DOI: 10.21917/ijivp.2019.0275

HIDE IMAGE AND TEXT USING LSB, DWT AND RSA BASED ON IMAGE STEGANOGRAPHY

Swati Bhargava and Manish Mukhija

Department of Computer Science and Engineering, Modern Institute of Technology and Research Centre, India

Abstract

In this modern era, where technology is increasing at rapid pace and made all day new developments, security is of highest priority. To protect facts into the unrecognizable form diverse technique are used for records hiding like steganography and cryptography techniques have been advanced. This paper securing the image by way of encryption is completed by LSB bits, DWT and RSA algorithm. This paper additionally presents new strategies wherein cryptography and steganography are mixed to scramble the information and in addition to cover the insights in some other medium through image processing (IP). The encrypted picture can be hiding in some other image by way of the use of LSB bits, DWT strategies so that the secret's message exists. RSA algorithm applied, receiver will use his/her private key because the secret data have been encrypted by recipient public key. Hide encrypted image in the cover image by DWT. Extract encrypted image from cover image and decrypt text by DWT. The proposed scheme is implemented in MATLAB platform the use of preferred cryptography and steganography set of regulations. Calculate PSNR and MSE. Also calculate the entropy of cover image and stego image. This method is secure for communication in the digital world with the digital data transmission.

Keywords:

Image Steganography, LSB bits, RSA, PSNR

1. INTRODUCTION

Steganography is the art and science of secured composing (cover up on display) and its strategies are being used from several years. Digital Steganography is the procedure of attaching digitized information by concealing it into another bit of information. Today, in digital age the simple access to any type of information, for example, audio, video, pictures and content make it defenseless against numerous threats [1]. The information should be guarded secure thus that it could be gotten to just by the approved work force and any unapproved client can't have any entrance of that information. Data sharing is increasing as thousands of messages and data is being transmitted on internet every day from one place to another. The protection of data is prime concern of the sender. The need is that correct data should be sent but in a secret way that only the receiver should be able to understand the message. At first procedure of cryptography was designed to send secret messages over spots. In cryptography message was encoded in the other message in encrypted such that only the person as a sender and receiver get to know the way to decrypt it [2]. A cryptographic key was important to decode message that was known by people who are under approved. The constraint of cryptography was that other individual came to realize that the message had a hidden text in it thus the likelihood of message being decoded by other individual expanded. The Limitation is overwhelmed by technique for steganography was individual presented. The word that has a place with Greek language. In Greek, steganography is known as the "covered writing". First of the all steganography was person required in the Greece. They use to enter the message on a wooden tablet and after that apply wax on it to conceal the composed information. The strategy for steganography was vastly improved than cryptography as in it information is being covered up in picture. The picture was then disregarded web. It had advantage over cryptography as now the middle person does not come to know whether data is hidden in the image or not. The information must be unscrambled from picture by the approved individual as he most likely is aware the marvel to interpret it and had the approved key with him that was required to decoded data. The reliability as well as the security of data transmission also gets improved with invention of the process known as steganography as now no outsider could change data which is sent. The imperceptible sign is referred to as watermark and the given sign is known as cover work. This cover work may be an image, audio or a video file [3]. A steganography set of rules consists of the watermark shape, an embedding algorithm, and an extraction or detection set of rules. Steganography may be embedded within the pixel area or a remodel area [4]. Digital steganography is a technique designed to secure a via hiding that message inside every other item so that it can be saved secret from all and sundry except the intended recipient. Steganography strategies may be divided into two groups: Visible and invisible, the visible steganography is used if steganography is meant to be visible by human eyes, For example, an emblem inserted into corner of an image. While the invisible steganography is embedded into more than a few image through sophisticated algorithms and is hidden to human eyes [5].

1.1 TEXT FILES STEGANOGRAPHY

The method of hiding secret information in a text is known as text steganography. Content steganography wants less memory as it can just store text files. It gives snappy correspondence or exchange of records starting with one PC then against the next. Text steganography is not commonly used as text files containing a large amount of redundant data. [6]

2. RELATED WORK

Trivedi and Rana [7] presents about Steganography is put into practice of hiding secret message or the secret information within further multimedia data so as to is text, the image, audio or the video. The power of steganographic method lies in its capacity to remain the message as covert as likely and also quantity of information so as to can be concealed, as huge as possible. In spite of fact that many approaches by now exist in the steganography researches are going away on in the field. This paper gives a survey on the methods used in this area.

