates the good amount of security from LSB-mapping Steganographic technique.

Table 4.3. Sensitive analysis

Encryption and decryption keys / Parameters	1234	1234	1234	1234
	1235	2345	1236	0123
UACI	18.977	28.5185	22.74107	19.3986
NPCR	90.6815	89.9969	87.2961	89.9924
PSNR	34.5857	24.0721	28.1735	24.082
CORRELATION	0.9791	00.0468	0.7679	-0.00463
MSE	21.7475	254.607	98.24666	254.607

Figure 4.6 shows the PSNR, RMSE between the information image of 2DWT image and Decrypted chaos information image. PSNR value 51.916 indicates the similarity between the two. Figure 4.7 shows the PSNR, RMSE and Correlation between the pay load image a recovered payload image indicates that almost payload is achieved with multiple layers of Crypto - Steganographic algorithm. Since correlation is almost 8. Figure 4.8 shows the Sensitive analysis - Mosaic Encryption. The UACI and NPCR values are calculated between the two reconstructed payload images by small variation in encrypted key.

Figure 4.3: GUI of sensitive analysis between payload secret image and retrieved image

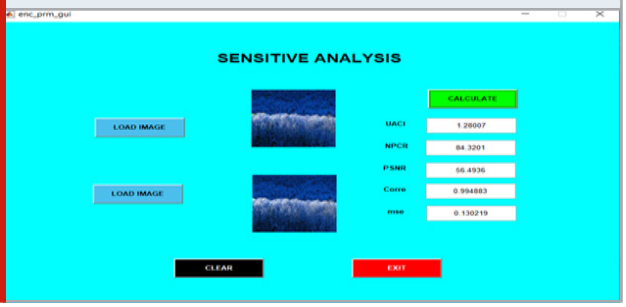


Figure 4.4: Creation of mosaic encrypted image

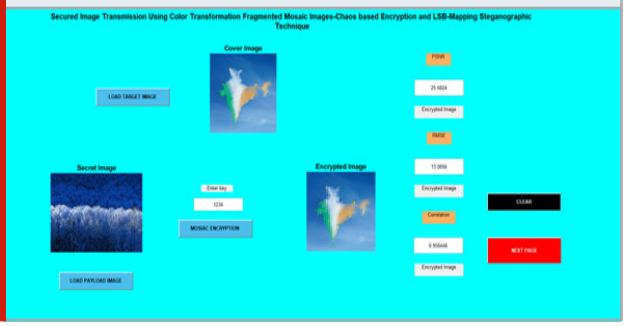


Figure 4.5: Creation of Detailed components and Stego of information part of Mosaic Image

Multilayer Cryto-Stegano algorithm is very sensitive to a small change in mosaic encryption key leads to large difference in the reconstructed payload. Figure 4.9 shows Sensitive Analysis – Discrete Wavelet Transform Output and IDWT Output. The UACI and NPCR values are calculated between 2DWT image and IDWT image which shows that IDWT reproduced the DWT input

