Secured Face Identity of Image Photograph by FIFFCT and Selective LSB Hiding Technique

Y. Manjula1*, K. B. Shivakumar2

[1]Assistant Professor, Dept. of ECE, Sri Siddhartha Institute of Technology, Tumakuru, Karnataka, India.
[2]HOD, Dept. of TCE, Sri Siddhartha Institute of Technology, Tumakuru, Karnataka, India.

ABSTRACT: The use of photo identity is post important aspect in today's digital transaction system the business units, government, private sectors and also research units are using the images for transferring and communicating secret data. This increases the importance to improve the security of person's identity in photo images through cryptography and steganography techniques. The present paper propose a new technique called Photo image security using fractal image encryption and modified LSB hiding method. The paper discuss the method of fractal image encryption based on finite field cosine transform (FIFFCT) and also about modified LSB technique. The preparation of message which is used for embedding in the photo is also explained clearly. The evaluation parameters for analyzing both cryptographic and stenographic techniques are also clearly examined in two layers. The robustness of the algorithm is analyzed by key sensitive analysis. The differential attacks are applied for evaluating the robustness of proposed method. This paper provides future scope in image security algorithms.

***Index Terms* - Cryptography, steganography, FIFFCT, Selective LSB technique, Differential attacks.**

1. INTRODUCTION

The rapid increase in usage of digital data i.e., both personal and organizational data, increases difficulty in handling the computational complexity locally.so the data is outsourced to cloud server .This increases the importance of protecting the personal identification information in images. The face detection and recognition algorithms are frequently used many primary applications such as state police, hospitals, department of commerce who maintain the large database of images.

An algorithm for extracting the features of the faces has been developed for enhanced identification of faces [1], based on the shape of face .Edge detection is performed based on the multiple scale filter for getting the edges. These edges are linked to form a face contour for identification of faces. Conventional neural networks based on deep learning frame works object detection are used for detection of faces in the images. A set of face images are taken and compressed in to one face data which is compared to analyse the face [3].

The efficiency of face detection algorithms influence the efficiency of face recognition algorithms. However the facial characteristics detection and analysis algorithms are used for illegal activities .A face recognition system is used ATM [4] for the authentication purpose. Illegal users can access the data of facial information from the digital multimedia applications to harm them by causing the adverse effects. So the visual features of the face in the communication channel has to be secured. The person's identity in biometrics features or iris information has to be safeguarded by designing a model implementing the cryptographic and stenographic algorithms.

Number of techniques are proposed for generating the keys which are used for encryption and stenographic algorithms which based on chaotic maps and fractal images [5].

The Mandrill bulb set of fractal images are used in [6].the matrix operations are applied to the fractal image and its compressed image for encryption and decryption.

The protection of images is achieved by [7] in which The original image is summed with a random image to form a combined image and the combined image is saved in set of two separated set of features called V1 and V2.These features are encrypted with holomorphic encryption and then placed ,in cloud. The original image is protected since the retriever should have both V1 and V2 to get the image.

The proposed method use one face detection algorithm for detecting the faces , two encryption methods for encrypting the faces and one stenographic method to secure the faces in the image photograph. A secret message called face information data, having the information of faces is generated based on the detected faces. This message is embedded in the encrypted faces inserted image photograph. The finite field cosine transform is selected for first encryption algorithm as it is defined in integer modulo P to overcome the adverse values over the real valued transforms and then encryption based on fractal images is implemented.

2. CONCEPTUAL KNOWLEDGE USED FOR PROPOSED METHOD

2.1 FACE DETECTION MODEL:

Number of algorithms are implemented for face detection in the images [6-10]. In an image different faces appear in any position of the image, have different aspect ratios and different sizes , the fixed scale Sliding window is used to scan the whole image.

The face detection method function is available in MATLAB toolbox. This function uses Gabor feature extraction method and neural networks.

Once the function is used then the faces from the images are detected by showing the face information data on the face itself. The position of face, width and height of the face are known. By implementing a simple program the faces are extracted from the photograph .This faces are stored in the file for further processing.

2.2 FINITE FIELD COSINE TRANSFORM:

The Finite field cosine transform is used because it is defined over integers modulo P and so avoids inaccurate values in real value transforms [11]. A type two FFCT is defined [12] as below

Let λ ϵ GF(p) be an element with multiplicative order 2N .The finite field cosine transform (1 D) of the vector x = $[x_0,x_1,x_2,x_3\ldots\ldots x_{N-1}]$, x_i ϵ GF(p) is given by the vector X = $[X_0,X_1,X_2,X_3\ldots\ldots X_{N-1}]$, X_k ϵ GF(p) whose elements are

$$X_k = \sqrt{\frac{2}{N}\sum_{i=0}^{N-1}\delta_k x_i \cos\lambda\left(k\frac{2i+1}{2}\right)} \quad [20] \qquad (2.2a)$$

Where

$$\delta_k = \begin{cases} \sqrt{\frac{1}{N}} & \text{if} \quad k = 0 \\ 1 & \text{if } k = 1,2,3 \ldots\ldots\ldots\ldots N-1 \end{cases} \qquad (2.2b)$$

The inverse FFCT can be computed according to the following formula

$$x_i = \sqrt{\frac{2}{N}\sum_{i=0}^{N-1}\delta_i X_k \cos\lambda\left(k\frac{2i+1}{2}\right)} \qquad (2.2c)$$

The forward transformation equation can be represented in matrix format as X=Tx, where T is the Transformation matrix corresponds to the elements obtained directly from (1) .Similarly the inverse transformation can also be written as x=T^{-1} X.

The two dimensional FFCT transformation extended from 1 D equations of matrix U with dimension N*N can be computed by

C=TUT^{-1} (mod p) **(2.2d)**

Where U is the input matrix and T is the transformation matrix.

The proposed method uses the RGB Color image and this Color image is converted in to three Color planes red, blue and green planes. Each channel has pixel values ranging from 0 to 255. Choosing the value p = 257, which is required for transformation equation (4) is defined form the paper [13].

The FFCT transformation matrix of size 8*8 derived from equation (1) used for encryption method mentioned in proposed method is

$$T=\begin{bmatrix} 15 & 15 & 15 & 15 & 15 & 15 & 15 & 15 \\ 137 & 163 & 98 & 106 & 151 & 159 & 94 & 120 \\ 160 & 6 & 251 & 97 & 97 & 251 & 6 & 160 \\ 163 & 151 & 120 & 159 & 98 & 137 & 106 & 94 \\ 242 & 15 & 15 & 242 & 242 & 15 & 15 & 242 \\ 98 & 120 & 106 & 163 & 94 & 151 & 137 & 159 \\ 6 & 97 & 160 & 251 & 251 & 160 & 97 & 6 \\ 106 & 159 & 163 & 120 & 137 & 94 & 98 & 151 \end{bmatrix}$$

Where T is orthogonal transformation matrix which satisfies the equation

$$TT^{-1}=T^{-1}T=I_N \qquad (2.2e)$$

2.3 Fractal Images:

The fractal images are obtained by replacing the kernel at various scales of magnification which have unique properties. The fractal image can be generated by using mathematical equation. The number of fractal images can be generated from an image by repeating implementation of the equation along with variations in kernel. Choice of image for deriving fractal images is purely dependent on the sender and receiver parametric requirements. Internet resources are available to generate fractals.

