ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

Encrypted Steganography: A Combined Approach for Enhancing Image Security

Ripal Rathod[1], Darshana Mistry[2], Khushbu Patel[3]

M.Tech Student, Department of Electronics and Communications Engineering, Ganpat University, Mehsana, India[1]

Technical Associate, eiTRA, Ahmedabad, India [2]

Engineer, eInfochips, Ahmedabad, India[3]

ABSTRACT*:* In this paper, an end to end algorithm to provide a kind of data security which uses both cryptographic and steganographic approaches to yield better security systems which helps to provide strong security to the confidential image data is proposed and designed. The algorithm uses twofold encryption of confidential image data and LSB embedding for image steganography. Encryption is provided by using Matrix Reordering Technique with Diagonal Approach of Pixel Shuffling and Symmetric Block Cipher named Blowfish. The encrypted data is then hidden into an appropriate cover image using Spiral Approach of LSB Embedding which help resist visual attacks.

KEYWORDS*:* Steganography, Cryptography, Matrix Reordering Technique, Blowfish, Spiral Approach for LSB Embedding

I. INTRODUCTION

Every day, a large amount of data are either accessed or transferred from one place to another via internet. The data sent over internet are facing the constant threat of being stolen or changed for some nefarious purposes. For this very obvious reason, the information security or data security is the highest priority.

The main techniques for information security involve Steganography and Cryptography. Steganography refers to the method of hiding the information in a manner such that it can escape detection. The secret data can be retrieved at the receiver side. Cryptography is a piece of technology of converting the information in a form which is unintelligible to everyone other than the authorized person. By using some pair of algorithm, the secret data is converted in a form which is unreadable. The unreadable data is sent over the internet and the receiver can retrieve the original secret data by applying the algorithm.

Both Steganography and Cryptography can be implemented using different algorithms. There exists some pros and cons for both of these methods hence, according to the application, the algorithm can be selected. Steganography and Cryptography alone are prone to attacks and they can be hacked. One good approach is to combine both Steganography and Cryptography and use them to create an algorithm which provides enough amount of security.

A. *Steganography*

Steganography is an art of hiding the confidential information in a manner that none other than the authorized person can predict the existence of the information. In steganography, confidential information is hidden in somecover data. The cover data is sent through the network and even if it has been accessed illegally, no one can predict the presence of secret data within it.

To embed the secret data within the cover data, a lot of steganographic techniques have been developed. Also, according to various types of data like Text, Images, Audio and Video files, the steganographic schemes vary. As media files i.e. images, audio and video data are quite large in size, they are used as cover data to hide some secret information within them. Using media files, one can hide large amount of secret data but particularly, the audio and video data are so large in size that their processing and transmission can be time consuming and as a result, normally images are used as cover data or medium.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

One such approach for hiding secret data into images is LSB Embedding method. In LSB Embedding method, the least significant bit(s) of cover image are replaced by the confidential data bits. The least significant bit(s) are used for embedding purpose because they do not play a major role in the visual quality of image and hence, the cover image looks as less tempered as possible. Generally, the embedding is done either on the last LSB, last two LSBs or last 3 LSBs.

B. *Cryptography*

Cryptography is a technique of information security using which the confidential data can be converted in a form that is completely unintelligible. This process of conversion is known as Encryption. After performing Encryption on the confidentialdata, the data is sent over the network so even if illegal access of data is performed, the intruder cannot understand or read the data as he/she is unaware of the protocol usedfor Encryption. Classical approach of Cryptography uses Transposition and Substitutional Ciphers which were in practice in history. These approaches use positions transformation of alphabets. Modern approach of Cryptography is currently in use which uses algorithms that have a key to encrypt and decrypt information. These keys convert the confidential data into some unreadable format through encryption and then return them to the original form through decryption.The modern approach can be divided into Symmetric and Asymmetric Key Encryption. Both of these types have their own advantages and disadvantages hence, according to the application, proper algorithm is selected. In Symmetric Key encryption, same private key is used for encryption as well as decryption while Asymmetric Key encryption requires a Key pair, one of which is used for encryption and the other one is used for decryption. Symmetric Key ciphers produce strong cryptosystems and comparatively more efficient. AES, Blowfish, Twofish, RSA are some known Symmetric Key ciphers.

