Mosaic Covert Communication for Data Security

Nagendra M S[1]
PG Student, Department of Electronics & Communication Engineering, Sri Siddhartha Institute of Technology, Tumakuru, Karnataka, India

Manjula Y[2]
Assistant Professor, Department of Electronics & Communication Engineering, Sri Siddhartha Institute of Technology, Tumakuru, Karnataka, India

Dr. M Z Kurian[3]
Professor & Head, Department of Electronics & Communication Engineering, Sri Siddhartha Institute of Technology, Tumakuru, Karnataka, India

---***---

Abstract— The security of the image needs to be warranted when it is directed over Internet. The menace can be deliberate or accidental. Guaranteeing security comes with cost. In many of the cases, only a tiny portion of the whole image contains the sensitive information and only that portion need to be safeguarded. Securing only a small portion of the image is cost-effective, efficient, achievable and easier to implement. To do this, various encryption algorithms put together with Steganography methods are in use. In this work, securing the face in the photo of an individual using two level of encryption is discussed. The face is sliced from the main image and Fractal encryption is applied to get cipher image. Additionally, this cipher image is cosine transformed and the recovery information is lodged using LSB algorithm. Inspired by this, a little modification is proposed to the existing work in which, encryption phase is replaced by Mosaic phase. Mosaic technology is a powerful tool using which real sized images can be completely secured using covert communication. Here, mosaic technique is utilized to hide only a part of the image. Using this method, faces are swapped by Mosaics so that, it is less inclined to Hackers attack. The implementation details and experimental results for Mosaic image creation are briefly discussed. The results were pleasing with high PSNR, less RMSE and high correlation.

Keywords- Image Mosaic; Fractal Images; Cosine transform; LSB hiding

I. Introduction

This is a digital world. Exchange of information over internet had become integral part of life. When data is sent over internet, it is really not safe for lot of obvious reasons. The channel is unsafe for transmission of any type of unprotected data. Hacking, Steganolysis, malwares, cyber criminals contribute in their own way to make the channel an unsafe. Therefore, there is a strong need for ensuring the security and integrity of data. In some cases, unauthorized access to the data needs to be stopped.

Variety of solutions is being practiced since a long time. Encryption and password security are the most common methods. In the recent approaches, as a measure of additional security, the encrypted and password protected data is sent covertly. Cryptography takes care of encryption aspect and Steganography take care of covert communication aspect. Both have their own advantages and disadvantages

A. *Securing Image*

There are various types of data are transmitted over internet such as textual messages, voice messages (audio), various types of photos (image data) and video. They are together called as multimedia content. Various types of data encounter various types of attacks.

The data in the form of an “image” occupies majority of portion of the data being circulated in internet. An image can hold huge amount of data in the pictorial form or, it can be used as a container to hold other form of data. (Example: An image containing hidden text information). In any case, the image needs to be safeguarded from various types of possible attacks.

The definition of “securing an image” varies depending upon the context. In some cases, the whole image need to be safeguarded and in some other case, only a small portion of image need to be safeguarded.

If it is an image containing medical information (x ray report), each and every pixel of image is important and complete image need to be secured. If it is an image containing banking transaction details, the account numbers are the only sensitive information and only that portion need to be secured.

In the similar way, if a photograph of an individual is shared, his biometric information is sensitive and hence, it is good idea to hide/blur only that potion of image (face). This work mainly focuses on securing the face in a photograph of an individual.

B. *Importance of Face*

The biometric information of an individual (iris, thumb impression, marks on the face, eyebrow pattern) is always private and need to be kept confidential. Face contains the majority of the biometric information and additionally, face is the mere basic identity of a person.

Powerful and easily accessible free tools are available for extraction of facial information. Ample of image processing tools are also available using which, the extracted face can be manipulated and used for illegal and harmful activities. A duplicated and edited face can cause damage in various ways. An edited face can harm woman's dignity. An ID card containing duplicated photo can cause potential damage to an organization. Hence, facial information needs to be secured whenever it is shared in a public medium.

II. Conceptual Knowledge Used

A. *Face detection model*

In an image containing the photo of an individual, the face may appear in any position (depending on posture) and can be of any size. The faces may have different aspect ratio also. Using a gliding window, the face can be detected on the whole image [12] - [14].

A built in tool available in MATLAB is used to detect the face. Upon detection of face, the tool will display all the information associated with face (dimension, position etc.). Using a simple piece of code, the face and face related information is extracted. The extracted face and the related information are saved for further processing.