Iterated function Systems (IFS) [4] are used for generating fractal images. IFS has better conceptual simplicity and good ability to reproduce natural variations with complex phenomena in fractal images. This method of generating the fractal images derives the efficient key for encryption.

A fractal image is scanned in Zigzag format [14] to convert a two dimensional matrix in to one dimensional vector .This vector is used for preparing the key stream. The size of one dimensional vector will have N^2 elements for a N*N matrix. These N^2 elements are reshaped back to N*N two dimensional matrix. The procedure is as shown in figure.

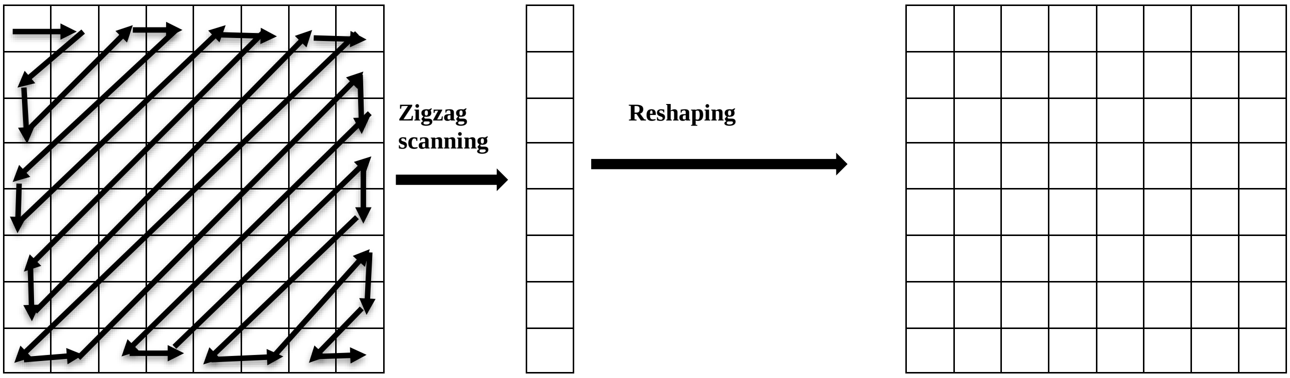


Figure2.1: Zig zag scanning method and reshaping of image.

2.4 Chaotic LSB Substitution:

The image which carries the message is called container the secret message can be of any type. [15]. The container is a Color image which is converted in to red, blue and green planes .these planes will have the pixel vales ranging from 0-255. Each plane pixel values are in byte size. The total size of the container image is then calculated. Then the secret message is converted into binary values.

The conventional LSB substitution method is selected by chaos [15]. The Röseller oscillator equations of chaos are defined by the set of equations shown below

$$\frac{dx}{dt} = -(y + z) \qquad (2.4a)$$

$$\frac{dy}{dt} = x + ay \qquad (2.4b)$$

$$\frac{dz}{dt} = b + z(x - c) \qquad (2.4c)$$

Where initial values of x, y z are defined along with control parameters a, b, c.

By solving equations from 2a to 2c the position of the pixel is derived. The pixel position which is derived from the equations is the pixel choosed for hiding the message bit. The message bit is embedded in the LSB bit of the choosed pixel. This method is iterated until the complete secret message is embedded.

3. EVALUATION TECHNIQUES

The proposed algorithm has two security algorithms, and therefore the evaluation techniques are applied for both methods.

3.1 Evaluation of Cryptographic algorithms: The evaluation process uses the following parameters,

3.1.1 Correlation between the pixels of original face and cipher face. The original face will be having high correlated adjacent pixels and the encryption algorithm should reduce the correction of adjacent pixels in cipher image.

The Correlation coefficient (ρ) between two N dimensional vectors x and y is calculated by using equation 3.4.

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - \frac{1}{N}\sum_{j=1}^{N} x_j)(y_i - \frac{1}{N}\sum_{j=1}^{N} y_i \qquad (3.1)$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - \frac{1}{N}\sum_{j=1}^{N} x_j)^2 \qquad (3.2)$$

$$D(y) = \frac{1}{N}\sum_{i=1}^{N}(y_i - \frac{1}{N}\sum_{j=1}^{N} y_j)^2 \qquad (3.3)$$

$$\rho = \frac{cov(x,y)}{\sqrt{D(x)D(y)}} \qquad (3.4)$$

3.1.2 The visual analysis is done by finding the histograms of original face and the cipher face. The histogram of original face will be having uneven distribution of pixel intensities but histogram of cipher face will be having uniform distribution.

3.1.3 The randomness in the image is measured by the average information of an image called Entropy. High correlation values between adjacent pixels refers the more predictability of information. The unpredictability of information will be high for a flat histogram. Histogram of an image is given by

$$\boldsymbol{H}(\mathrm{X}) = -\sum_{\mathrm{i}=1}^{\mathrm{n}} \mathrm{p_i} \log_2 \mathrm{p_i} \qquad (3.5)$$

Where $p_{i=}\frac{Number\ of\ occurences\ of\ the\ intensity\ level\ i}{Number\ of\ intensity\ levels}$

3.1.4 The resistance of the proposed algorithm against the differential attacks is made by Sensitivity measures: If sensitivity is high the cryptosystem is more efficient. The cryptosystems efficiency is measured by sensitivity analysis. The analysis can be done in two phases.

Phase i: When there is a small change in key then there should large difference in the cipher face. To find that, first the original face is encrypted to get the cipher face 1 named as Q1. Then encryption is done to the original face with a small change in key to get the cipher face 2 named Q2. Then NPCR, UACI and MSE between the Q1 AND Q2 is determined which is shown. High values refers to large sensitivity.

Phase ii) When there is a small change in the original face then there should be large difference in cipher image .To find that, first the original face is encrypted to get the cipher face 1. Then encryption is done to the original face with a small change in face to get the cipher face 2. Then NPCR, UACI and MSE between the Q1 AND Q2 is determined which is shown. High values refers to large sensitivity.

It is clear that NPCR concentrates on the absolute number of pixels which changes value in differential attacks, while the UACI focuses on the averaged difference between two paired cipher text images.

Mean absolute error is the measure of error between the original face and cipher face. If the original face pixel position is OF(x, y) and Cipher face pixel position is CF (x.y), and size of the face is M*N then

$$MAE = \frac{1}{M*N} \sum_{i=0}^{N} \sum_{i=0}^{M} |OF(i,j) - CF(i,j)| \quad (3.6)$$

$$\mathrm{D(i.j)} = \begin{cases} 0 & \text{:Q1(i,j)=Q2(i.j)} \\ 1 & \text{:Q1(i,j)=Q2(i,j)} \end{cases} \quad (3.7)$$

$$\mathrm{UACI} = \frac{1}{M*N} \sum_{i=0}^{N} \sum_{j=0}^{M} \left| \frac{Q1(i.j) - Q2(i,j)}{255} \right| * 100\% \quad (3.8)$$

$$\mathrm{NPCR} = \frac{1}{M*N} \sum_{i=0}^{N} \sum_{j=0}^{M} D(i,j) * 100\% \quad (3.9)$$

$$\mathrm{MSE} = \frac{1}{M*N} \sum_{i=0}^{N} \sum_{i=0}^{M} [Q1(i.j) - Q2(i,j)]^2 \quad (3.10)$$

3.2 Evaluation of stenographic algorithm:

The Evaluation of stenographic algorithm is done by finding the PSNR and correlation values between the original photograph and retrieved photograph.