C. *Combined Approach – Steganography and Cryptography*

As providing security to the Image data is focused, it is known that only cryptographic practice or only steganographic practice is not enough for better protection. The reason for not using only cryptography is that, the encrypted image data looks very random and unusual, that is the very goal of cryptography, but existence of this kind of random data itself indicates that encryption has been performed and hence, it takes attention of adversaries and cryptanalysts. At the same time, if only steganographic algorithms are used for image data hiding, then intruders can retrieve the confidential information by performing steganalysis as simple steganography algorithms are very general in use.For the above stated reason, cryptography and steganography alone are not that much efficient in providing better information security. Solution to this problem can be provided by implementing a security approach in which both cryptography and steganography are combined together.

II. ALGORITHM – ENCRYPTED STEGANOGRAPHY

One such combine approach is designed here, which uses Matrix Re-ordering and Blowfish algorithms to perform encryption of data and Spiral approach for LSB embedding to perform data hiding. In Fig.1, block diagram for the algorithm is shown.

Original image in Fig. 1 is confidential message image. Encryption algorithms are applied on it and Encryptedimage is achieved. This Encrypted image is embedded in some vessel image i.e. cover image to get Stego image. After LSB extraction of Stego image and decryption processes, the original confidential message image can be retrieved.

Encrypted Steganography includes the following major algorithms.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

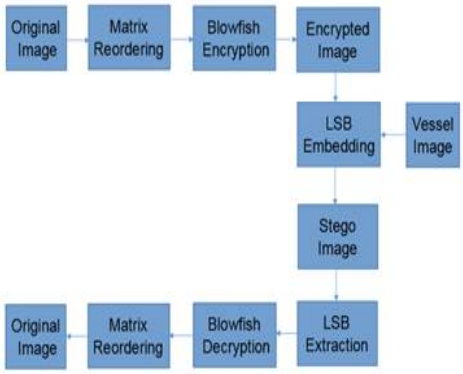


Fig. 1. Block diagram of Encrypted Steganography

1) Matrix Re-ordering Technique:

To provide a basic encryption to image data, Matrix Re-ordering Technique is used. In Matrix reordering, the original image pixels positions are transformed with respect to some specific scan pattern. This results in the output image which has its pixels at very different positions than that of the original image. This kind of pixel shuffling results in a scrambled image. The scrambling can be based on any scan patterns known. To perform pixel shuffling in a manner other than the existing methods, [1] suggests a new approach for pixels shuffling i.e. matrix reordering. The suggested pattern is to use Diagonalapproach for pixel shuffling which is shown in Fig. 2.

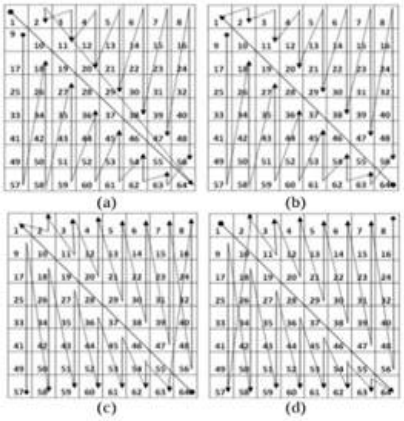
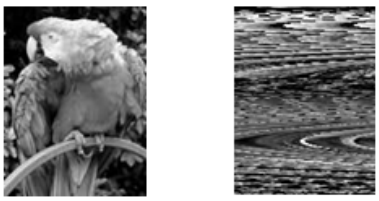


Fig. 2. Diagonal Approach for Pixel shuffling

Reference [1] shows that the diagonal patterns show less correlation with the original image than that of the existing scan patterns show. Such Matrix Re-ordering is applied as a first step in the algorithm. Pixel shuffling is performed on both grayscale as well as color images.

The result of using Matrix Re-ordering Technique with diagonal approach on the image “parrot.png” with dimensions 120x160 is shown in Fig.3.