B. *Finite field cosine transforms [FFCT]*

In contrast to regular Cosine transform, finite field Cosine transform is defined for integers so that, it avoids fractional values when computation is done in real time. This method uses a transformation matrix T which is of the order 8 x 8 and results in 1D (one dimensional array). [20]

Let λ be an element whose value ranges from zero to 2N. Let vector y = $[y_0,y_1,y_2,y_3........y_{N-1}]$ is an ID array whose FFCT need to be calculated. Let Y = $[Y_0,Y_1,Y_2,........Y_{N-1}]$ denote the array after transformation. The elements of Y are defined using following equations

$$Y_k=\sqrt{\frac{2}{N}}\sum_{I=0}^{N-1} \partial_k\, y_i \cos \lambda\left[k\,\frac{2i+1}{2}\right] \qquad (01)$$

$$\partial_k = \begin{cases} \sqrt{\frac{1}{N}}, & y = 0 \\ 1, & y = 1,2 \ldots N-1 \end{cases} \qquad (02)$$

The above set of equations yields the result in 1D. Since the image is a collection of pixels in 2D, the one dimensional matrix needs to be converted in to two dimensional matrix.

Let D denote a 2D matrix of the order N x N. Let U denote set of 8 x 8 pixels (because, transformation matrix is of the order 8 x 8). Let q denote a whole number and q= 257. Then the two dimensional matrix D us defined as

$$D=TUT^{-1}\ (\grave{}\mathrm{mod}\ q) \qquad (03)$$

For the construction of matrix U, each pixel id split in to its tree colour plane (Red, Green & blue) and transformation is separately applied to each plane.

Finally, an 8 x 8 FFCT converted coefficients are generated and they are rearranged and replaced to their original positions.

C. Fractal Images

The fractal images are like recursive functions. A recursive function call itself i.e a new (call to a) function is "generated" by present function and this will continue infinitely. Similarly, in Fractal images, an image can be derived from existing images by zooming in the details. There are many examples in nature for Fractal images (Example: a tree structure).

In images processing, fractal images are generated by running a "Kernal" at different scaling and by shifting the positions. Many free tools are available over internet to generate Fractal images. These tools use mathematical equations for fractal image generation. The systems that produce this kind of images are called as "Iterated Function Systems – IFS". The number of Fractal images to be generated depends upon requirements at sender and receiver. In the prosed system, Fractal images are used for two purpose i) Key generation ii) encryption of face [15] [16].

Key generation: 8 fractal images are generated (2D) and they are converted into one dimensional array. Likewise, eight 1D arrays are created and all those arrays are EXORed to generate key.

Face encryption: The fractal images which are generated are EXORed by pixel by pixel and bit by bit to generate encrypted face.

D. Sensitivity

The way in which the system responds for a trivial variation in the input parameters is referred as sensitivity. In the proposed work, encryption key and extracted images are the inputs. Hence, for s small change in either of them, there has to be a drastic change in the manner in which system responds. A good system should have high sensitivity.

Change in Encryption key (with sane face as input): Two keys namely key1and key2 need to be generated. There has to be a minute change (few bits change) between key1 and key2. Taking the same Face as the input, two cipher faces Q1 and Q2 need to be generated using key1 and key2. NPCR, MSE, UACI need to be calculated between Q1 and Q2. If the sensitivity of the system is high, there has to be huge change in these values.

Change in face (with same key as input): A face F1 is extracted and a small change is made to F1 to get F2.Cipher faces Q1 and Q2 are generated using same key. UACI and other parameters need to be calculated between Q1 and Q2. If the values are more, system has high sensitivity.

E. Mosaic Technology

Mosaic system needs two images as input. A container image (Called as target image) and an image containing furtive information (Clandestine image). Target image which is similar to colour distribution and ambiance to that of Clandestine image is selected. If the size of those images do not match, resizing need to be done using arithmetic encoding. The target image may be selected from a pre-existed database [2] [3] [6] [7].

Both of these images are crumbled in to equal sized blocks and the dimension would typically be 4x4, 8x8 or 16x16. The basic parameters i.e mean and standard deviation is calculated for each and every lump. The blocks are arranged such that, one with least mean and standard deviation will be first in the list and with more value, will occupy the last place. A lump of Clandestine image is selected, matched to an appropriate lump of target image; and this process is reiterated for all the lumps of the system. This completes the creation of "mosaic of the target image". The mosaic structure approximately looks like target image and upon quality improvement by colour transformation, it look similar to target image. The mosaicked image will barely attract the concentration of hacker and though it attracts, it is not dangerous with respect to the security of data dwelled..

$$\text{mean}=\frac{1}{n}\sum_{i=1}^{n} k_i \qquad (04)$$

$$\sigma=\sqrt{\frac{1}{n}}\ \sum_{i=1}^{n}(k_i - mean)^2 \qquad (05)$$

The new value of mean is calculated by subtracting it from pixel vale and using which, new standard deviation values are calculated.