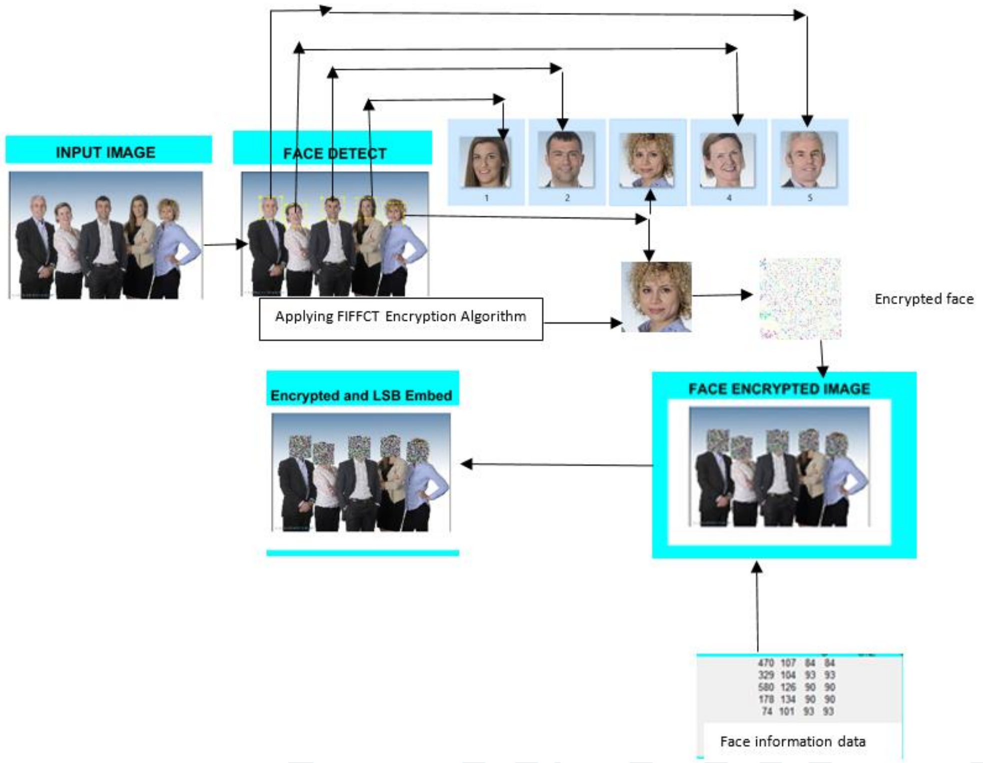
4. THE PROPOSED METHOD

4.1 SENDER SIDE:

The proposed system can be implemented by taking the Color photograph containing the faces which are to be safeguarded. The image size is calculated take as N*N matrix .Then the image pixel values are extracted these values ranges from 0 to 2^{24} since there are total of 24 bits from three planes of red ,blue and green with eight bits for each plane.

The system implementation is shown in figure 4.1 as follows:

1. The number of faces present in the Color photograph are detected and extracted using the algorithm mentioned in section 2.1.
2. The faces which are extracted in step1 are encrypted using fractal image finite field cosine transform mentioned in sections 2.2 and 2.3
3. The encrypted faces are then embedded back in to the original image named as cipher face image.
4. The message is prepared which is used after de embedding the image.
5. Modified LSB steganography using chaos is implemented on the cipher face image to hide the message which is generated in step 4 for decrypting the face.



470	107	84	84
329	104	93	93
580	126	90	90
178	134	90	90
74	101	93	93

Figure 4.1: Proposed method: Sender side

Terminology used in encryption and embedding algorithms.
Original Color photograph – **OCP**,
Face information data: information of all faces consists face position, height and width.
Original image for fractals – **OIF**,
Cipher face 1 or encrypted face with fractal image encryption algorithm – **CF 1**
Cipher face 2 or encrypted face with FFCT algorithm – **CF 2**
Ciphered photograph (CP): Original Photograph inserted with cipher faces

4.1.1 FACE DETECTION AND EXTRACTION PHASE:

Detection of face from the original image is performed by using the face detection method, mentioned in section 1 of chapter 2.An input image of size 1024 *1024 is considered and then the gradient of the image is calculated by taking the mean of all the pixels intensities of the image.Face detection algorithm is implemented. Once the faces are detected the face information data is selected. The face information consist the starting pixel position, size i.e., face width and height of each face. Using the face information the faces are cutted out from the image and stored in a file for encryption purpose. Encryption is done in two phases.

4.1.2 ENCRYPTION PHASE:

The faces which are detected will be the inputs to the encryption phase. Each face is considered for encryption and cipher face is derived, similarly all the faces are encrypted and cipher faces derived. The size of the face considered in proposed method is 128*128.

The face is the input image for encryption algorithm. Size of the face is altered with the required width and height. Image is then first encrypted with fractal image algorithm mentioned in chapter 2, section 2.3. Cipher face 1 is the output of fractal image encryption algorithm. Taking cipher face 1 as input image, FFCT algorithm is implemented to get cipher face 2.

4.1. 2. 1 PSEUDORANDOM KEY GENERATION USING THE FRACTAL IMAGES:

The receiver and sender both having a common image called original image (OIF) for generating fractals. Using this image the fractal images are generated using the method mentioned in section 2.3. If there are 2^k fractal images F_1, F_2, F_3…….F_{2^k}, are available on both sides of communication, only **S,** where $S \leq 2^k$, number of fractal images are chosen for key generation. Hence S is a variable of the system key. Fractal images selected for the key generation will be having same resolution as the plain image. The proposed system uses S=8 which means eight fractal images are selected from the available 2^k fractal images[4].

The key stream is generated by zig zag scanning all the 8 fractal images by reshaping each into a matrix and the finally XOR ing the resulting reshaped fractals. This method is shown in the figure.