(a) (b)

Fig. 3. (a) parrot.png image (120x160 – grayscale) (b) Encryption1.png

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

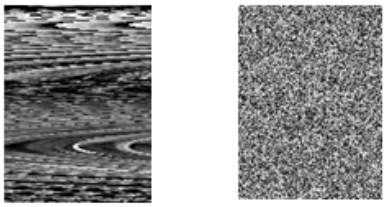
By applying Martix Re-ordering algorithm, a shuffled image can be achieved. This is kind of basic encryption of image data. The shuffled image looks enough random to be predicted for content.

2) Blowfish Algorithm:

Blowfish is a symmetric key 64 bit block cipher designed by Bruce Schneier in 1993. It is private key algorithm having one main key expandable to 56 bytes and sub-keys of total 4168 bytes. The algorithm is unpatented, license-free and available as open source [2]. It works on 16 round feistel cipher. Using 16 round feistel structure with a sufficiently random main key and combination of main key dependent sub-keys can provide enough amount of encryption.

Here, blowfish algorithm is applied on the shuffled image achieved using Matrix Re-ordering technique. Blowfish further encrypts the shuffled image and make it more random and completely unintelligible.

The result of Blowfish encryption on the pixel shuffled image achieved using Matrix Re-ordering is shown in Fig. 4.



(a) (b)

Fig. 4. (a)Encryption1.png (b) Encryption2.png

By applying Blowfish encryption, the image data become visually completely random after application of blowfish algorithm.

3) Spiral Approach for LSB Embedding:

For Steganography purpose, the most widely used approach is to use LSB Embedding Method. Conventionally, the embedding is performed row-wise or column-wise on cover image data but the technique is well known and hence, the steganography can be detected in visual attacks. With time many researchers have tried to modify the LSB Embedding schemes and improved it in different manners to protect the Stego image from visual attack. One such improvement can be achieved via Spiral approach for LSB Embedding [3]. The goal of the Spiral Embedding is to have a simple algorithm to embed content into a cover image using a particular pattern for LSB embedding that will resist a visual attack. Size related information for the message image is stored in the cover image at some known location so that message image can be retrieved properly at the receiving end.

Here, the message data encrypted via Blowfish algorithm is concealed in a sufficiently large cover image using Spiral approach. The size of the message image i.e. the height and width are a part of metadata information. Also, a particular signature or footprint which can be a fixed number or a character pattern is sometimes concealed in the cover medium to indicate the particular algorithm used. Here, the signature used is dependent on the size data. Spiral approach for LSB Embedding works efficiently with 1, 2 and 3 LSBs per pixel of cover image. The location of signature depends on the embedding bits used.

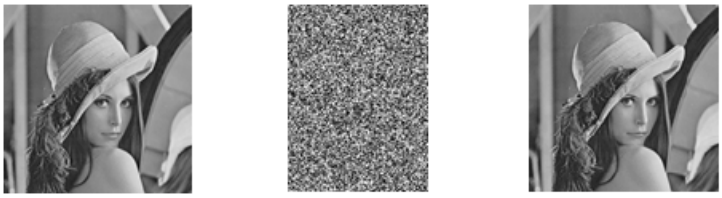
First of all, for this algorithm an appropriate cover image is chosen which can accommodate the secret message image and metadata information for desired embedding bits per pixel of cover image. Once such cover image is selected, the encryption is performed on message image data. As encryption used here is twofold, Matrix Re-ordering algorithm is applied first to get shuffled data and then on this shuffled data, Blowfish algorithm performs second level encryption. This step yields us completely unfathomable message image. Such a message image is hidden in the selected cover using either of 1, 2 or 3 LSBs embedding with algorithm signature. Fig. 5 shows Cover image, Message image and Stego image.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016



(a) (b) (c)

Fig. 5. (a) CoverImage.png (b) Encryption2.png (c) StegoImage.png

After successful embedding, the Stego image is achieved. Stego image looks almost similar to the cover image (Fig. 5). Stego image contains the confidential information and transferred via internet. At the receiver side, the concealed confidential message image can be retrieved using Desteganography and Decryption methods according to the algorithms used for Steganography and Encryption. Size related data is used for getting dimensions of the message image while a unique metadata dependent signature or footprint is embedded along with confidential data for knowing the algorithm used. Signature works as another check point while metadata received seem correct but no embedding have taken place or embedding is performed using different algorithm. Once the metadata and signature are retrieved correctly, the embedded message image can be retrieved byapplying the Desteganography for particular LSBs embedding and Blowfish encryption key. Exact reverse flow of algorithms or ciphers are used at the time of retrieval of confidential data.

