A Secure Image Transmission using Image Mosaics, 2D DWT and RSA Encryption

Mr. Nagendra M S[#1], Mrs. Manjula Yerva[#2], Dr. M. Z. Kurian[#3]
Dept. of E & C, SSIT, Sri Siddhartha Academy of Higher Education, Tumakuru, Karnataka, India.

Abstract: **Security of an image when it is in transit is a serious matter of concern. The advent of computing systems, new inventions in image processing fields, Artificial Intelligence have contributed considerably for the insecurity of an image. Conceptually, a strong encryption powered by sophisticated Cryptographic algorithm can protect any type of multimedia data. But encryption changes the format of data and it is not a good idea to use it with an image. Reason being that, an encrypted noise like image attracts hacker's attention and secondly, lossless recovery of original image is not possible from an encrypted image. An alternative for securing the image is covert communication using Steganography methods. Here, message is concealed; but if existence of data is discovered in any way, the security is compromised. Therefore, there is a need for a system which exploits the advantages of both Cryptography and Steganography. The proposed system combines those two and provides "Stenographic Encryption" security for an image being sent in the channel. An image which needs to be sent secretly and securely is called the Secret Image. Another image which is similar to secret image in background and colour characteristics - is selected and it is called Target Image. The secret image is sliced into small chunks and a mosaic of target image is created (Mosaic Encryption). The mosaic encrypted image will undergo 2 levels 2 dimensional DWT (Discrete Wavelet Transform) which separates information part and details part. Also, 2D DWT compresses the image. RSA encryption is applied to information part. The detailed part and RSA encrypted information part are merged together to form the combined image. A large cover image is chosen and the combined image's bits are embedded into pixels of cover image using advanced LSB method which gives the stego image. This stego image is sent to receiver over channel. At the receiver, combined image is extracted from the stego image. RSA decryption is applied to information part and IDWT is applied to get the mosaic image. The secret image is reconstructed using the mosaic image. The proposed method will give two levels of encryption protection (Mosaic encryption and RSA encryption), compression facility (DWT) and Stenographic facility (LSB hiding). Nearly lossless recovery of Secret image is possible. The experimental results were pleasing with high PSNR and Correlation and less RMSE. The system is implemented using MATLAB tool.**

Keywords: Cryptography, Steganography, Mosaic Encryption, 2D DWT, RSA Encryption, LSB embedding

I. INTRODUCTION

Security of the data is always a matter of concern over time. The amount of data is being exchanged for various reasons is growing along with the growth of human civilization. Even during the ancient time, there were threats to the security of data when it was in transit. Of course, the data was transmitted in "offline" mode in that time. Even then, there was matter of concerns related to data stealing. Various methods were developed to tackle the situation. Crypto writing, Wax board method are few of the methods employed. Most of the data in old days were mainly of textual form and hence, security measures developed were concentrated mainly on securing textual information. In those days, "Mosaic" was used for the sake of "decoration" and which was merely an art in those days. Also, various Crypto-Writing were followed. Steganography was carried out by wax sheet writing and other methods.

With the advent of computer system, all the methods of Cryptography and Steganography stated above have been automated and powerful software tools are now available to carry out those methods. Mosaic which was an art in those days, is now been developed as a Mosaic encryption technology [1]. All the Crypto-Writings are now being done by software. (RSA is one of such encryption method). Steganography (information hiding) is being achieved using LSB method. Also, a new technology called Discrete Wavelet Transform is also developed which splits up an image into various parts based on the frequency bands and also provides compression facility.

Section II is about literature survey of Mosaic technology, LSB data hiding methods, DWT and RSA technology. Section III explains those techniques in detail with flow charts and algorithms. Section IV explains the proposed method for image security using these methods. Section V focuses on results an analysis. Section VI is about conclusion and section VII details References.

II. LITERATURE SURVEY

A mosaic is a 'big' and an art like image which is built from small slices of another image or by using hundreds of small sized images. If the slices of image used for creation of mosaic are generated using a single image, it is called "Crystallization Mosaic Technique" or "Single Picture Mosaic" [1]. If the slices used for creation of mosaic are from different images, it is called "Multi Picture" mosaic or "Photo Mosaic" [4]. The mosaic technique can also be used for reconstruction of ancient and worn out materials like palm tree writings, embossed sculpture etc. This

method is called as "Ancient Mosaic Technique" [5]. A randomly shaped container image is "best filled" with randomly sized small images like a JigSaw puzzle and hence, this method is called "Puzzle Mosaic" [6].