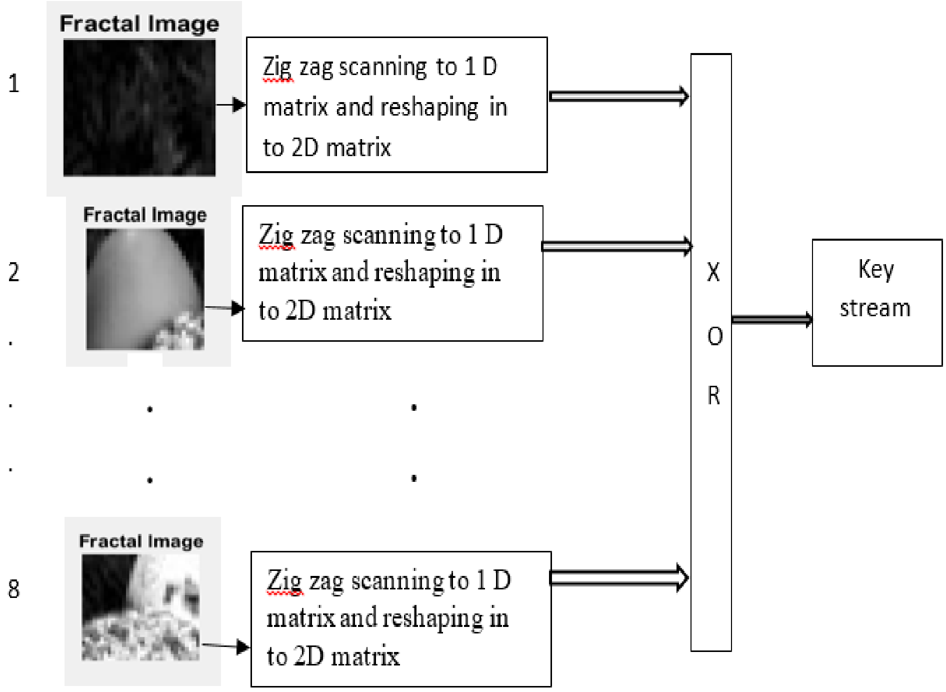

Fractal Image
1
Zig zag scanning to 1 D matrix and reshaping in to 2D matrix
Fractal Image
2
Zig zag scanning to 1 D matrix and reshaping in to 2D matrix
Fractal Image
8
Zig zag scanning to 1 D matrix and reshaping in to 2D matrix
X O R
Key stream

Figure 4.3: Generation of key stream from fractal images

4.1.2.2 ENCRYPTION ALGORITHM:

PHASE 1. (FRACTAL IMAGE ALGORITHM)

Step i. The key stream is generated by selecting the fractals, scanning the each fractal in zig zag fashion and reshaping into matrix and finally XORing eight reshaped fractals.
Step ii. Encryption of each face is done by bit by bit XORing with the key stream generated in step 1 to get CF1.

PHASE 2. (FFCT ALGORITHM)
Step iii. Cipher face 1 which is of size 128*128 is divided in to 8*8 blocks and FFCT is applied to each block.
Step iv. The transformed 8*8 sized blocks are then grouped to get the cipher face 2.
Repeat all the above 4 steps for all the faces detected in the photograph to get the cipher faces. The procedure is shown in the figure 4.4

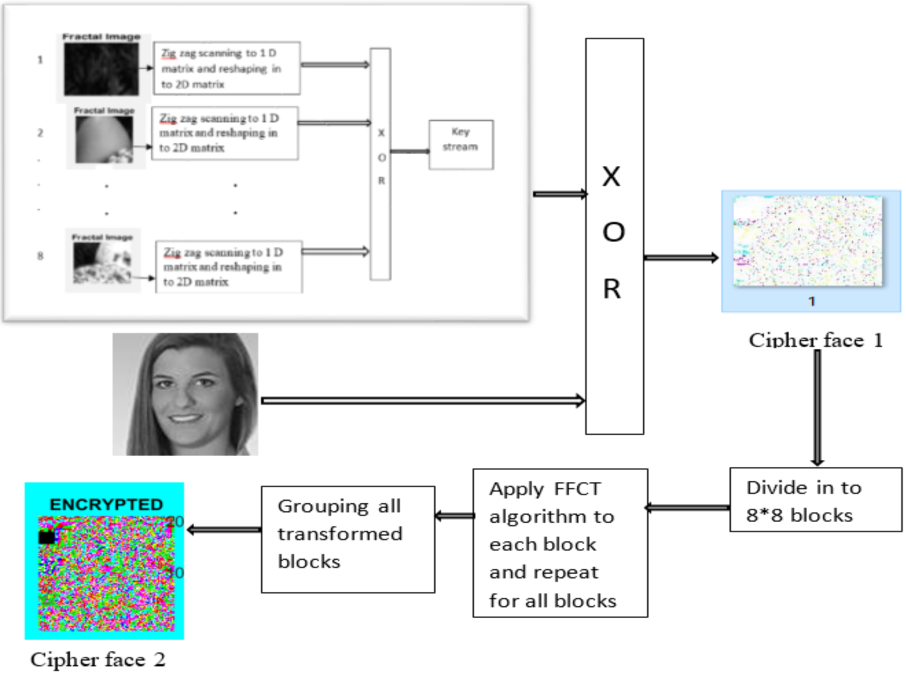

Fractal Image
1
Zig zag scanning to 1 D matrix and reshaping in to 2D matrix
Fractal Image
2
Zig zag scanning to 1 D matrix and reshaping in to 2D matrix
8
Zig zag scanning to 1 D matrix and reshaping in to 2D matrix
X O R
Key stream
X O R
1
Cipher face 1
Divide in to 8*8 blocks
Apply FFCT algorithm to each block and repeat for all blocks
Grouping all transformed blocks
ENCRYPTED
Cipher face 2

Figure 4.4: Encryption procedure

4.1.3 Imbibing the cipher faces in the original photograph (OCP):

Using the function available in MATLAB tool box the cipher images are reinserted in the place of original faces. The function takes the original photograph, the face information data and the cipher faces generated as inputs for implanting the reinsertion of cipher faces in the photograph.

The procedure is shown in the figure 4.5.

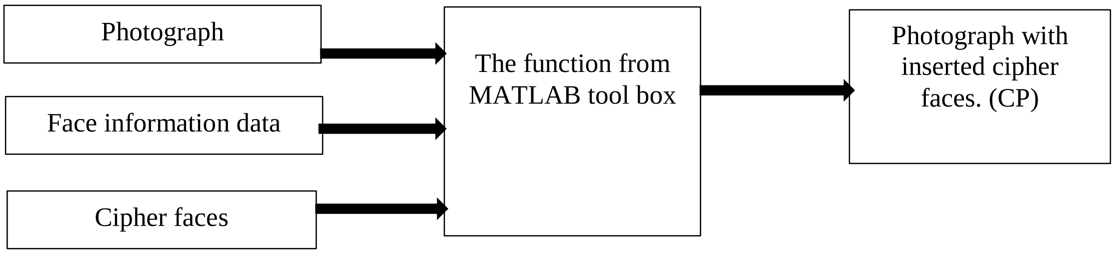

Photograph
Face information data
Cipher faces
The function from MATLAB tool box
Photograph with inserted cipher faces. (CP)

Figure 4.5: Imbibing the cipher images in the photograph

4.1.4 Modified LSB technique Using chaos:

The user needs the face information date for recovering the faces once it reaches in the destination. So in this section the message is generated form the face information and also discuss the method of hiding the message.

The message consisting the face information data is hidden in CP to send the information undetected by the third party by Modified LSB stenographic method implementation. This implementation provides security such that only authorised user can decrypt the faces by using the correct keys.