Isla et al. [8] presents about the rapid development of data communication in modern era demands secure exchange of information. Steganography is reputable process for hiding data on or after an unauthorized access. Steganographic techniques hide secret data in different file formats such as: image, text, audio, and video. In this paper, a new image steganography method based on nearly each one major bit (MSB) of image pixels is proposed. Moreover, the presented method is not simply secure, but computationally proficient as well.

Shakeela et al. [9] proposes a simple and robust method of audio data embedding into videos. Robustness in this method comes because of the use of double coding mechanism. Here double coding means using two kinds of codes on the same data one after another. This provides more security and reliability to the hidden data into video. The process performed in wavelet area by means of pseudo random codes and the more codes. The presentation of technique is evaluated by the MSE known as (Mean Square Error) and PSNR also called (Peak Signal to Noise Ratio). The obtained test result doesn't affect much to the quality of extracted audio data.

Sateesh et al. [10] provide security to the data using cryptography and Steganography techniques together. The combination of these two techniques can provide robust platform for secured data communication System. Here, they make a Cipher text of text message by means of Cryptography approaches and then the method conceal the Cipher text interested in Multimedia by means of Steganography approaches. They have used SDES algorithm in Cryptography intended for data Encryption and the Decryption, LSB way of Steganography to conceal Cipher text into the image.

Ahmed and Khodher [11] compares eight methods by means of steganography of Arabic language texts for dissimilar search algorithms to believe a secret key. All methods use random numbers to generate the secret key. The objectives are to assess each way and to choose the best method that provide the most excellent solution suitable to conceal the Arabic language texts. Secret sharing is fourth-best way in security, linear regression is best way for lucidity and capability of covert message hiding, whereas remarkable value of decomposition is best method in conditions of security and the toughness, Huffman code provides covert message compression safety and clearness, and steganography in Microsoft word documents use the protocol in layer one of single–double quote, which is frail in security.

Makwana and Chudasama [12] presents about the focus is on rising data safety by means of dual steganography. In double steganography covert message is 1st embedded into wrap medium and then outcome stego-object will be another time embedded interested in other cover up medium. Mentioned paper in addition provide a quantifiable estimate of dual steganography in conditions the decrease in the mean square error also known as (MSE) and therefore increase in peak signal to noise ratio also known as (PSNR) measure among original host files and generate stenographic files. A beginning outcome shows the high imperceptibility of proposed way as well as hiding capability of obtainable method.

Thenmozhi and Menakadevi [13] presents about message figure is compacted by means of the SPIHT way of lossless compression and after that it is encoded in to other image. Image contains a combination of RGB layers. If the method, considers a pixel as an 8-bit value then each pixel has the value in the range of 0 to 255. This algorithm compress secret message image through SPIHT and change in to binary sequence, divides binary sequence in to blocks, modify order of block by means of a key-based at random generate permutation, concatenates the permuted blocks could be changed in to permuted binary sequence, and at that time utilizes the Least-Significant-Bit (LSB) come close to embed the permuted binary series interested in image. After completion of pixel value altering all images is located in a sequential mode. In the decoding surface the message image is being decoded and decompressed so as that message image can be obtained.

3. USING TECHNIQUES: LSB, RSA, DWT

3.1 LSB

The Least Significant Bit (LSB) is one of the important strategies in spatial domain image steganography. LSB is the base massive piece inside the byte estimation of a photo pixel. The LSB based picture steganography installs the diversion name in minimum great predictable bits of pixels approximations of the blanket photo. It exploits the truth that the level of accuracy in lots of picture formats is a lengthy way greater than that perceivable through average human inspired and prescient. Thusly, an altered picture with moderate forms in hints may be unclear from the interesting through an individual, just by taking a looking at it. In LSB approach only four bytes of pixels are adequate to grip one message byte. Remaining bits in the pixel left overs the equal [16].