The pixel intensity value can be represented in 8 bit format. A small change in the LSB bits can hardly affect the pixel intensity value. Hence, these bits are used for data embedding. In *sequential LSB methods* [7] the pixels of the container image are sequentially selected and payload bits are embedded in to the binary representations of these pixels. In *Random LSB methods* [8], payload bits are clinched into LSB positions of container image pixel in a random way. In LSB 'replacement' method [9] , LSB positions of pixels (which are in binary representation form) are straight away replaced by payload bits. This method is simple but it degrades the quality of container image. In LSB 'matching' method [10], instead of simply replacing the LSB bits by payload bits, a "matching" between them is done either by adding or subtracting binary one. This method is better compared to LSB replacement method and also preserves histogram of Container image. An improvement to LSB matching is proposed in [2] in which, only one LSB bit of container image is modified for every two bits of information.

Wavelet refers to a small portion of wave which crosses zero reference. [11] Explains the fundamentals of *wavelet transform* and Discrete Wavelet transforms (DWT). [12] Suggest the comparison of compression ratio achieved by DCT (Discrete Cosine Transform) and DWT and found that, DWT's compression ratio is 50% more than DCT. [13] Proposed a de-noising method using DWT transform by edge detection and applying de-noising algorithms. [14] and [15] explains how DWT can be used to process and improve the quality of satellite images. They mainly concentrate on improving the contrast and resolution of satellite images by employing DWT with SVD (Single Value Decomposition).

RSA is an asymmetric key Cryptographic method using which, text messages and images are encrypted. [16] and [19] explains the implementation methods of RSA algorithm on images. [17] Explains the details of RSA algorithm implemented on an image with a numerical example for key generation, encryption and decryption. [18] Suggest grid based RSA in which, an image is sliced in to various blocks; these blocks are mixed in a random way and RSA is applied to each block individually. [20] Explains the calculation time needed for encryption process for various values of 'p' and 'q'. [21] Compares RSA and AES algorithms and found that, RSA gives better results. [22] Suggest improvements to RSA algorithm in which, pixel values are converted into strings before applying encryption. [23] Details a system which employed RSA for encryption and LSB for data hiding.

III. Conceptual Knowledge Used

A. Mosaic Technology

The image that is to be sent covertly is called secret image. Another image called as "Target Image' is selected. The Target image is selected such that, it belongs to same field, approximately similar background and colour distribution. Also, the size of both the images (Secret Image and Target Image) should match. If there is a mismatch in size, the Target Image is resized to match the dimension of Secret Image. The goal is to create a mosaic image (using the chunks of secret image) which reassembles the target image. The mosaic image so built is sometime called as "Mosaic Encrypted Image" [1]. Fig. 01 shows that a cat's image is created using the pieces of dog's image

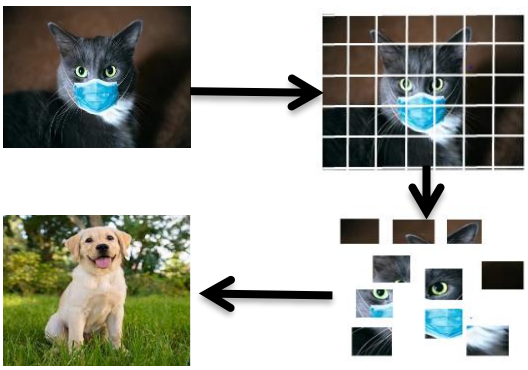


Fig.1: Example of Mosaic Image creation

The secret image "S" and target image "T" are sliced into equal sized small pieces (8 x8, 16 x 16 etc.) and are arranged in rising order of mean and standard deviation. The mean and standard deviation are calculated as shown in equation 01and 02.

$$\text{Mean for each slice of S} = m_h = \frac{1}{k}\sum_{i=1}^{k} h_i \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (01)$$

$$\text{Standard deviation for each slice of S} = d_h = \sqrt{\frac{1}{k}\sum_{i=1}^{k}(h_i - m_h)^2} \ldots\ldots\ldots\ldots\ldots\ldots (02)$$

The slices of secret image and target image are one – to – one mapped and mosaic image is created. Colour transformation scheme is applied on mosaic image to improve the image quality aspects and to get better visual experience. Colour transformation equations are shown on equation 03 and 04.