F. Chaotic LSB Substitution

For hiding a data using any type of LSB methods, a container / target image is needed. It acts as a carrier for message bit stream. In this work, a colour image (24 bit) is elected and embodied in three colour matrix. Each matrix can clench at least one bit of data. The size of the image is later estimated based on number of pixels. The message to be embedded is transformed into bit brooks. The assortment of pixels into which these bits to be embedded is calculated (selected) based on following set of equations as defined by Chotic algorithm [21].

$$\frac{di}{dt} = -(j+k) \qquad (06)$$

$$\frac{dj}{dt} = (i+pj) \qquad (07)$$

$$\frac{dk}{dt} = q + k(i-r) \qquad .(08)$$

With the predefined initial values, calculation is done using control parameters p, q, r and a pixel is selected for data hiding. This course is iterated for all the message bits

III. Proposed Method

A. *Existing System*

For the realization of proposed system [1] [9] [11], a colour image denoted using 24 bit is selected. The image should of course contain a sensitive information to be protected (it's a face in this case). The image size is calculated in two dimension as N x N. As the image is characterized using 8+8+8= 24 bits, in reality, 224 Combination of colures is possible. But "8 bits" in a group of three is considered.

The system operation is shown in figure 1.

i) Using face extraction algorithm explained in section 2.a, the face and related details are extracted.
ii) The extracted faces will undergo two level of encryption (Fractal encryption followed by FFCT encryption)
iii) All the necessary information for decryption is clinched in to encrypted face using LSB algorithm explained in section 2.f.
iv) The encrypted and "loaded" faces are replaced o their original positions.
v) The "secured" photograph is sent to receiver.

3.1 Face detection and extraction phase:

In the full sized image, only the "region of interest" (it's a face in this case) need to be recognized. This is done using edge detection and other tools available in MATLAB tool. The tool rifts the image into chunks of 1024 x 1024, calculates the pixel intensity and also gradient with respect to central pixel. Exploiting these values, the tool identifies the face along with its allied information (position, size, height and width etc.). With the help of simple piece of code, the faces are sliced from original image and stored in a separate file. In the later stage, two levels of encryption is done on these faces [17] [18].

3.2 Encryption phase (two level of encryption)

The faces which are identified and sliced from the original image are considered as the input for encryption. If there are more than one face is detected, encryption is applied on each face separately. Upon encryption (two level), visible faces are converted in to cipher face. The maximum permissible size for a face in the proposed system is 128 x 128.

The dimension of the faces is altered if needed by encryption algorithm. In the first phase of encryption, Fractal image technique is applied to derive cipher face 01. This acts as input to the upcoming phase. Here, already encrypted image undergo second level of encryption using FFCT technique. The final outcome is cipher face-02. [9] - [11].

3.3 Generation of Random key using Fractal images

A "Unique Image – UI" with same resolution are used at both sender and receiver for Fractal image generation. Conceptually, infinite number of Fractal images can be generated. In this work, it is assumed that 2^k images are generated out of which, only "G" [Where $G<2^k$] number of Fractal images are selected for key generation. G is a predetermined system constant and in the present case, G=8. So, 8 Fractal images [out of 2^k images] are considered for key generation. All the eight

Fractal images are of same resolution. Fractal images are 2 Dimensional and hence, they are transformed into 1D by "Zig-Zag" scanning. Each Fractal images yield single 1D array. Later, all the eight 1D arrays are EXORed to get the key. Once key generation is complete, all the one dimensional arrays are reverted back to two dimensional arrays.

3.4 Swapping original face with Cipher face

The original faces are swapped with encrypted faces (cipher faces) by using the built in functionality of MATLAB. While doing so, the tool considers Face and the allied information as the input. Exploiting which, the actual coordinates of the face is identified [9].

The existing face field id deleted and vacant place is filled with cipher face. Hence, the facial information is "secured".