The LSB Steganography Algorithm is as follows:

```
Input: A cover image C and a message m
Output: A stego-image S
Step 1: Generate random sequences using seed (stego-key) save as path []
Step 2: $index = 1$
Step 3: for $i = 1$ to length($m$) do
Step 4: $n$ = path[$index$]
Step 5: $S_n \leftarrow \mathrm{LSB}(C_n) = m_i$
Step 6: $index \leftarrow index + 1$
Step 7: end for
```

3.2 RSA (RIVEST SHAMIR ALDEMAN)

RSA is the utmost usually used public key encryption set of rules. RSA computation consists of integers modulo $n = p*q$. It asks for a key of at least 1024 bits for suitable safety. 2048-bit duration keys offer extremely good protection. Generally used for relaxed communication channel and for authentication to identification provider. RSA is simply too sluggish for encrypting large volumes of information. But it's miles harshly used for key distribution. Following steps are followed in RSA to generate the public and private keys

Step 1: Consider two large prime numbers p and q such that p ~= q.2.

Step 2: Compute $n = p*q$

Step 3: Compute $\varphi(pq) = (p-1) * (q-1)$

Step 4: Consider the general public key k_1 such that GCD ($\varphi(n)$, k_1) = 1; 1 < k_1 < $\varphi(n)$

Step 5: Select the private key k_2 such that k_2* okay mod$\varphi(n)$ = 1 Encryption and Decryption are carried out as follow Encryption:

Step 6: Calculate cipher text C from plaintext P such that C=P^$k_1$mod$n$ Decryption: P = C^k_2 mod n = P^k_1k_2 mod n [14]

3.3 DISCRETE WAVELET TRANSFORM (DWT)

The strategy of DWT is used to study the multi-level signal switch can consider the signal at extraordinary frequency bands so that it is an extraordinary targets by method for breaking down it into estimate and unique inflection. The calculation rule is dividing the photo into 4 at each new band, 3 obstructs on the focal points of the photograph (*LH*, *HL*, *HH*), and the fourth (*LL*) looks for the greatest vital information for the eye (low frequencies), which appears to be the reason for the resulting recurrence [17]. The method uses this picture to break into sub photograph: high and Low pass filter. The DWT can be followed:

$$X_f\left(a_2b\right)=\int_{-\infty}^{+\infty} f\left(t\right)\frac{1}{\sqrt{a}}\Psi^*\left(\frac{t-b}{a}\right)dt \qquad (1)$$

LL	***HL***
LH	***HH***

Fig.1. Four bands of DWT

4. PROPOSED WORK

4.1 DESCRIPTION OF THE PROBLEM

The statement of the problem includes inserting a secret message in the LSB of each RGB pixels value of the cover picture. In this approach, the study implemented a technique called LSB insertion on the images. This is a challenging process that will inspire us to combine two technologies. One of them is RSA algorithm from cryptography and LSB substitution from steganography. The main target of this research is to provide double security to the secret message by applying encryption algorithm as well as steganography technique. So, dual security of data is achieved in this proposed work. Here the asymmetric key cryptography algorithm is used to encrypt the message where symmetric key algorithm is used in existing technique.

4.2 PROPOSE METHODOLOGY

The proposed scheme has been implemented in the MATLAB platform for the use of steganography set of preferred cryptography and regulations. The Fig.2 of the proposed statistics shows the work of the protection plan.

The Fig.2 is the proposed system architecture of this research work. In this, many steps are followed. So the whole algorithm is subdivided into subsections.

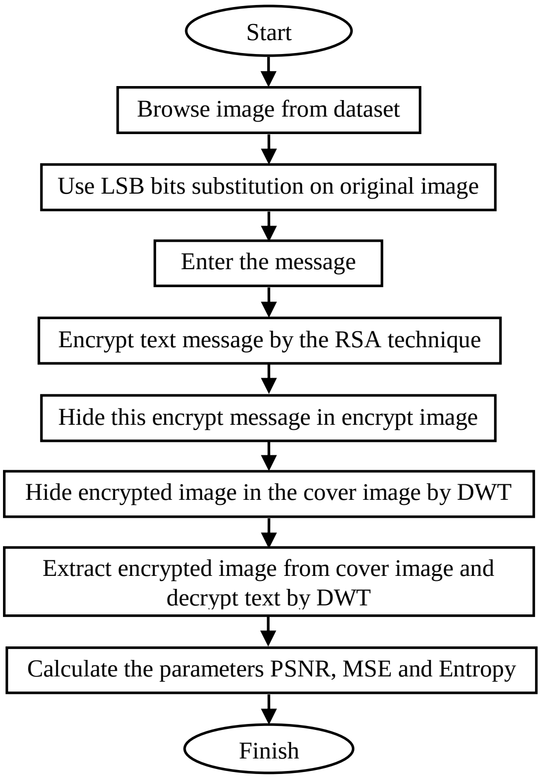
Start
Browse image from dataset
Use LSB bits substitution on original image
Enter the message
Encrypt text message by the RSA technique
Hide this encrypt message in encrypt image
Hide encrypted image in the cover image by DWT
Extract encrypted image from cover image and decrypt text by DWT
Calculate the parameters PSNR, MSE and Entropy
Finish