Mean for each slice of T= $m_h' = \frac{1}{k}\sum_{i=1}^{k} h_i'$ …….....……..…... (03)

Standard deviation for each slice of T= $d_h' = \sqrt{\frac{1}{k}\sum_{i=1}^{k}(h_i' - m_h')^2}$ ……... (04)

After the colour transformation phase, residual values are noted (if generated) and the blocks of Mosaics are rotated in various directions to reduce RMSE. The final recovery information is noted and password protected if needed. At the receiver end, secret image is reconstructed using the mosaic image.

B. 2 Level, 2 dimensional Discrete Wavelet Transform (2D DWT)

DWT is a mathematical tool which generates wavelet coefficients [11], [13]. When DWT is applied to an image, it extracts principal facts in a time-frequency domain. The principal advantages of DWT are feature extraction and data compression. When DWT is applied to an image, it divides the image into low frequency coefficients (They contain the main information) and high frequency coefficients (they contain edge information). When a two level DWT is applied in two dimension (first in horizontal direction and the in vertical direction), it splits up the image in into four sub bands as shown in Fig. 02

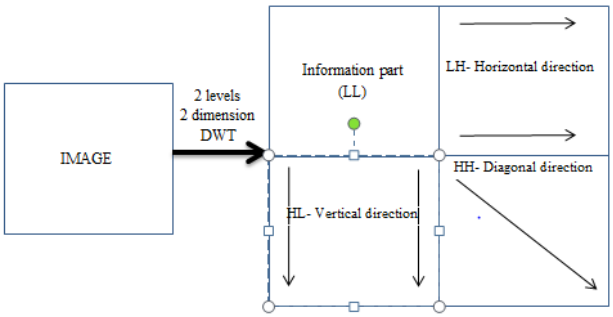


Fig. 2: Generation of various sub bands when DWT is applied to an image

The LL sub band contains the vital information and hence, it is usually encrypted using a key. The other three sub bands contain the edge details in various directions (Horizontal, Vertical and Diagonal) and they contain lot of redundant information. By the property of DWT, these redundant data is compressed. Hence, just by applying DWT to an image, sensitive part can be isolated and redundant part is compressed. The inverse DWT (IDWT) will combine all these sub bands and will construct the original image. Fig. 03 shows the result of applying DWT to an image.

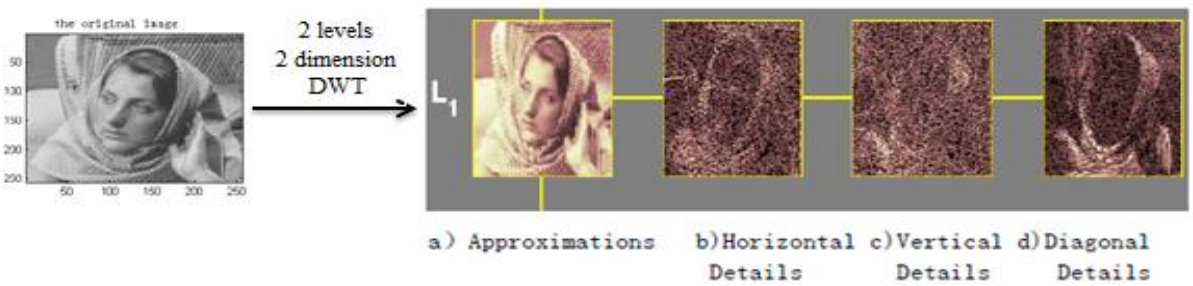


Fig. 3: When DWT is applied to an image

C. Advanced LSB method

LSB hiding is a Stenographic method which aims at covert communication. A container image (sometimes called Cover Image) of larger size is selected and the information bits are clinched into LSBs of each pixel of container image. Generally, LSB hiding methods modify one bit of pixel for every one bit of information. The advanced LSB method [2] will modify only one bit of pixel for every two bits of payload. This method increases the "capacity" (the amount of data that a container image can hold) considerably.

Following scheme is used for LSB data hiding. Let C denote last two bits of pixel and P denote two payload bits.

Case A: (When C < P):

1. Number to be added is denoted by "X"; X=P-C-1
2. Last 2 bits of Stego pixel is denoted by "S"; S = C+X

3. Repeat this procedure till all payload bits are embedded

Case B: (When C > P):

1. Difference is denoted by "D"; D = C-P
2. Number to be added is denoted by "X"; X=3-D
3. Last 2 bits of Stego pixel is denoted by "S"; S = C+X

For the recovery of payload bits from the stego image at the receiver end, just *a binary one* is needed to be added to last two bits of stego pixel. Table 01 shows the example for embedding and recovery of payload bits when last two bits of pixel are "01" and payload bits are 00, 01, 10 and 11. The table can be expanded in the similar way for other combinations of payload bits and LSB of pixel.