Figure 4.6: DE embedding, 2IDWT and Chaos decryption resultant images

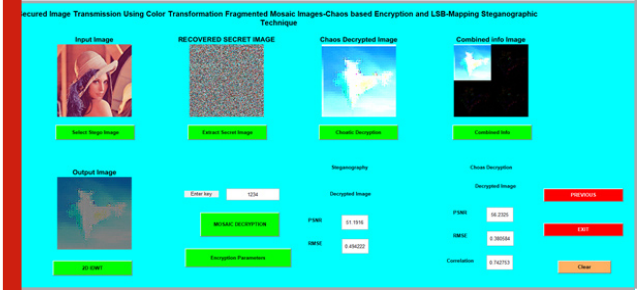


Figure 4.7: Sensitive analysis -Mosaic Encryption

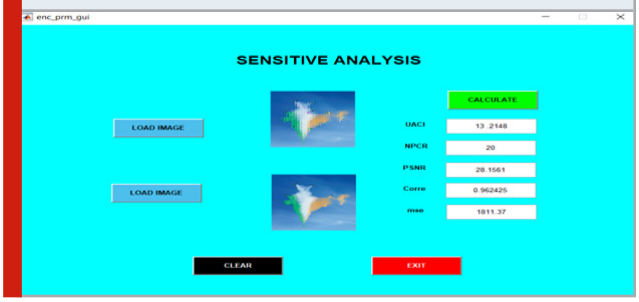


Figure 4.8: Sensitive analysis – Differential attacks – Mosaic Encryption

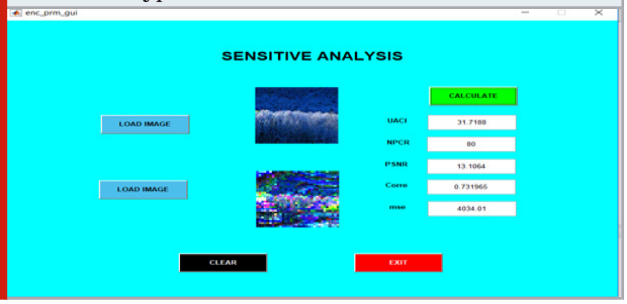
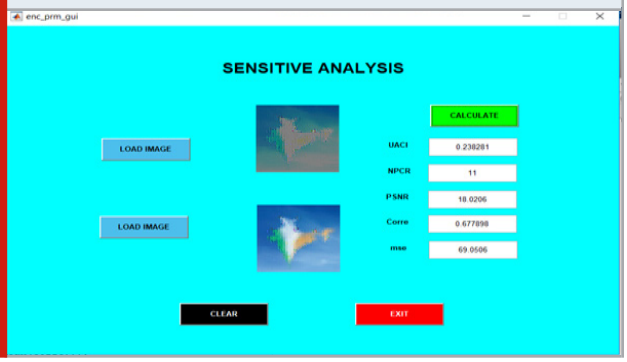
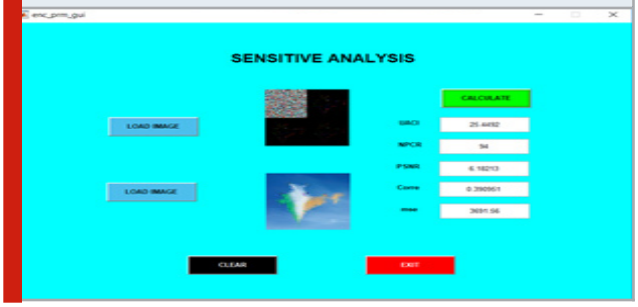


Figure 4.9: Sensitive Analysis – Discrete Wavelet Transform Output and IDWT Output



mosaic encrypted cipher successfully. Figure 4.10 shows Sensitive Analysis – Mosaic Encrypted Image: Cipher 1 and Chaos Encrypted Output Cipher 2. The values of UACI and NPCR are nearing to standard values which are 33% and 100%.

Figure 4.10: Sensitive Analysis – Mosaic Encrypted Image: Cipher 1 and Chaos Encrypted Output Cipher 2



Comparisons: A comparative study of different data hiding techniques' has made and listed out values of PSNRS of B. Karthikeyan et al., (2017), Ranjan & Bhonsle(2016), Mohammad Obaidur Rahman and Muhammad Kamal Hussein (2018) with the proposed method. The table 4.4 is listed the values of PSNRs of all algorithms using 512*512 cover images and hiding a data of size 256*256 image . Existing methods gives one layer security having low PSNRS. But present method with multiple layer crypto-stego techniques it is giving better PSNRS. Table 4.4 shows the comparison Values.

Table 4.4. Comparisons of PSNRS of existing methods with the proposed method.

Cover Image	Karthikeyan. (2017)	Ranjan Bhonsle (2016)	Mohammad (2018)	The Proposed Method
AIR	54.39	57.67	63.33	67.9657
LENA	57.45	57.80	64.23	68.3793
PEPPER	50.53	57.65	62.48	70.8291
BABBOON	43.46	57.58	63.33	68.024

CONCLUSION

The proposed algorithm is a comprehensive method of combining the cryptographic and Steganographic techniques to protect and control access of secure data. Using mosaic encryption technique the secret image is camouflaged to target image and hence the crypto -stego algorithm is more efficient to secure data. Also original secret image is recovered lossless. Less correlation values between the encrypted image and original shows the desired randomness in the cipher image. Good experimental results shows the feasibility of implementing the algorithm effectively.