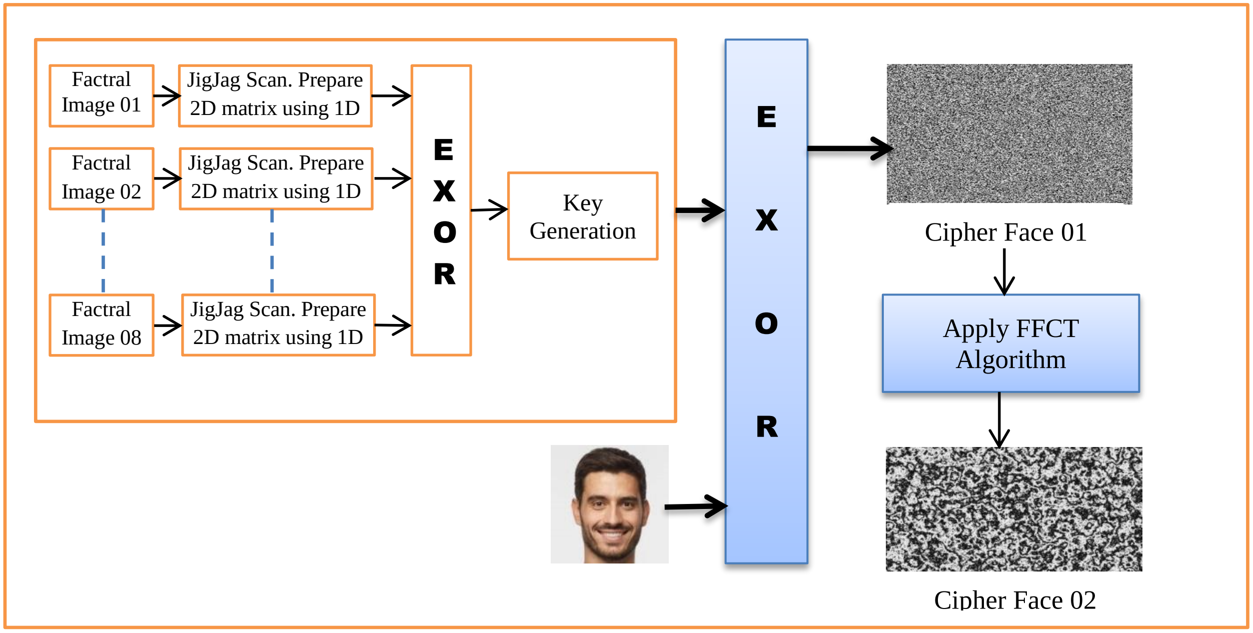


Figure 1. Face Encryption using Fractal images and FFCT transform

3.5 Choes based BSB method

At the receiving end, decryption need to be done on cipher face to get original face; to do this, "facial information" is needed at receiver also. This information is required to be sent to receiver confidentially along with cipher faces. For this reason, LSB methods are employed.

The facial information (which is now in a form of bit stream) is clinched into pixels of cipher face using algorithm explained in section 2.f. Only authorized user who knows the values used at sender (p, q and r values) can decode this information.

B. Upgraded system

The existing system is very much efficient in terms of encryption and associated security. It performs well in terms of sensitivity, NPCE and UACI. But the method can still be improved in terms of following points.

1. After two levels of encryption, the encrypted image looks like a noise image. This will easily grab the attention of a hacker
2. Off the two encryption methods, one is from frequency domain (Cosine transform) and the other is from spatial domain.
3. Set of dots in the place of face – does not give pleasant visual experience.
4. Generating Fractal images from the same Unique Image every time – an alternative method sounds better.
5. As there are 2 levels of encryption, they system implementation could become complex.

A new method which shows improvement upon all the above points can be implemented using "image mosaic" technology. Using mosaic method, a whole image can be sent securely or, a *selected portion* of the image is safeguarded by masking the sensitive area with mosaics. The second application is explained on the following section. Upgraded system is shown in Fig. 4.

3.6 Mosaic Covert Communication for data security

As such, "Image Mosaic" is an efficient technology [2] – [6] using which, a complete image can be hidden (morphed) in anther image and can be sent securely. Figure 02 and Figure 03 shows the implementation details of mosaic technology. In Fig 2, generic block diagram is explained and figure 5 shows the MATLAB implementation. Table 01 details the experimental results. Mosaic concept is explained in detail in section 2.e.

Following are the steps involved in creating a "mosaic" of an image (usually called target/cover/container image) using another image (Usually called Clandestine/message/data image).