The message consists of two fields, one is for size of the data and second is the data itself. For one face the message has two parts but if there are more number of faces the fields are again subdivided. The format of message is shown in the figure. For example from figure the data field consist of 152 which is position of x, 15 is position of y, then height is 42 and width is 34.

SIZE	DATA
013	152-15-42-34

Figure 4.4: Format of message

4.1.4.1 Algorithm for segmentation technique:

The method of embedding the message in the photograph contained cipher faces is mentioned in section 2.4 of chapter 2. This method is implemented in the proposed algorithm. The parameters used for initial values of x, y, z and a, b, c which gives the position of pixel in which the LSB bit has to be replaced are defined . Mutual agreement of users is compulsory for defining the values of parameters. In our proposed method the value of z is 0, since the position of pixel is two dimensional.

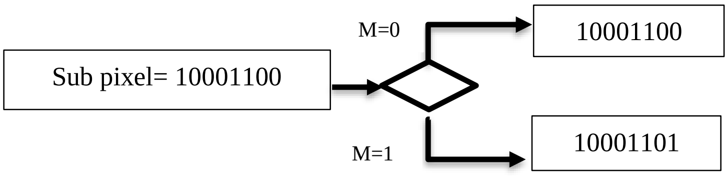
In this method of steganography the message generated is hided in the photograph contained the cipher images called CP. The CP is divided in to RGB sub pixels each of 8 bits. The pixel values will be in the range from 0 to 2^{24} . Once the hiding of message is done then the image is called as stegophotograph.

The Algorithm is as follows:

Step 1. Convert the message M in to stream of binary bits.

Step 2. The selection of sub pixel position form the CP is generated using the discussed method in section 2.4, chapter 2.

Example:



Step 3. Compare the message bit with the LSB bit of sub pixel. If both are same no need to change the value, if not replace the bit as shown in example.

Step 4. Repeat the steps 2 and 3 until the all the bits are hidden in the photograph CP.
After the four steps the stegophotograph is obtained.

4.2 RECEIVER SIDE:

The receiver gets the Stegophotograph which contain cipher faces, face information data included in it. To get back the Photograph with original faces first DE embedding algorithm has to be implemented to get the face information data and the with the face information data the cipher faces are extracted and then cipher faces are decrypted first by applying IFFCT and the XORing with the fractal images. The Procedure is shown in figure 4.2. The phases of the algorithm are followed:

a. **RECOVERING THE FACE INFORMATION DATA:** Applying the initial position values of x, y, z and defining the values of a, b, c (from sec 2.4 chapter 2) the position of the pixel is derived and then the pixel value is considered for recovering the message bit from LSB of the of pixel value. This step is repeated until all the bits of message are recovered.

b. **EXTRACTING THE CIPHER FACES FROM THE CIPHERED PHOTOGRAPH:** With the message recovered in phase 4.1, the information about number of faces, position of faces are determined. Then the cipher faces are extracted out from the CP.

c. **DECRYPTING THE CIPHERED FACES:** The decryption of the ciphered faces which are extracted in phase 4.2 is explained in this phase.

i.APPLYING THE IFFCT ALGORITHM: One cipher face is considered first for decryption and is repeated for all the cipher faces. Each cipher face is resized and the divided in to 8*8 blocks .The apply the IFFCT algorithm , explained in the section 2.2 to get back the original block.
After applying the IFFCT all the blocks are grouped to get back the cipher face 1.

ii.XORING WITH THE GROUPED FRACTAL IMAGES: The cipher face 1 is XORed with the key stream generated in the step 1 of 4.2.2 section.

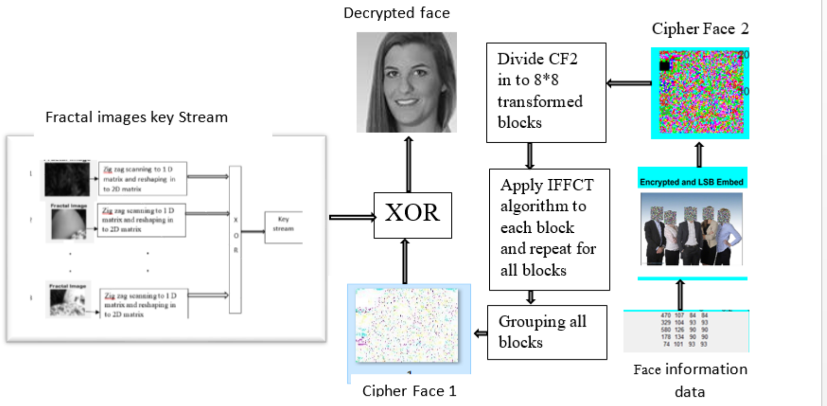


Figure 4.5: Decryption of cipher face 2

The two sec 5.3.1 and 5.3.2 are repeated until all the faces are decrypted.

d. **RECONSTRUCTING THE ORIGINAL PHOTOGRAPH:** After reconstructing all the faces, the faces are inserted in the photograph using the face information data.