REFERENCES

Afrakhteh. M & Ibrahim S (2010) Adaptive steganography scheme using more surrounding pixels. Computer Design and Applications (ICCDA) pg.no:25-27.

A Ranjan M. Bhonsle (2016) Advanced technics Toshared & protect cloud data using multilayer steganography and cryptography, Proc. of IEEE International Conference on Automatic Control and Dynamic Optimization Techniques.

B. Karthikeyan, A. Deepak, K. S. Subalakshmi, A. Raj, and V. Vaithiyanathan(2017) A combined approach of steganography with LSB encoding technique and DES algorithm Proc. of 3rd International Conference on Advances in Electrical, Electronics, Information, Communication and Bioinformatics IEEE 978-1-5090-5434-3.

Chang Chen W Le (2010) High payload steganography mechanism using hybrid edge detector. Expert Systems with Applications.

C.-H. Hsu, A study of chaotic image encryption algorithm, M.S. thesis Electrical Engineering Department, Chung Yuan Christian University.

C. K. Chan and L. M. Cheng (2004) Hiding data in images by simple LSB substitution Pattern Recognition vol. 37, pp. 469–474.

C. Sumathi, T. Santana, and G. Umamaheswari (2013) A study of various steganographic techniques used for information hiding International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4.

F. Belkhouche and U. Qidwai (2003) Binary image encoding using 1D-chaotic maps, in Proceedings of the IEEE Region 5 Annual Technical Conference, pp. 39–42.

J. Fridrich, (1998) Symmetric ciphers based on two-dimensional chaotic map, Int. J. Bifurcate. Chaos, vol. 8, no. 6, pp. 1259–1284.

J. Fridrich, M. Goljan, and R. Du (2001) Invertible authentication Proc. SPIE vol. 3971 pp. 197–208.

J. Tian,(2003) Reversible data embedding using a difference expansion IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896.

Mohammad Obaidur Rahman, Muhammad Kamal Hossen (2018) JCSNS International Journal of Computer Science and Network Security, An Approach for Enhancing Security of Cloud Data using Cryptography and Steganography with E-LSB Encoding Technique

VOL.18 pg. No.9.

N. Akhtar (2015) An LSB Substitution with Bit Inversion Steganography Method, Smart Innovation, Systems and Technologies, Springer India, vol. 43, pp 515–521.

Parameshachari, B. D., Rashmi P. Kiran, P. Rashmi, M. C. Supriya, Rajashekarappa, and H. T. Panduranga. "Controlled partial image encryption based on LSIC and chaotic map." In ICCSP, pp. 60-63. 2019.

Parameshachari, B. D., H. T. Panduranga, and Silvia liberata Ullo. "Analysis and Computation of Encryption Technique to Enhance Security of Medical Images." In IOP Conference Series: Materials Science and Engineering, vol. 925, no. 1, p. 012028. IOP Publishing, 2020.

Prabu, S., V. Balamurugan, and K. Vengatesan. "Design of cognitive image filters for suppression of noise level in medical images." Measurement 141 (2019): 296-301.

R. M. May, Simple mathematical models with very complicated dynamics, Nature, vol.261, no.5560, pp.459–467.

V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y.-Q. Shi,(2009) Reversible watermarking algorithm using sorting and prediction IEEE Trans. Circuits Syst. Video Technol., vol. 19, no. 7, pp. 989–999.

W.-H. Lin S.-J. Horng W. Kao P. Fan, C.-L. Lee, and Y. Pan (2008) An efficient watermarking method based on significant difference of wavelet coefficient quantization, IEEE Trans. Multimedia, vol. 10, no. 5, pp. 746–757.

W. Zhang, X. Hu, X. Li and N. Yu (2013), Recursive histogram modification: Establishing equivalency between reversible data hiding and lossless data compression. IEEE Trans. Image Process. vol. 22, no. 7, pp. 2775–2785.

X. Li, B. Yang, and T. Zeng (2011), Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection, IEEE Trans. Image Process, vol. 20, no. 12, pp. 3524–3533.

Y. Hu, H.-K. Lee, K. Chen, and J. Li,(2008),Difference expansion based reversible data hiding using two embedding directions, IEEE Trans. Multimedia, vol. 10, no. 8, pp. 1500–1512.

Z. Ni, Y. Q. Shi, N. Ansari, and W. Su,(2006) Reversible data hiding, IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362.