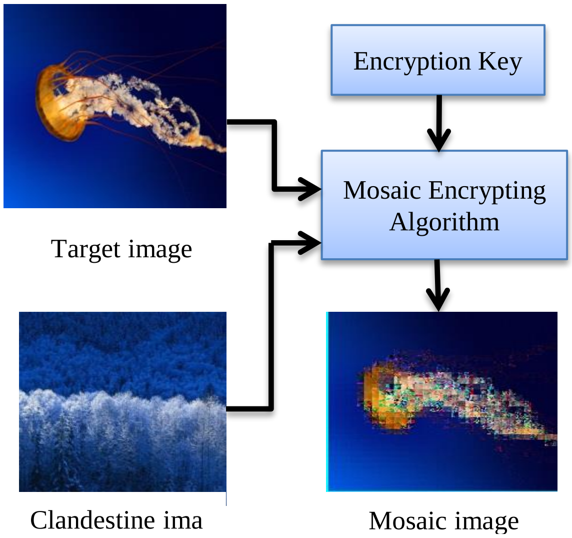
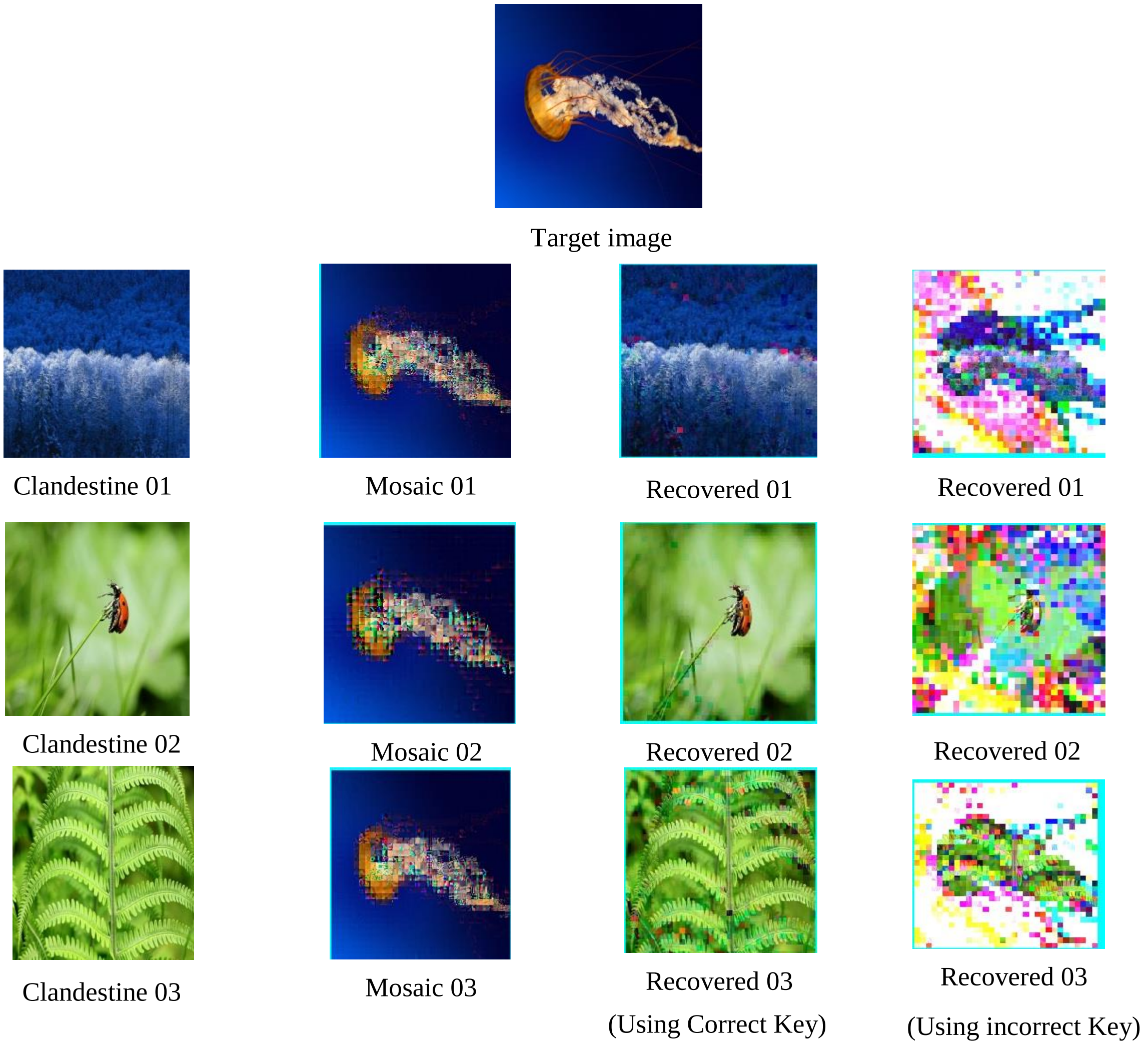


Figure 2. Mosaic Creation flow chart



Target image

Clandestine 01 Mosaic 01 Recovered 01 Recovered 01

Clandestine 02 Mosaic 02 Recovered 02 Recovered 02

Clandestine 03 Mosaic 03 Recovered 03 (Using Correct Key) Recovered 03 (Using incorrect Key)

Figure 3. Mosaic creation, Recovering of Clandestine image using correct key and incorrect key

Usually two images of approximately same size and similar background are selected.

1. The image to be sent securely and clandestinely is called image 01 and the other image is called image 02.
2. Both the images are split into small but equal sized shards. (Usually, 4x4 or 8x8. In some cases, rectangular shape).
3. For the two sets of shards so generated, mean and standard deviations are calculated.
4. Shards are then arranged in the increasing order of their standard deviation.
5. Based on calculations as explained in section 2.e, "most matching" shards of one set (image 01's set) are mapped to the shards of another set (image 02's set). This process is repeated for all the shards of the two sets. The number of pieces (shards) in the two sets is equal; there will be a "one-to-one" mapping. A rough mosaic is created. It is needed to manipulate the rough mosaic to look like an "image". Following steps take care of that aspect.
6. Colour transformation is applied on each piece based on equations 04 and 05.
7. If further fine tuning is needed, the shards are little tilted in all 360 degree. To decide upon this angle either RMSE or PSNR or any other aspect is taken as reference.
8. All the above mentioned procedure can be controlled with a key [8].
9. The recovery information is generated and it needs to be shared with receiver.

10. The key used and the recovery information – are embedded into mosaic image itself using various LSB insertion technologies.