TABLE I
LSB HIDING AND RECOVERY EXAMPLE WHEN LAST TWO BITS OF PIXEL ARE "01"

Last 2 bits of Cover Pixel **"C"**	Payload bits **"P"**	Case	Number to be added to Cover pixel **"X"**	Stego pixel after embedding msg bits **"S"**	Retrieved msg bits by adding binary one (at Receiver)		Last two bits of cover pixels…		Comment
							Before embedding	After Embedding	
01	00	B	2	01+10= 11	11+1=00		01	11	One bit change
01	01	B	3	01+11= 00	00+1=01		01	00	One bit change
01	10	A	0	01+00= 01	01+1=10		01	01	No change
01	11	A	1	01+1= 10	10+1=11		01	10	Compensated

D. RSA encryption Algorithm

RSA is a powerful encryption algorithm that was initially used to encrypt textual messages [16], [19]. RSA is an asymmetric encryption method which uses two separate keys for encryption and decryption. *Public key* is used for encryption and *private key* is used for decryption. The private key and public key are mathematically linked but it is impossible to derive the private key of a user using his public key. The public key is openly shared to sender and private key is kept confidential. Fig. 4 shows the example of RSA encryption and decryption applied to an image using MATLAB tool. The RSA encryption scheme for images mainly has two phases as follows;

1. Key generation
2. Encryption of the image

Key Generation

During this phase, public key (e, n) and private key (d, n) of a user are calculated using two "large" prime numbers 'p' and 'q'

1. Two large prime numbers p and q are assumed
2. A value 'n' is calculated as n = p x q
3. A value "phy" is calculated as phy = (p-1) x (q-1)
4. A value 'e' is calculated such that, 'e' and 'phy' are co-prime to each other. GCD (e, phy) = 1
5. A value 'd' is calculated such that [d x e] % [phy] = 1
6. The public key of a user is (e, n)
7. The private key of the same user is (d, n)

Encryption of Image

During this phase, the image to be encrypted is divided in to equal sized small blocks (8x8 or 16x16) and RSA scheme is applied on each block. The image is rebuilt using the encrypted blocks to get the encrypted image which is called "Cipher image". The detailed steps are as follows

1. Read the original image "S" (2D) which needs to be encrypted.
2. Divide the image S in to k number of W sized blocks.(W = 8x8 or 16x16)
3. Represent each W sized block as one dimensional array. Let it be called as "m'.
4. RSA scheme is applied on each array "m" separately. The "m" array will get encrypted and will become "c". The encryption is done such that $c = m^e \bmod n$
5. W sized blocks are rebuilt using encrypted arrays "c". Using these encrypted blocks, main image S is rebuilt which is now called as cipher image and look like a noise image.
6. At receiver end, decryption is done and "m" is recovered using the formula. $m = c^d \bmod n$

Fig. 4: Example of RSA encryption and decryption; p=13, q=31, n=403, phy=360, e=7, d=103

IV. Proposed System

Fig. 5 (Sender side) and Fig. 6 (Receiver side) explains the proposed system in detail. The main goal is to send the secret image "S" from sender to receiver covertly with additional encryption protection. At the receiver end, the secret image "S" needed to be recovered successfully. This method is inspired by [3]. The Choes based encryption is replaced by RSA algorithm.