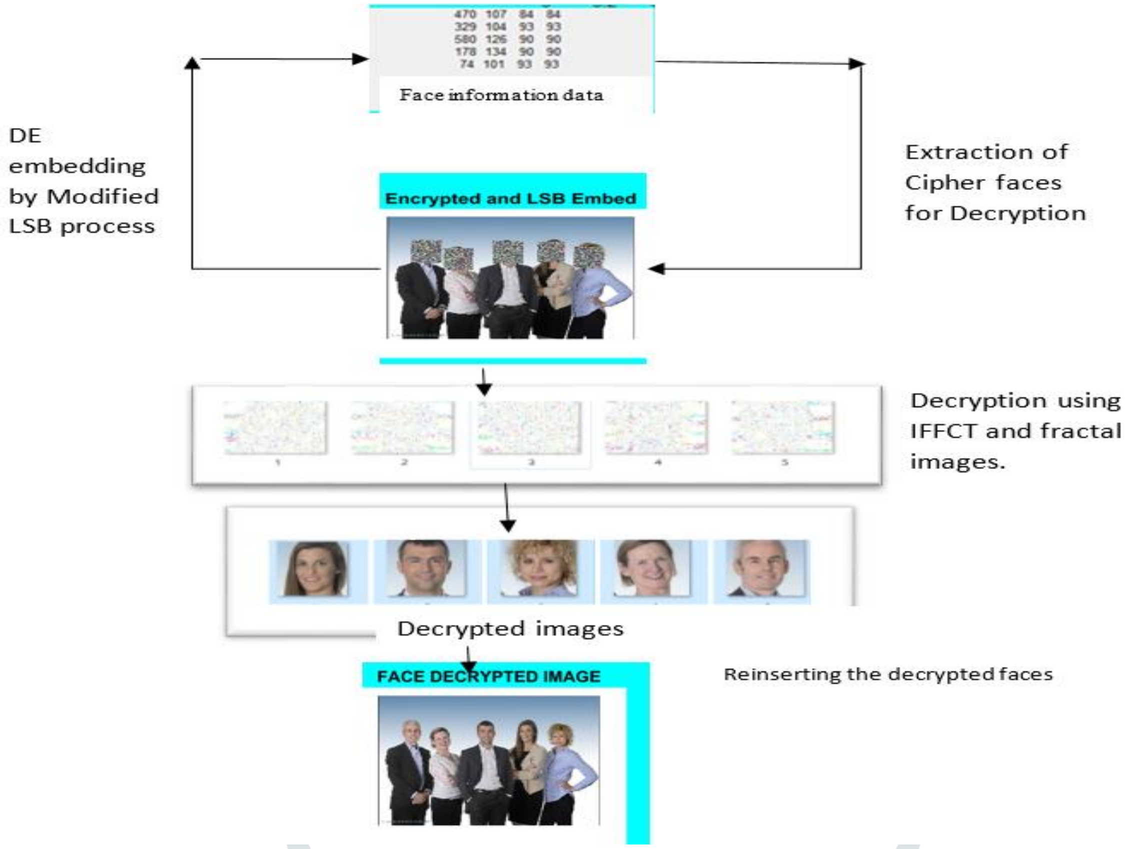

470 107 84 84
329 104 93 93
580 126 90 90
178 134 90 90
74 101 93 93
Face information data
DE embedding by Modified LSB process
Extraction of Cipher faces for Decryption
Encrypted and LSB Embed
Decryption using IFFCT and fractal images.
Decrypted images
FACE DECRYPTED IMAGE
Reinserting the decrypted faces

Figure 4.2: Proposed method: Receiver side

5. Experimental Results .

1) The uniform histograms in figure 5.1 refers to equal distribution of all the intensity values decreases the predictability of information.
2) Figures 5.2 and 5.3shows the correlation values of the encrypted face are nearing to zero which refers the less correlation between the adjacent pixels in the cipher face.
3) The correlation between the original face and decoded face shown in figure 5.4 is nearing to 1 which refers the efficiency of the proposed algorithm.
4) The predictability of random source is measured by the parameter Entropy. If the value of entropy is 8 then the unpredictability of random source is high. The entropy of recovered Lena image shown in table 5.1 is nearing to 8.The Comparisons are made with existing methods.
5) The PSNR and correlation are calculated between the photograph of original faces and recovered stego photograph refers the efficiency of the stenographic algorithm.
6) Measure of sensitivity is implemented on standard Lena image, Q1 is cipher image of original Lena and Q2 is cipher image of Lena with small change. From figure 5.4, as mentioned in 3.1.4 phase ii , The proposed method is very sensitive to small changes.
7) Measure of sensitivity is implemented on standard Lena image, Q1 is cipher image of original Lena and Q2 is cipher image of Lena with small change in key. From figure 5.5, as mentioned in 3.1.4 phase ii, the proposed method is very sensitive to small changes.

5.1 Figures and Tables

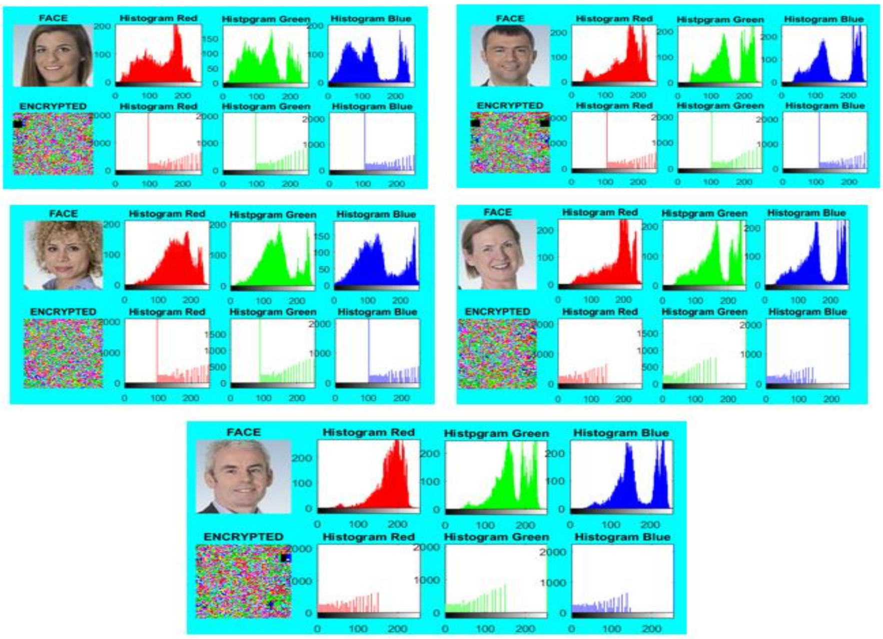


Figure 5.1: The histograms of extracted faces and their cipher faces

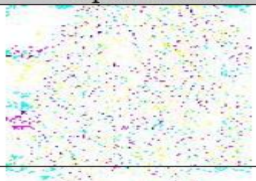
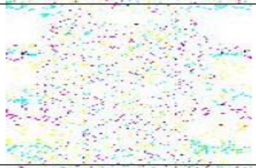
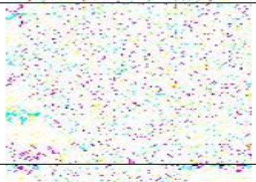
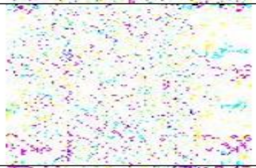
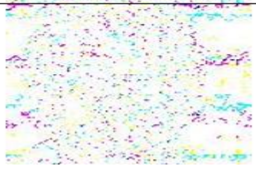
Original Faces	Correlation Values		Cipher Faces	Correlation Values	
	HR	0.975983		HR	0.25946
	VR	0.987212		VR	0.250502
	DR	0.963904		DR	0.171579
	HR	0.968472		HR	0.26602
	VR	0.981789		VR	0.240748
	DR	0.950735		DR	0.198055
	HR	0.959856		HR	0.1565
	VR	0.962932		VR	0.16124
	DR	0.932062		DR	0.11014
	HR	0.970578		HR	0.21481
	VR	0.980245		VR	0.201414
	DR	0.932062		DR	0.163259
	HR	0.956323		HR	0.29505
	VR	0.980245		VR	0.26067
	DR	0.9577411		DR	0.201049