3.7 Securing the face in the image of an individual using Mosaic

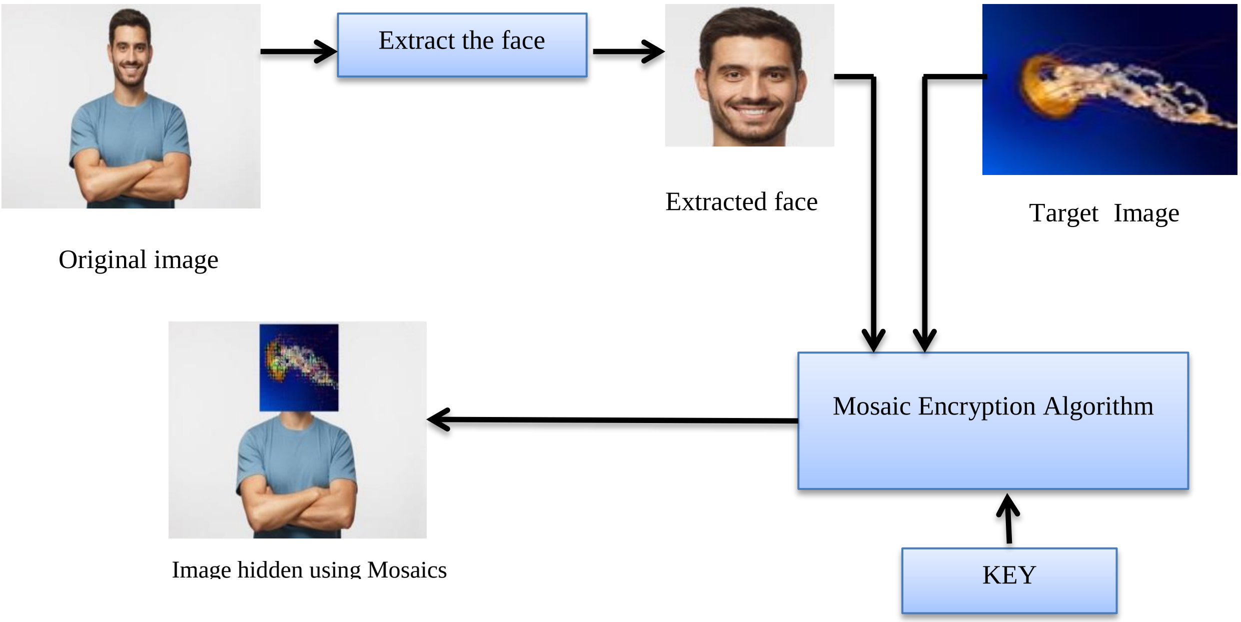


Figure 4. Securing the face using Mosaic Encryption

The mosaic technology explained so far can also be used to hide (secure) any sensitive part of the image (Example : 'Face' of an individual's photo, 'account number' in the fund transfer screenshot etc) Figure 04 explains how the face of a person can be secured using Mosaic technology Following steps explains it in detail.

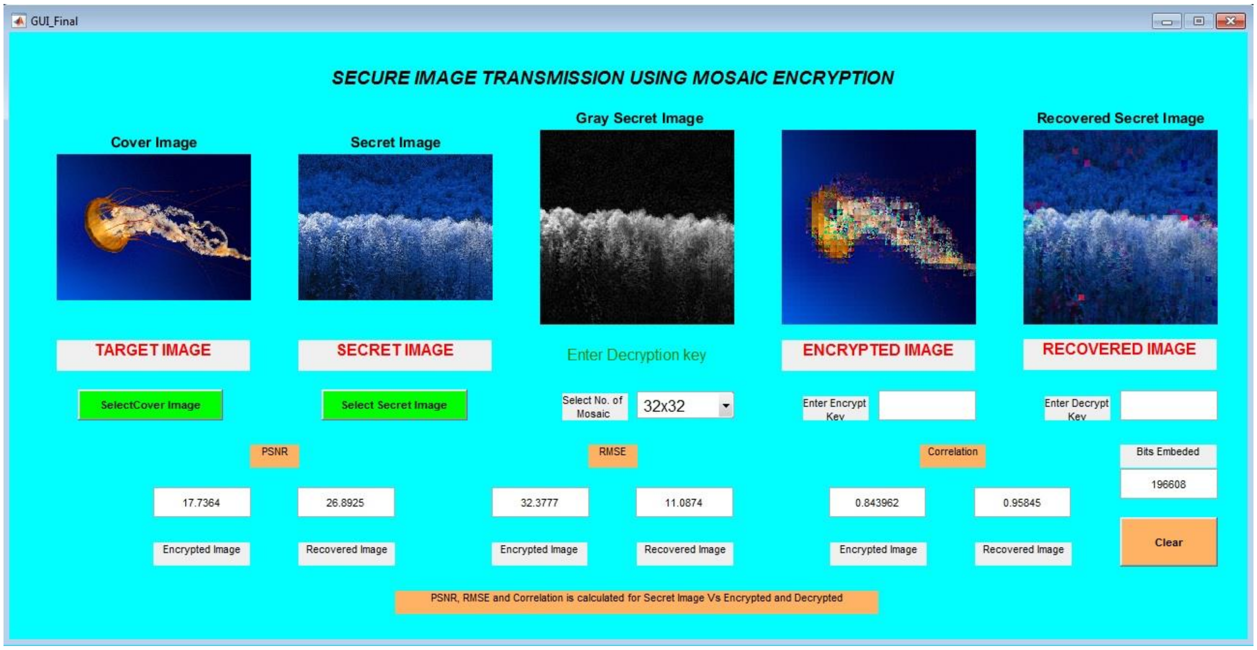
1. The sensitive area of the image considered is identified. (It is "face" in the example considered).
2. The face is extracted using the process explained in section 2.a. The height, width and position of the face is noted down which constitutes to face recovery information.
3. A "suitable" target image is taken. The target image so considered should be from similar background and colour contrast.
4. Fractal images are generated out of Target image and encryption key is generated using these Fractal images as explained in section 2.c.
5. Using the Face, target image and the key generated in step 4, a mosaic image is generated using mosaic encryption algorithm explained in section 2.e. Mosaic recovery information is noted down. The mosaic image is superimposed in the place of actual face. Thus, the sensitive area is secured!
6. The face information generated in step 1, the fractal key generated in step 4, the mosaic recovery information generated in step 5 – are gathered together and converted into bit stream.
7. All these information are needed in receiver side.