Any nefarious attempts to retrieve the confidential data illegally can literally fetch nothing. The reason behind it is that the combination of algorithms used together is not easy to identify. For steganography, metadata information, signature of algorithm and embedding strategy remain hidden to all unauthorized persons. Even if the steganography is hacked successfully, all one can get is random encrypted data. Further, getting the confidential data is difficult as Blowfish encryption is hard to be attacked for enough long and random keys.

III. INTRODUCTION TO QT BASED GUI

Qt is a cross-platform application framework which is used to generate GUIs of applications and can be run on numerous hardware and software platforms with very little change. Qt uses standard C++ with extensions including signals and slots that simplifies handling of events, and this helps in development of both GUI and server applications which receive their own set of event information and should process them accordingly. Qt supports many compilers, including the GCC C++ compiler and the Visual Studio suite [4].

Qt provides a visual debugger, a code editor called Qt Creator and integrated GUI layout and forms designer. GUI applications can be built in Qt and can be run on different desktop environments, mobile or cellphone devices and embedded Linux devices.

One such Qt based GUI of the application representing the end to end algorithm described here is created in Qt Creator. The GUI named as Encrypted Steganography, provides options for both Steganography and Desteganography. Options for performing up to 3 LSBs embedding and Blowfish encryption key are also provided which stay user dependent. The encryption key should be known to both sender and receiver side as Blowfish uses private key encryption. Application of the wrong encryption key at receiver side, generates some random image which is completely unintelligible. Hence, it is very important to have the same encryption key at both sender and receiver side as a shared secret.

IV. RESULTS AND ANALYSIS

The algorithm designed here uses grayscale cover images and works well for both grayscale and color message images. The embedding capacity for concealing color message image in cover medium is low as the data amount almost three times than the grayscale message image and as a result only small color images can be concealed in the cover image. The results in series of Fig.6 show all steps for Encrypted steganography.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

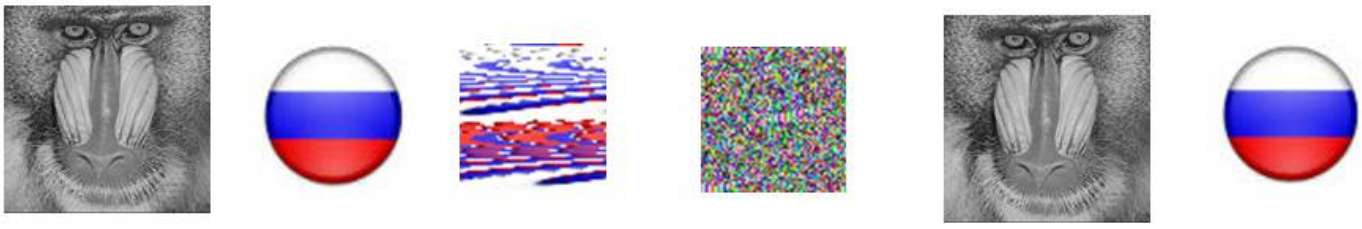
(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

1) Results:

Result images for following Cover and Message images are shown.

Cover image : gray_baboon.png (512x512)
Message image : logo.jpeg (64x64)



(a) (b) (c) (d) (e) (f)

Fig. 6. (a) CoverImage.png (b) MessageImage.jpeg (c) Encryption1.png (d) Encryption2.png (e) StegoImage_1bit.png (f) MessageRetrieved1.png

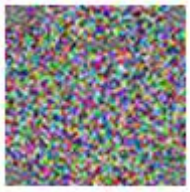


Fig. 7. MessageRetrieved2.png

Fig. 6(a) and 6(b) show Cover image and Message image respectively. Fig. 6(c) is the image yielded after applying Matrix Re-ordering Technique. Fig. 6(d) is the result of application of Blowfish encryption on Fig. 6(c). Fig. 6(e) shows the Stego image generated by embedding the Fig. 6(d) with Spiral approach in Fig. 6(a). And Fig. 6(f) is the Message image retrieved at the receiver side after Desteganography and Decryption stages with correct encryption key. Fig. 7 is the result of application of incorrect encryption key.