Figure 5.2: The correlation values of original faces and their cipher faces

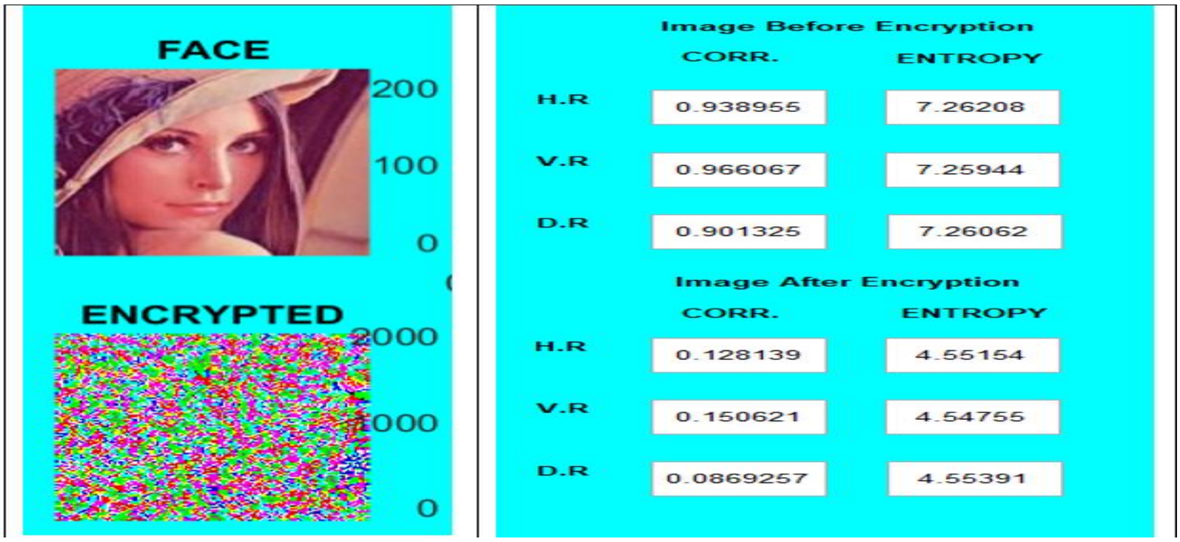


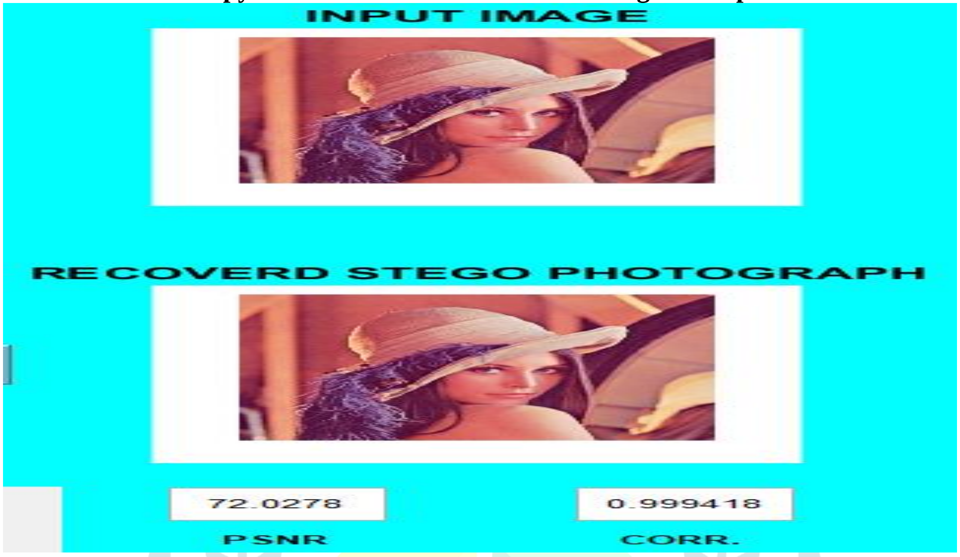
Image Before Encryption

	CORR.	ENTROPY
H.R	0.938955	7.26208
V.R	0.966067	7.25944
D.R	0.901325	7.26062

Image After Encryption

	CORR.	ENTROPY
H.R	0.128139	4.55154
V.R	0.150621	4.54755
D.R	0.0869257	4.55391

Figure 5.3: Correlation and Entropy Values of the Standard Lena Image on Implementation of Proposed Method



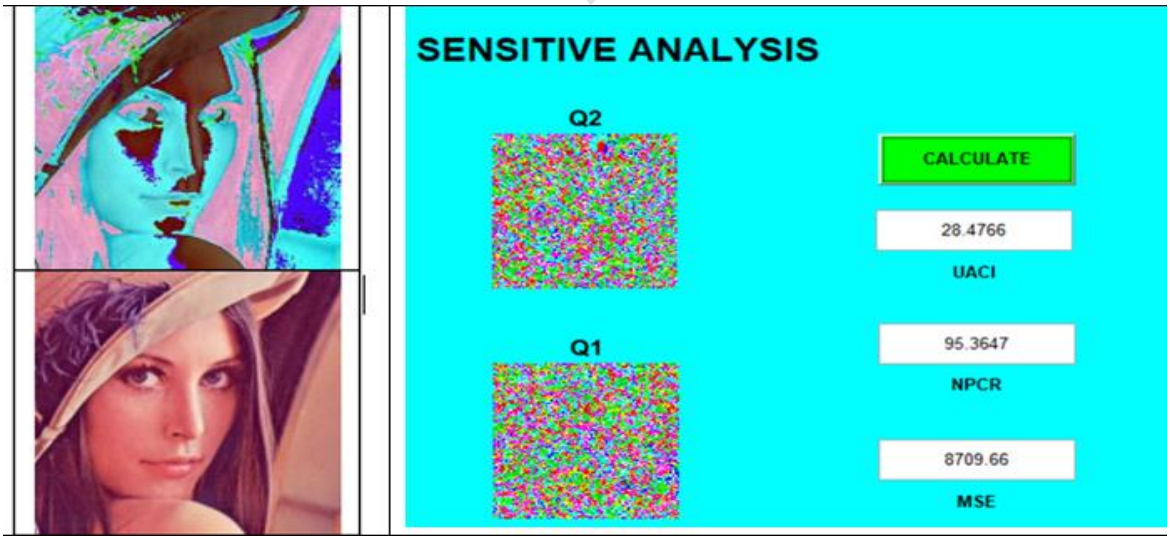
PSNR: 72.0278

CORR.: 0.999418

Figure 5.4: PSNR and Correlation between original photograph and recovered photograph

Table 5.1: Entropy analysis

Entropy	Method
7.855	proposed
7.9855	[14]
7.9560	[21]
7.9970	[20]
7.9969	[22]