8. The bit stream generated in step 7 is embedded into mosaic area using any LSB method. Chos based LSB in the present system

9. The "loaded" image of step 8 is sent to receiver.

To implement the upgraded system, few of the technologies from the existing systems are used (Face identification, Face extraction and replacement).Instead of FFCT encryption, mosaic encryption is used. (Which is implemented and results are explained in next section). A modified version of fractal key generation is used. Here fractal images are generated using target image. For LSB hiding, existing LSB algorithm is used. The mosaic creation and Clandestine image regeneration is fully implemented. The development of rest of the sub systems the integration of various systems is planned for future.

IV. Experimental Results



Select No. of Mosaic: 32x32
Enter Encrypt Key:
Enter Decrypt Key:

PSNR: 17.7364 Encrypted Image | 26.8925 Recovered Image
RMSE: 32.3777 Encrypted Image | 11.0874 Recovered Image
Correlation: 0.843962 Encrypted Image | 0.95845 Recovered Image
Bits Embeded: 196608

PSNR, RMSE and Correlation is calculated for Secret Image Vs Encrypted and Decrypted

Figure 5. Mosaic creation and recovering original Image using MATLAB

Figure 3 shows how various Clandestine images are tried with a target image. Table 01 summarises the results for all the combinations shown in Figure 3. Figure 5 shows the MATLAB screen for one combination (Clandestine 01 with target image). Following are the observations

Table 1. Results of Mosaic Creation and recovery of Clandestine image

Target Image	Clandestine image	PSNR between		RMSE between		Correlation between	
		Encrypted Image	*Recovered Image*	*Encrypted Image*	*Recovered Image*	*Encrypted Image*	*Recovered Image*
Target 1	*Clandestine 1*	17.7364	26.8925	32.3777	11.0874	0.843962	0.95845
	Clandestine 2	16.4197	28.5508	37.8199	8.63242	0.785902	0.978359
	Clandestine 3	17.7947	28.5508	32.0765	8.63242	0.844649	0.978359

1. The mosaic created successfully "morphs" the target image. The mosaic image nearly looks like a target image in a quick glance. That was the basic requirement.
2. The Clandestine image can be successfully regenerated using the correct key.
3. The Clandestine image *cannot be reconstructed* at the receiver end if user enters a *wrong key*. The recovered image looks like noise image. This ensures the security

4. There is a high PSNR between Clandestine image and recovered image. It means that, less noise is added during mosaic encryption and recovery process.
5. PSNR between Clandestine image and mosaic image is less; means that, lot of noise is present in mosaic. Hence, it is tough to extract Clandestine image directly from mosaic image without a proper key.
6. Similar comments holds good for RMSE values. There is very less RMSE ("error"!!) between Clandestine image and recovered image. Also, there is lot of error (high RMSE value) between Clandestine image and mosaic image. Both the cases contribute to rise in the security of mosaic encryption.
7. There is a high correlation (more then 0.9) between Clandestine image and recovered image. It infers that, recovered image is almost similar to Clandestine image.
8. There is less correlation between Clandestine image and mosaic image. This is an expected quality. Lesser the correlation, tough to guess the Clandestine image from mosaic image.
9. Mosaic creation and recovery of Clandestine image from mosaic – takes very less computational time using MATLAB tool. (Few milliseconds).