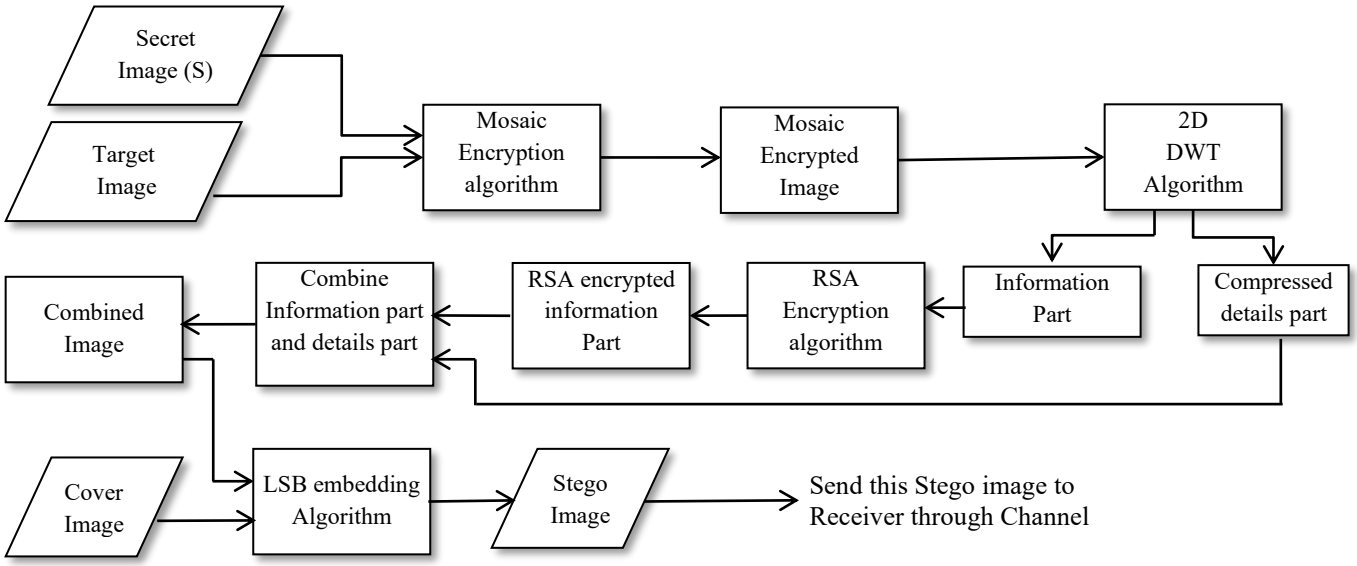


Fig. 5: Proposed system's block diagram: Sender side

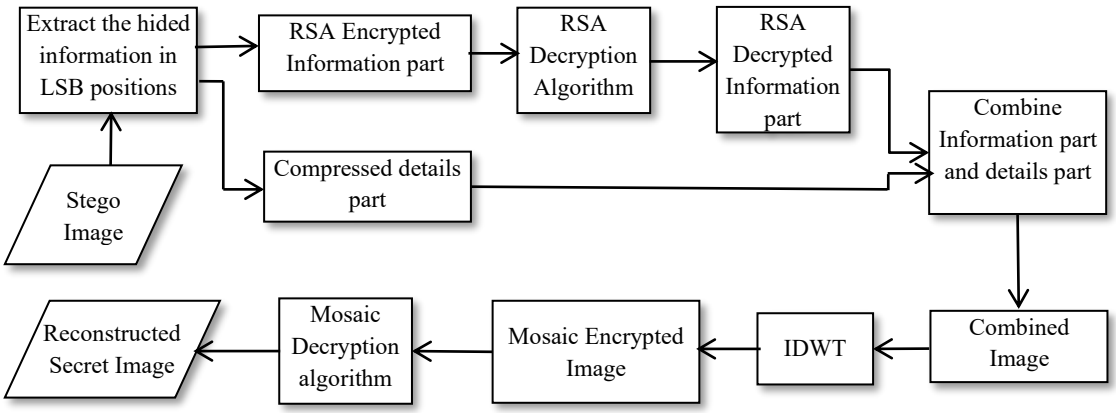


Fig. 6: Proposed system's block diagram: Receiver side

To begin with, 24 bit colour image is given as input to the system. The mosaic of that image is created using a suitable target image (The target image should have similar background and colour characteristics as that of secret image). 2D DWT is applied on Mosaic encrypted image and "information part" (LL Sub band) and "details part" (LH, HL and HH sub bands) are separated. The details part is compressed by the basic property of DWT. RSA

encryption is applied on information part. The encrypted information part and other three compressed sub bands (LH, HL and HH) are clubbed to get the "Combined image". A container image (which should be 8 times bigger than combined image) is selected and combined image is hided into LSB positions of container image pixels usig Advanced LSM algorithm [2]. The output at the sender is stego image. This is sent to receiver through channel.

The stego image acts as the input to the receiver. Combined image is extracted from the LSB positions of pixels of stego image. RSA decryption is applied on encrypted information part. IDWT is applied to get the Mosaic encrypted image. Secret image "S" is rebuilt using the mosaic image. In this way, a secret image is sent covertly and securely from sender to receiver and at the receiver end, secret image is successfully recovered.

V. Experimental Results

The proposed system is realized using MATLAB tool running on Windows 07 (or above) operating systems. Fig. 7 shows Mosaic creation process at sender side. Fig. 8 shows 2D DWT operation, RSA operation and LSB hiding process at Sender side. Fig. 9 shows operations happening at receiver side where combined image is extracted from Stego image, IDWT is applied and secret image is rebuilt using Mosaic image. Fig. 10 shows the input secret image at sender side and recovered secret image at receiver side. Table 02 details experimental results. The initial cover image is taken as a group photo, faces are extracted and extracted faces are used as cover image. The user is free to choose his own cover image instead of faces.