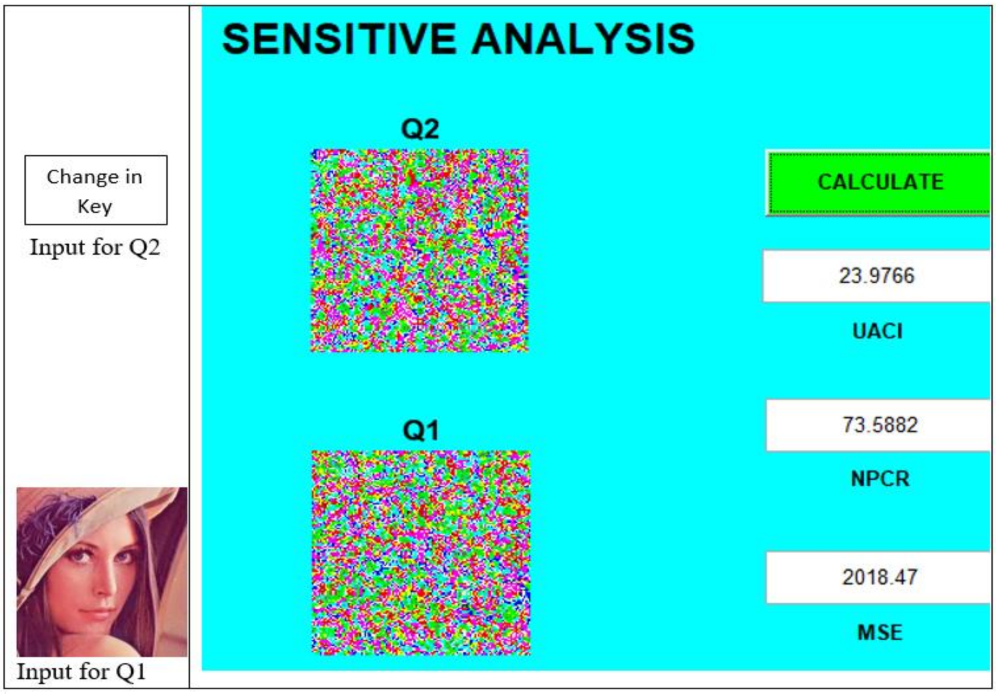


UACI: 28.4766

NPCR: 95.3647

MSE: 8709.66

Figure 5.5: Sensitive analysis for small change in original face



SENSITIVE ANALYSIS

UACI: 23.9766

NPCR: 73.5882

MSE: 2018.47

Figure 5.6: Sensitive analysis for small change in key

6. CONCLUSION

The proposed system is an efficient method for securing the faces in the photograph, since two level encryption algorithms and a steganography algorithm are used. The detection of faces is a bit tough process with the tools from MATLAB, since some other regions also recognised as faces. Matching the sizes of the faces in different phases of the proposed method is challenging. The robustness of the proposed method is thoroughly analysed with the help of different parameters like, correlation, entropy, histogram analysis and also by differential attacks.

7. REFERENCE

1. Jianguo Wang , Tieniu Tan 2000 , A new face detection method based on shape information, National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Sciences, P.O. Box 2728, Beijing 100080, People's Republic of China, Received 5 October 1998; received in revised form 17 November 1999:463-471.
2. Zhong-Qiu Zhao, Member, IEEE, Peng Zheng, Shou-tao Xu, and Xindong Wu, Fellow , 2019, Object Detection with Deep Learning: A Review, IEEE Transactions On Neural Networks And Learning Systems.
3. D. Arun Kumar, B.Inian 2019, Face Recognition Based New Generation ATM Machine”,5th International Conference on Advanced Computing & Communication Systems (ICACCS):1-19.
4. P. S. Addison, 1997, Fractals and Chaos: An Illustrated Course, CRC Press.
5. A. J. J. Lock, C. H. Loh, S. H. Juhari, and A. Samsudin , May2010 , Compression-encryption based on fractal geometric, in Proceedings of the 2nd International Conference on Computer Research and Development(ICCRD’10):213–217.
6. Qizheng Wang, Ling Gao, Hao Wang, And Xiaochao Wei, 2019 IEEE. Translations , Face Detection for Privacy Protected Images: 2169-3536 .
7. Michel Owayjan, Amer Dergham, Gerges Haber, Nidal Fakih, Ahmad Hamoush, Elie Abdo,2013 , Face Recognition Security System , Research gate
8. B.Amos, B.Ludwiczuk, and M.Satyanarayanan, 2016 ,Open Face: A general-propose face recognition library with mobile publications, ,https://cmusatyalab.github.io/open face/.
9. P Buyssens and M Revenu, 2013, Visible and infrared face identification via sparse representation, ISRN Machine Vision, vol.2013, ArticleID579126:10pages,
10. M.Qiu, Z.Jian, J.Ynag, andL.Ye,Fusing , 2015, two kinds of virtual samples for small sample face recognition ,Mathematical Problems in Engineering,Article ID 280318:p.10.
11. J. B. Lima, 2015,Fast algorithm for computing cosine number transform,Electronics Letters, vol. 51, no. 20: 1570–1572.

12. M.M .D’Souza, H.M.deOliveira , R.M. deSouza , and M.M. Vasconcelos, , 2004, The discrete cosine transform over prime finite fields,” in Telecommunications and Networking—ICT 2004: 11thInternational Conference on Telecommunications, Fortaleza ,Brazil, August1–6, 2004.Proceedings,vol.3124 of Lecture Notes in Computer Science, Springer, Berlin, Germany: 482–487.
13. J.B.Lima and R.M.C.D’Souza,2012, Histogram uniformization for digital image encryption, in Proceedings of the 25th Conference on Graphics, Patterns and Images (SIBGRAPI ’12), IEEE, Ouro Preto, Brazil: 55–62.
14. Mervat Mikhail, Yasmine Abouel seoud and Galal ElKobrosy, 2017, Two-Phase Image Encryption Scheme Based on FFCT and Fractals”, Hindawi Security and Communication Networks Volume, Article ID 7367518, https://doi.org/10.1155/2017/7367518: 13 pages.
15. M. Jim´enez Rodr´ıguez, C. E. Padilla Leyferman, J. C. Estrada Guti´errez, M. G. Gonz´alez Novoa, H. G´omez Rodr´ıguez, and O. Flores Siordia, 2018, Steganography applied in the origin claim of pictures captured by drones based on chaos, Ingenier´ıa e Investigation , vol.38, no.2: pp.61– 69.
16. W. Stallings, 2006, Cryptography and Network Security: Principles and Practices, Pearson Education India.
17. N.Rawal and Dhawan, 2013, A survey report on image encryption techniques, International Journal of Engineering Research and Technology, vol.2, no.10.
18. N. Agrawal and, M.Savvides , 2009, Biometric data hiding :A 3factor authentication approach to verify identity with a single image using steganography , encryption and matching , in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, CVPR 2009, Miami, Fla, USA: 85–92.
19. Octavio Flores Siordia ,1 Juan Carlos Estrada Gutiérrez,1 Carlos Eduardo Padilla Leyferman Jorge Aguilar Santiago , and Maricela Jiménez Rodr-guez1, 2018,System to Safeguard the Identity of Persons in Photographs through Cryptography and Steganography Techniques Using Chaos , https://doi.org/10.1155/2018/4853134, Hindawi Security and Communication Networks Volume, Article ID 4853134:16 pages.
20. S. Jayaraman, S. Esakkirajan, T. Veerakumar, 2009, Digital Image Procesing, McGraw Hill Education. Pvt Ltd, New Delhi.
21. M.A.Murillo -Escobar, C.Cruz-Hern´andez, F.Abundiz-P´erez, R. M. L´opez-Guti´errez, and O. R. Acosta Del Campo, “A RGB image encryption algorithm based on total plain image characteristics and chaos,” Signal Processing, vol. 109, pp. 119– 131.
22. U. C¸avus¸o˘glu, S. Kac¸ar, I. Pehlivan, and A. Zengin, 2017, Secure image encryption algorithm design using a novelchaos based S-Box, Chaos, Solitons & Fractals, vol.95, pp.92–101.
23. Z. Parvin, H. Seyedarabi, and M. Shamsi, 2016, A new secure and sensitive image encryption scheme based on new substitution with chaotic function, Multimedia Tools and Applications, vol. 75,no.17:10631–10648.