V. CONCLUSION

Securing the sensitive part of an image is an important challenge being encountered when an image is sent over internet. Extracting only the sensitive area (face) and applying two levels of encryption (Cosine transforms and Fractal encryption) was explained. Though this method ensures security, noise like image is always prone to attracting the interest of a hacker. Therefore, a new way of securing the sensitive portion using image mosaic was explained. Mosaic technology is a powerful tool exploiting which, complete image can be sent covertly. In the proposed system, it is used for securing only the sensitive area. Experimental results of Mosaic technology were satisfactory. There was a high PSNR, less RMSE and high correlation between Clandestine image and reconstructed image. The proposed method has lot of scope for further enhancement.

VI. REFERENCES

[1] Manjula Y and K B Shivakumar, " Secured Image Transmission Using Color Transformation Fragmented Mosaic, Chaos Based Encryption and LSB – Mapping Steganography Technique," Biosc.Biotech.Res.Comm. Special Issue Vol 13 No 13 (2020) Pp-58-66 Print ISSN: 0974-6455 Online ISSN: 2321-4007 CODEN: BBRCBA, doi: http://dx.doi.org/10.21786/bbrc/13.13/9

[2] Manjula Y and K B Shivakumar, "Secured Face Identity of Image Photograph by FIFFCT and Selective LSB Hiding Technique," Biosc.Biotech.Res.Comm. © 2020 JETIR July 2020, Volume 7, Issue 7: ISSN-2349-5162 doi: 10.6084/m9.jetir.JETIR2007042, https://www.jetir.org/view?paper=JETIR2007042

[3] I. Lai and W. Tsai, "Secret-Fragment-Visible Mosaic Image–A New Computer Art and Its Application to Information Hiding," in IEEE Transactions on Information Forensics and Security, vol. 6, no. 3, pp. 936-945, Sept. 2011, doi: 10.1109/TIFS.2011.2135853.

[4] D. G. Singhavi and P. N. Chatur, "A new method for creation of secret-fragment-visible-mosaic image for secure communication," 2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Coimbatore, 2015, pp. 1-5

[5] Li YL., Tsai WH. (2011) New Image Steganography via Secret-Fragment-Visible Mosaic Images by Nearly-Reversible Color Transformation. In: Bebis G. et al. (eds) Advances in Visual Computing. ISVC 2011. Lecture Notes in Computer Science, vol 6939. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-24031-7_7

[6] A. S. Chavan and A. A. Manjrekar, "Data embedding technique using secret fragment visible mosaic image for covered communication," 2015 International Conference on Information Processing (ICIP), Pune, 2015, pp. 260-265, doi: 10.1109/INFOP.2015.7489390.

[7] N. V. Gaikwad and S. P. Metkar, "Improving the visual quality of secret fragment visible mosaic image," 2016 Conference on Advances in Signal Processing (CASP), Pune, 2016, pp. 207-211, doi: 10.1109/CASP.2016.7746166.

[8] NN. Meghana and H. Chetan, "A New Method For Secret Image Transmission via Mosaic Fragments using ECC Key," 2019 IEEE International WIE Conference on Electrical and Computer Engineering (WIECON-ECE), Bangalore, India, 2019, pp. 1-5, doi: 10.1109/WIECON-ECE48653.2019.9019933.

[9] Y. Chen, E. J. Lu and C. Wang, "Privacy image protection using fine-grained mosaic technique, " 2013 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference, Kaohsiung, 2013, pp. 1-4, doi: 10.1109/APSIPA.2013.6694264.

[10] S. Kuldiwar and D. Parasar, "Reversible color transmission of compressed fragment-visible mosaic image," 2015 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Madurai, 2015, pp. 1-8, doi: 10.1109/ICCIC.2015.7435751.

[11] Kim, Junhwan&Pellacini, Fabio. (2002). Jigsaw Image Mosaics. ACM Transactions on Graphics - TOG. 21. 657-664. 10.1145/566570.566633.

[12] 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.

[13] 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.

[14] D. Arun Kumar, B.Inian 2019, Face Recognition Based New Generation ATM Machine",5th International Conference on Advanced Computing & Communication Systems (ICACCS):1-19.

[15] P. S. Addison, 1997, Fractals and Chaos: An Illustrated Course, CRC Press. ISBN 9780750304009

[16] 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.

[17] Qizheng Wang, Ling Gao, Hao Wang, And Xiaochao Wei, 2019 IEEE. Translations, Face Detection for Privacy Protected Images: 2169-3536 .

[18] Michel Owayjan, Amer Dergham, Gerges Haber, Nidal Fakih, Ahmad Hamoush, Elie Abdo,2013 , Face Recognition Security System , Research gate

[19] Masoud Afrakhteh and Subariah Ibrahim, "Adaptive steganography scheme using more surrounding pixels," 2010 International Conference On Computer Design and Applications, 2010, pp. V1-225-V1-229, doi: 10.1109/ICCDA.2010.5541442.

[20] 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.

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