2) Calculations:

For 1 bit LSB embedding, few calculations are noted here.

- Cover image dimension =512x512= 262144 pixels
- Message image dimension=64x64 = 4096 pixels
- For 1 bit LSB embedding,
- Number of bits of message image to be concealed =4096x8x3= 98304 message bits (3 for color RGB image)
- Metadata information size= 96 bits
- Total bits = 98400 bits

For 1 bit per pixel of cover image, total of 98400 pixels of cover image are required to contain the particular message image.

In the same manner as shown above, 2 bit and 3 bit embedding can also be performed. For 2 bit and 3 bit embedding, the embedding capacity increases but at the same time we need to compromise on the Stego Image quality. For steganography, the tradeoff always exists between embedding capacity and Stego image quality.

3) Analysis:

The encrypted steganography provides better security and Stego quality when compared with the traditional LSB embedding steganography. This happens because the encryption procedures makes data more random before hiding them. This can be justified by the following result. When a message image is hidden in the cover which has smooth background or has smooth color variations as discussed in earlier chapter, simple steganography makes the Stego image looks tempered.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

The results of Fig 8 and 9 show such an artefact when 3 bit LSB is used.

(a) (b)

Fig 8 (a) Cover Image (b) Message Image

(a) (b)

Fig 9 (a) Conventional LSB embedding (b) Encrypted Steganography

In the Fig. 9(a), in the upper part of Stego image, horizontal lines are visible. In Stego image where these lines appears, embedding has been done. Stego image with Encrypted Steganography doesn't show such lines. The image is good enough even though the same amount of embedding is done and can be seen in Fig 9(b). Fig 10 shows the zoom in part of Fig 9(a) where horizontal lines are clearly visible.

Fig 10 Zoom in part of the Fig 9(a)

Traditionally, the image quality is measured with the indices like MSE and PSNR. Table 1 shows the Stego image quality using these indices comparing with cover image. From this table, it can be analyzed that the Stego image qualitydeteriorates when number of embedding per pixel increases. Increase in mean squared error (MSE) and the respected decrease in peak noise-to-signal ratio (PSNR) depict the fact. Table 1 shows the results statistics. It can be observed that the Encrypted Steganography algorithm generates better quality of Stego images for all 1, 2 and 3 bit of LSB embedding as generally, PSNR value higher than 35 dB are considered visually good.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

TABLE 1
STEGO IMAGE QUALITY ANALYSIS

Sr. No	Stego Image Quality Analysis					
	Cover Image[1]	Message Image[2]	Emb. bits	% Emb.	MSE Value	PSNR (dB)
1	gray_lena (512x512)	g_parrot (160x120)	1	58.63	0.293	53.47
2	gray_lena (512x512)	g_parrot (160x120)	2	29.32	0.731	49.48
3	gray_lena (512x512)	g_parrot (160x120)	3	19.55	2.045	45.02
4	gray_board (480x640)	g_templ (130x100)	1	33.89	0.112	57.64
5	gray_board (480x640)	g_templ (130x100)	2	16.95	0.278	53.69
6	gray_board (480x640)	g_templ (130x100)	3	11.30	0.766	49.29
7	gray_baboon (512x512)	c_logo (64x64)	1	37.53	0.189	55.37
8	gray_baboon (512x512)	c_logo (64x64)	2	18.77	0.467	51.43
9	gray_baboon (512x512)	c_logo (64x64)	3	12.52	1.329	46.89
10	gray_stars (600x752)	c_windows (128x128)	1	87.17	0.335	52.88
11	gray_stars (600x752)	c_windows (128x128)	2	43.59	0.774	49.25
12	gray_stars (600x752)	c_windows (128x128)	3	29.05	2.254	44.60