Fig.2. Flow chart of proposed work

4.3 COVER IMAGE SELECTION

This is the initial process of the proposed system. First of all, the study selects a cover image from the dataset. If the browsed image is in RGB, then it had converted into grayscale image and it must be resized to 512×512 pixels. Some of the images of the image dataset are shown in Fig.3.

Fig.3. Sample Test Images

4.4 APPLY LEAST SIGNIFICANT BIT SUBSTITUTION

The Least Significant Bit (LSB) is one of the essential techniques in spatial domain photograph steganography. LSB is the bottom big bit inside the byte value of a photograph pixel. The LSB based picture steganography embeds the name of the game in least good sized bits of pixels values of the quilt photograph. Therefore, an altered image with moderate versions in hues might be indistinguishable from the unique via a human being, simply by looking at it. In LSB approach just four byte of pixels are sufficient to hold one message byte. Rest of bits in the pixel remains the equal.

4.5 ENCRYPTION PROCESS

RSA algorithm is used for encrypting the message. It is an asymmetric cryptography algorithm. Asymmetric means it works on two different keys. One is used for encryption and the other is for decryption. In this algorithm, the study encrypt data using public key and decrypt data using private key. The public key is common to everyone but the private key is kept private.

4.6 EMBEDDING PROCEDURE

The dual transform based steganography is advanced in that benefit a composite of integer wavelet transform and DWT to plant a secret image in the cover. The PSNR results are discussed in huge imperceptibility and the planting method to a combination of steganography and the cryptography. Here, encrypted data is embedded to the singular area of detail coefficient.

4.7 EXTRACTION AND DECRYPTION PROCESS

The receiver will use its private key to implement RSA algorithm, because the secret data recipient is encrypted by public key. Using the receiver's private key cipher text will be converted into original message which is in readable form. In the decrypting process, a hash function is used to detect the positions of the LSB and DWT where the data bits had been embedded. When the position of the bits had been specified, the bits are removed from the position in the same sequence as they were embedded. Hide the encrypted image in the image converted by DWT. Remove the encrypted image from cover image and decrypt the text by DWT.

4.8 QUANTITATIVE ANALYSIS

The Mean Square Error and Peak Signal to Noise Ratio are two parameters which are used for quantitative measure of proposed method. MSE is used to measure the error between the cover image and stego image. PSNR is used to measure the maximum noise which the signal tolerates. The Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) between the stego image and its corresponding cover image have been studied.

Calculate PSNR and MSE value of image steganography gray cover image by the following equations.

$$MSE(x) = \frac{1}{N}\left\|x - x'\right\|^2 = \frac{1}{N}\sum_{i=1}^{N}(x - x')^2 \tag{2}$$

where, *MSE* is Mean Square Error, *x* is cover Image, *x′* is Extracted Image, *N* is the size of cover Image.

$$PSNR(x) = \frac{10\log\left(double(m).\wedge 2\right)}{MSE(x)} \tag{3}$$

where, *PSNR* is peak signal to noise ratio, m is peak signal level for a color image have been taken as 255 and it is the maximum value of the Cover Image. For the analysis of cover image and stego image, another parameter is also used i.e. Entropy (Average information content). It measures the proportions of the details of the image. It is usually measured in units as bits.

$$E(p) = \sum_{i=0}^{G-1} P(i)\log P(i) \tag{4}$$

where, *P*(*i*) is probability density function of a given image at intensity level *l* and *G* is total number of grey levels in the image. If the entropy value of an image is high then it is considered to be having better quality and have more details.

5. RESULT ANALYSIS

In this result analysis, simulations and consequences of our projected system are revealed. In our experiment, the hardware environment of a personal computer with an Intel Core i5 2430M 2.4GHz CPU with 4GB RAM. The operating system is Windows 7 and running Matlab. The work is here defined in an easy and effective way. To present the work effectively, the graphical interface is designed. This is used to process the testing dataset and text which send securely in the communication channel along with specification of work stages. The Fig.2 display the graphical interface for the further processing.