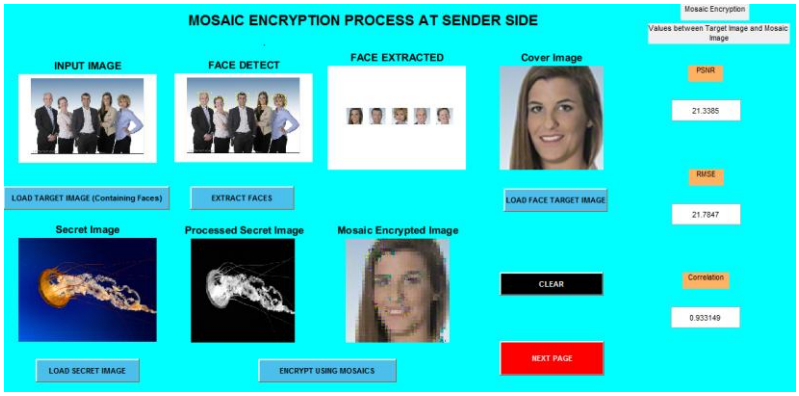


Fig. 7: Mosaic creation at sender side

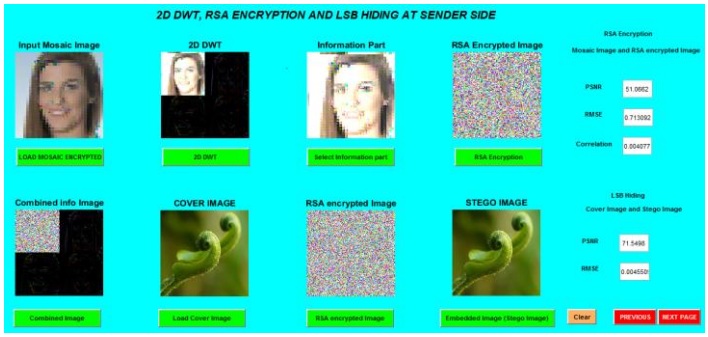


Fig. 8: DWT operation, RSA encryption and LSB hiding at sender side

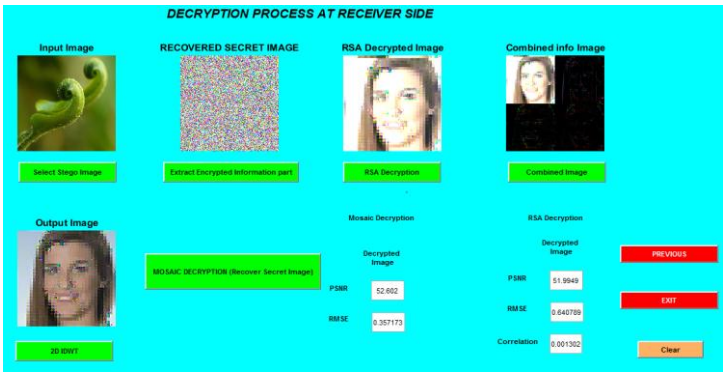
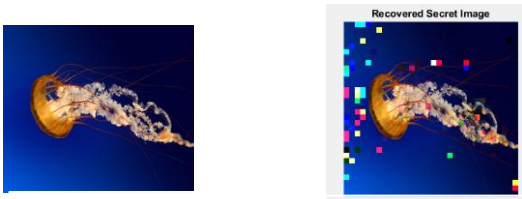


Fig. 9: Combined image extraction, RSA decryption and mosaic decryption at receiver side



Secret Image Recovered Secret Image

Fig. 10: Input secret image and recovered secret image from the proposed system

A. Result Analysis

Table 02 details experimental results for one set of images. The face is extracted from the main target image and used as target image. Mosaic is created, 2D DWT is applied and RSA encryption is applied to information part. Combined image is embedded in to cover image using advanced LSB method. The stego image is sent to receiver and secret image is recovered at receiver side by mosaic decryption, IDWT and RSA decryption.