1. Cover Images are in png format 2. “g_” stands for grayscale images, “c_” stands for colored images, and Message Images can be in png or jpeg format

V. CONCLUSION

From this paper, it can be concluded that Cryptography and Steganography play major role in data security. As both Steganography and Cryptography alone are prone to attacks, the combination of both them are used to generate algorithms that provide strong security. One such end to end algorithm named Encrypted Steganography for Image Security purpose designed here with combination of few algorithms. Matrix Re-ordering Technique along with Blowfish Algorithm makes a strong encryption. Spiral approach of LSB embedding hides the confidential data in a manner that can make the Stego images look almost similar to the Cover images and achieve a good amount of PSNR value. Comparing the Stego images generated using Encrypted Steganography algorithm to the Stego images generated using Conventional LSB method, it can be observed that the Stego images generated using Encrypted Steganography algorithm are better in visual quality. In addition to that, it can be observed that as the embedding bits per pixel increases, the PSNR value decreases.Also, a Qt based GUI for the same is prepared in order to make this algorithm more user friendly.

VI. FUTURE WORK

The algorithm can be modified further to embed data in color cover images. Researches are going on to make steganography more robust by improving LSB embedding method or by using techniques other than LSB embedding. As there exists a tradeoff between Stego Image quality and embedding capacity, to compensate the fact, compression

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

algorithms can be used to compress the confidential data before embedding. As a matter of fact, the compression algorithms must be lossless in this particular case as the concealed information is confidential.

REFERENCES

[1] Sivakumar, T., and R. Venkatesan. 'A Novel Image Encryption Approach using Matrix Reordering' WSEAS, Transactions on Computers, Print ISSN (2013): 1109-2750.
[2] 'Blowfish', http://www.schneier.com/cryptography/
[3] 'Least Significant Bit Embedding: Implementation and Detection'http://www.aaronmiller.in/thesis/
[4] 'Purposesandabilities', http://en.wikipedia.org/wiki/Qt_(software)
[5] Desai, M. S., Mudholkar, C. A., Khade, R., & Chilwant, P. 'Image Encryption And Decryptionusing Blowfish Algorithm'.
[6] Singh, P., & Singh, K. (2013). 'Image Encryption and Decryption Using Blowfish Algorithm in Matlab. *International Journal of Scientific & Engineering Research*, *4*(7), 150-154.
[7] Anjaneyulu, Kurmi, P. K., Jain, R. 'Image Encryption and Decryption using Blowfish Algorithm with Random number Generator' Anjaneyulu GSGN* et al. International Journal Of Pharmacy & Technology (2014).
[8] Patel, K., Utareja, S., & Gupta, H. (2013). 'Information Hiding using Least Significant Bit Steganography and Blowfish Algorithm'. *International Journal of Computer Applications*, *63*(13).
[9] Patel, K., Utareja, S., and Gupta, H. 'Triple Security of Information Using Stegnography and Cryptography' International Journal of Computer Applications (2013).*International Journal of Emerging Technology and Advanced Engineering, vol.3, issue 10, oct 2013.*

BIOGRAPHY

Ms. Ripal Rathod, received B.Tech degree in Electronics and Communication from DDU, Gujarat, India in 2013. Currently, she is pursuing M.Tech in VLSI and Embedded Systems from Ganpat University, Gujarat, India and doing internship from eInfochips Pvt. Ltd., Ahmedabad, India.

Mrs. Darshana Mistry, received B.E. degree from Sardar Patel University, Gujarat, India in 2002 and M.Tech degree from Nirma University, Gujarat, India in 2009. Currently, She is Technical associate in eiTRA, Ahmedabad, India and pursuing Ph.D from Gujarat Technological University in "Multi view Occluded Image Registration" under Dr. Asim Banerjee (DAIICT).

Ms. Khushbu Patel, received B.E. degree in Electronics and Communication from L.D.R.P – I.T.R, GTU, Gujarat, India in 2011 and M.Tech degree in VLSI and Embedded Systems from Ganpat University, Gujarat, India in 2014. Currently, she is working as an Engineer in eInfochips Pvt. Ltd., Ahmedabad, India.