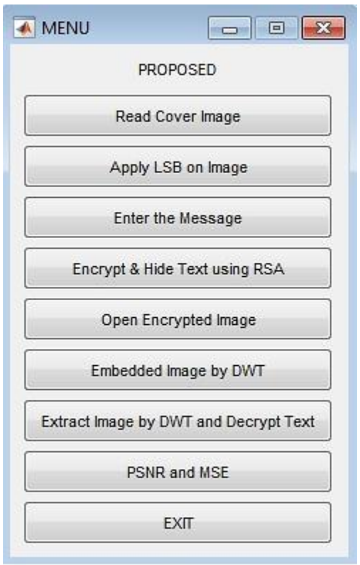

Fig.4. Main Menu

- Firstly browse the image from dataset where many images are available for the processing. Only one image can be chosen at a time of instant. The selected image is converted into the greyscale image. The greyscale image with size 512×512 is shown in Fig.5. It is the cover image for the steganography process.

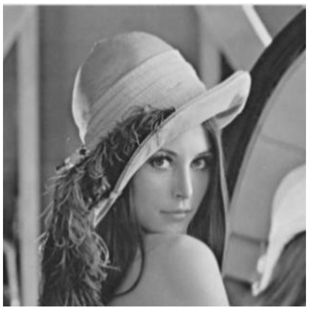

Fig.5. Cover Image

- After selecting the cover image, the LSB bits substitution is applied on the cover image. This is the original image which is embedded later to the stego image with DWT technique. So it is hard to detect the original secure data. The Fig.6 shows the LSB bits substituted image.

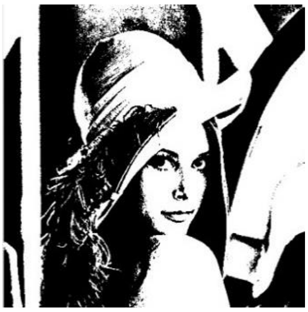

Fig.6. LSB bits substitution

- The plain text is entered by the sender which he/she want to send. After plain text is accepted, it will convert into cipher text using the RSA encryption technique.

Enter the text and also enter the prime number for key encryption.

Enter the message: hello

Implementation of RSA Algorithm

Enter the value of *p*: 19

Enter the value of *q*: 23

ASCII Code of the entered Message: 104 101 108 108 111

Cipher Text of the entered Message: 225 100 52 52 80

- Now the encrypted text is hidden behind the encrypted image. The use of RSA algorithm has made our technique more secure for open channel. The Fig.7 shows the stego image.

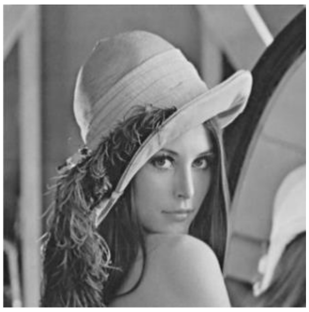

Fig.7. Stego Image

- After getting the stego image, it will be embedded into the original image. This image is transferred into the communication channel from sender to receiver which hides the encrypted image in which the message is hidden.

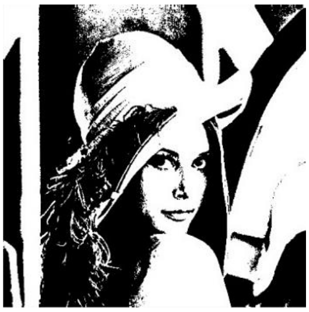

Fig.8. Embedded Image

There is two level protection is applied to the original message. First is the message is encrypted itself and then the cover image is also encrypted. Then it is embedded into original image.

- In the decoding process, the LSB extraction process is used to get the message bits. When the position of the bits had been specified, the bits are then extracted from the position in the same order as they were embedded. Extract encrypted image from cover image by DWT and decrypt text by RSA technique with receiver's private key.

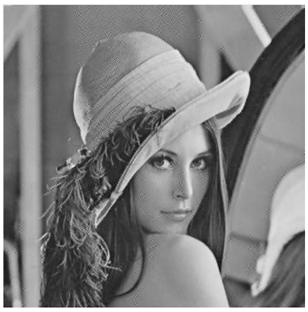

Fig.9. Extracted Image

***Decrypted ASCII of Message*: 104 101 108 108 111**

***Decrypted Message is*: hello**

- Now calculate MSE, PSNR and Entropy of the cover image and stego image. For the better results, high value of PSNR and low value of MSE is required. These values are calculated for some related images and shown below in tables and graphs.