TABLE II
EXPERIMENTAL RESULTS

Sender side			
Input Images			Output Image
Target image	Secret image	Cover Image	Stego image
The values as calculated between	PSNR	RMSE	CORRELATION
Target Image and Mosaic Image	21.3385	21.7847	0.933149
Mosaic Image and RSA encrypted image	51.0662	0.713092	0.004077
Cover Image and Stego Image	71.5498	0.00455093	----------
Receiver side			
Input Image		Output Image	
Stego image		Reconstructed secret image	
The values as calculated between	PSNR	RMSE	CORELATION
Mosaic Image at sender and reconstructed Mosaic Image at receiver	52.602	0.357173	---------
Testing of RSA: Before RSA encryption and After RSA decryption. Information part at sender and recovered information part at receiver.	51.9949	0.640789	0.00130206

On analysis of data in Table II, following conclusions can be drawn.

1. There is very less PSNR between target image and mosaic image at sender; also, very high RMSE value. This indicates that, lot of "noise" is added during mosaic encryption. Any hacker cannot predict the secret image from mosaic image. As the correlation is high, the recovered secret image from mosaic image is of good quality.
2. PSNR between Mosaic image and RSA encrypted image at sender is high and RMSE is low. This means that, RSA encryption do not add much noise. Also, the correlation is almost negligible. This shows the strength of RSA encryption and the image is highly encrypted
3. PSNR between Cover image and Stego image at sender is very high. This infers that, LSB embedding did not disturb the cover image much. Also, RMSE is negligible i.e., there is no "error" between cover image and stego image. This was very much needed in any covert communication.
4. The mosaic image created at sender and the mosaic image reconstructed at receiver (Image given to DWT at sender and image regenerated after IDWT at receiver) are compared. The PSNR is high and RMSE is low; which means that, less noise is added by DWT – RSA encryption – RSA decryption and IDWT process. And hence, there is less error (RMSE) between those mosaic images. This feature is essential for successful recovery of secret image.
5. The "information part" image generated at sender (when DWT is applied to mosaic image at sender) and the information part image regenerated at receiver (when IDWT is applied to combined image at receiver) are

compared. In other words RSA encryption and decryption process is tested. PSNR is high and RMSE is low; this indicates that, RSA algorithm didn't add much noise and hence, it's an efficient encryption algorithm.

VI. Conclusion

When an image needs to be sent securely over a channel, the system discussed so far efficiently provides two levels of encryption protection and it also supports covert communication. Mosaic sheme is powerful technology which provides both encryption protections (as the recovery information is password protected) and also helps for secret communication. The two level two dimensional DWT (2D DWT) provides data compression privilege and also, it reduces the time needed for next level of encryption process. The DWT separates out the information part (LL sub band) and hence, RSA encryption was needed to be applied to only ¼th part of the image. This saves lot of memory, computational effort and rime. RSA is a well-known encryption algorithm used for digital images. The length of RSA keys and the amount of security provided by RSA algorithm are directly proportional. The results were satisfactory and the secret image was successfully recovered at the receiver.

VII. References

[1] Lee and W. Tsai, "A New Secure Image Transmission Technique via Secret-Fragment-Visible Mosaic Images by Nearly Reversible Color Transformations," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 24, no. 4, pp. 695-703, April 2014, doi: 10.1109/TCSVT.2013.2283431.

[2] Shyla.M.K, K.B.Shivakumar, Rajendra Kumar Das, "Image Steganography using Improved Lsb-Mapping Technique with Enhanced Recovery Speed", International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-4, November 2019, DOI:10.35940/ijrte.B3701.118419, https://www.ijrte.org/wp-content/uploads/papers/v8i4/B3701078219.pdf

[3] Y Manjula 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, DOI: http://dx.doi.org/10.21786/bbrc/13.13/9, https://bbrc.in/secured-image-transmission-using-color-transformation-fragmented-mosaic-chaos-based-encryption-and-lsb-mapping-steganography-technique/

[4] A. H. Pascaline, L. C. F. Christopher, M. H. Khan and S. Pudaruth, "Using photomosaic and steganographic techniques for hiding information inside image mosaics," 2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Kochi, 2015, pp. 1893-1897,doi: 10.1109/ICACCI.2015.7275894.

[5] GENERATION OF GEOMETRIC ORNAMENTS IN ANCIENT MOSAIC ART, JOURNAL OF INDUSTRIAL DESIGN AND ENGINEERING GRAPHICS 6

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

[7] Y. P. Astuti, D. R. I. M. Setiadi, E. H. Rachmawanto and C. A. Sari, "Simple and secure image steganography using LSB and triple XOR operation on MSB," 2018 International Conference on Information and Communications Technology (ICOIACT), 2018, pp. 191-195, doi: 10.1109/ICOIACT.2018.8350661.