Table.1. Proposed PSNR and Proposed MSE

Image Name	MSE		PSNR (in dB)	
	Existing Technique [15]	Proposed Technique	Existing Technique [15]	Proposed Technique
Lena.jpg	1.7149	1.2041	64.89	71.2145
Baboon.jpg	1.7137	1.2038	64.88	71.2626
Coloredchips.bmp	1.6889	1.1947	64.73	72.3243
Peppers.bmp	1.7185	1.2050	64.83	71.1131
Pears.png	1.6932	1.1989	64.94	71.8331
Monalisa.png	1.7246	1.2118	64.83	70.3249

Table.2. Entropies of Cover Images and Stego Images

Name of the image file	Entropy of Cover Image	Entropy of Stego Image
Lena	7.4469	7.4470
Baboon	7.3606	7.3607
Colored Chips	7.1904	7.1905
Peppers	7.5818	7.5819
Pears	7.2587	7.2588
Monalisa	6.9881	6.9882

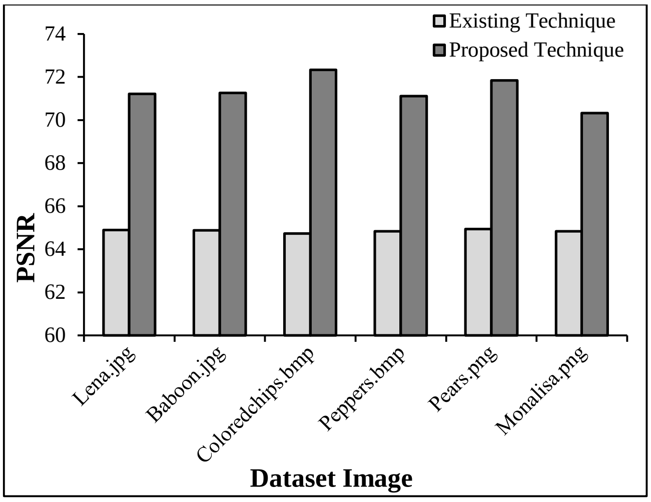

Fig.10. Graph of PSNR

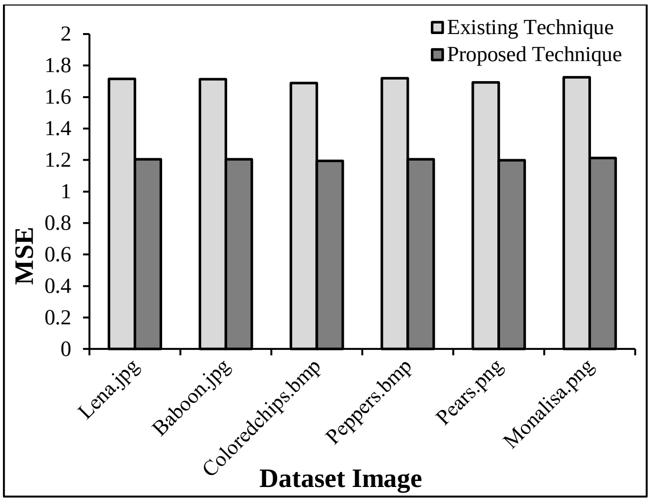

Fig.11. Graph of MSE

By comparing the MSE and PSNR values of all the images, MSE of images used is less and PSNR of the images in proposed technique is higher than the existing technique. High value of PSNR and low value of MSE is required to get output image similar to input image, so it gives the better result. The obtained entropy result of images shows that the entropy of stego image is slightly greater than cover image. It is because of the more hidden information is added to the cover image.

6. CONCLUSION

With the growth of digital age and internet, steganography has incredibly advanced people in a few years. Steganography, which is mainly shared with the cryptography, is a strong tool that secretly licenses to replacing the records. It will take a look at the attacker's information about each cryptography and steganography. If an attacker is capable to extracting information from the picture then he has to crack the hybrid cryptography, then the best he's going to get the proper records. The power of LSB-RSA and DWT hybrid increased the range of security in the proposed approach where the symmetric key cryptography algorithm is used for encryption in the existing technique. In the result of proposed approach, the encryption time is better than the triumphing method. It provides the extra protection in assessment to the triumphing one. It can be very difficult to use the attack of brute force in this technique because RSA can be used for LSB and DWT. As the improvement in existing technique, the proposed method obtains higher values of PSNR and lower values of MSE for images to achieve the better result. Exceptional steganography strategies can be used in the future with more hybrid cryptography for greater security.

REFERENCES

[1] Ashadeep Kaur, Rakesh Kumar and Kamaljeet Kainth, "Review Paper on Image Steganography", *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 6, No. 6, pp. 472-477, 2016.

[2] Mehdi Hussain and Mureed Hussain, "A Survey of Image Steganography Techniques", *International Journal of Advanced Science and Technology*, Vol. 54, pp. 1053-1059, 2013.

[3] Hemang A. Prajapati and Nehal G. Chitaliya, "Secured and Robust Dual Image Steganography: A Survey", *International Journal of Innovative Research in Computer and Communication Engineering*, Vol. 3, No. 1, pp. 534-542, 2015.

[4] Pratap Chandra Mandal, "Modern Steganographic Technique: A Survey", *International Journal of Computer Science and Engineering Technology*, Vol. 3, No. 9, pp. 894-901, 2012.

[5] Dipti Kapoor Sarmah and Neha Bajpai, "Proposed System for Data Hiding using Cryptography and Steganography", *International Journal of Computer Applications*, Vol. 8, No. 9, pp. 640-647, 2010.

[6] Kedarnath Choudry and Aakash Wanjari, "A Survey Paper on Video Steganography", *International Journal of Computer Science and Information Technologies*, Vol. 6, No. 3, pp. 786-792, 2015.

[7] Himani Trivedi and Arpit Rana, "A Study Paper on Video Based Steganography", *International Journal of Advance Research, Ideas and Innovations in Technology*, Vol. 3, No. 1, pp. 493-499, 2017.

[8] Ammad Ul Islam et al., "An Improved Image Steganography Technique based on MSB using Bit Differencing", *Proceedings of IEEE 6th International Conference on Innovative Computing Technology*, pp. 1478-1485, 2016.

[9] Shaikh Shakeela, P. Arulmozhivarman, Rohit Chudiwal and Samadrita Pal, "Double Coding Mechanism for Robust Audio Data Hiding in Videos", *Proceedings of IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology*, pp. 678-686, 2016.

[10] G. Sateesh, E.S. Lakshmi, M. Ramanamma, K. Jairam and A. Yeswanth, "Assured Data Communication Using Cryptography and Steganography", *International Journal of Latest Technology in Engineering, Management and Applied Science*, Vol. 5, No. 3, pp. 545-551, 2016.

[11] Hanaa M. Ahmed and Maisaa A.A. Khodher, "Comparison of Eight Proposed Security Methods using Linguistic Steganography Text", *International Journal of Computing and Information Sciences*, Vol. 12, No. 2, pp. 712-719, 2016.

[12] Jigar Makwana and S.G Chudasama, "Dual Steganography: A New Hiding Technique for Digital Communication", *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, Vol. 5, No. 4, pp. 1346-1354, 2016.

[13] M.J. Thenmozhi and T. Menakadevi, "A New Secure Image Steganography Using LSB and SPIHT Based Compression Method", *Proceedings of National Conference on Information Communication, VLSI and Embedded Systems*, pp. 843-850, 2016.

[14] Ting-Wei Chuang, Chaur-Chin Chen and Betty Chien, "Image Sharing and Recovering based on Chinese Remainder Theorem", *Proceedings of International IEEE Symposium on Computer, Consumer and Control*, pp. 487-494, 2016.

[15] Shivani Chauhan and Janmejai Kumar, "Multiple Layer Text Security using Variable Block Size Cryptography and Image Steganography", *Proceedings of* 3rd *IEEE International Conference on Computational Intelligence and Communication Technology*, pp. 1406-1412, 2017.

[16] B. Padmavathi and S. Ranjitha Kumari, "A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique", *International Journal of Science and Research*, Vol. 2, No. 4, pp. 1656-1662, 2013.

[17] Sachin Gaur and Vinay Kumar Srivastava, "Robust Embedding of Improved Arnold Transformed Watermark in Digital Images using RDWT-SVD", *Proceedings of 4th IEEE International Conference on Parallel, Distributed and Grid Computing*, pp. 799-805, 2016.