[8] X. Zhou, W. Gong, W. Fu and L. Jin, "An improved method for LSB based color image steganography combined with cryptography," 2016 IEEE/ACIS 15th International Conference on Computer and Information Science (ICIS), 2016, pp. 1-4, doi: 10.1109/ICIS.2016.7550955.

[9] A. Arora, M. P. Singh, P. Thakral and N. Jarwal, "Image steganography using enhanced LSB substitution technique," 2016 Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC), 2016, pp. 386-389, doi: 10.1109/PDGC.2016.7913225.

[10] M. Khosravi, S. Soleymanpour-moghaddam and M. Mahyabadi, "Improved pair-wise LSB matching steganography with a new evaluating system," 6th International Symposium on Telecommunications (IST), 2012, pp. 982-986, doi: 10.1109/ISTEL.2012.6483129.

[11] Discrete Wavelet Transform, Image Processing: Principles and Applications. Tinku Acharya, Ajoy K. Ray, Copyright 0 2005 John Wiley & Sons, Inc.

[12] A. H. M. J. I. Barbhuiya, T. A. Laskar and K. Hemachandran, "An Approach for Color Image Compression of JPEG and PNG Images Using DCT and DWT," 2014 International Conference on Computational Intelligence and Communication Networks, 2014, pp. 129-133, doi: 10.1109/CICN.2014.40.

[13] Z. Xizhi, "The Application of Wavelet Transform in Digital Image Processing," 2008 International Conference on MultiMedia and Information Technology, 2008, pp. 326-329, doi: 10.1109/MMIT.2008.134.

[14] A. Sharma and A. Khunteta, "Satellite image contrast and resolution enhancement using discrete wavelet transform and singular value decomposition," 2016 International Conference on Emerging Trends in Electrical Electronics & Sustainable Energy Systems (ICETEESES), 2016, pp. 374-378, doi: 10.1109/ICETEESES.2016.7581412.

[15] R. Thriveni and Ramashri, "Edge preserving Satellite image enhancement using DWT-PCA based fusion and morphological gradient," 2015 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), 2015, pp. 1-5, doi: 10.1109/ICECCT.2015.7226022.

[16] Mukherjee, S. Sinha, S. Chakrabarti and T. Mukhopadhyay, "A meticulous implementation of RSA Algorithm using MATLAB for image encryption," 2017 1st International Conference on Electronics, Materials Engineering and Nano-Technology (IEMENTech), 2017, pp. 1-6, doi: 10.1109/IEMENTECH.2017.8076979.

[17] Karrar Dheiaa Mohammed AlSabti and Hayder Raheem Hashim, "A New Approach for Image Encryption in the Modified RSA Cryptosystem Using MATLAB", Global Journal of Pure and Applied Mathematics .ISSN 0973-1768 Volume 12, Number 4 (2016), pp. 3631-3640, © Research India Publications http://www.ripublication.com/gjpam.htm

[18] Binay Kumar Singh and Sudhir Kumar Gupta, "Grid-based Image Encryption using RSA", International Journal of Computer Applications (0975 – 8887)Volume 115 – No. 1, pxc3902166, April 2015, https://research.ijcaonline.org/volume115/number1/

[19] Shankar K, "An Optimal RSA Encryption Algorithm for Secret Images", International Journal of Pure and Applied Mathematics, Volume 118 No. 20 2018, 2491-2500, ISSN: 1314-3395 (on-line version), url: http://www.ijpam.eu

[20] Ali E. Taki El_Deen, El-Sayed A. El-Badawy, Sameh N. Gobran, "Digital Image Encryption Based on RSA Algorithm", IOSR Journal of Electronics and Communication Engineering (IOSR-JECE), e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 9, Issue 1, Ver. IV (Jan. 2014), PP 69-73, www.iosrjournals.org

[21] D. M. Alsaffar et al., "Image Encryption Based on AES and RSA Algorithms," 2020 3rd International Conference on Computer Applications & Information Security (ICCAIS), 2020, pp. 1-5, doi: 10.1109/ICCAIS48893.2020.9096809.

[22] F. H. M. S. Al-Kadei, H. A. Mardan and N. A. Minas, "Speed Up Image Encryption by Using RSA Algorithm," 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS), 2020, pp. 1302-1307, doi: 10.1109/ICACCS48705.2020.9074430.

[23] S. Mittal, S. Arora and R. Jain, "PData security using RSA encryption combined with image steganography," 2016 1st India International Conference on Information Processing (IICIP), 2016, pp. 1-5, doi: 10.1109/IICIP.2016.7975347.