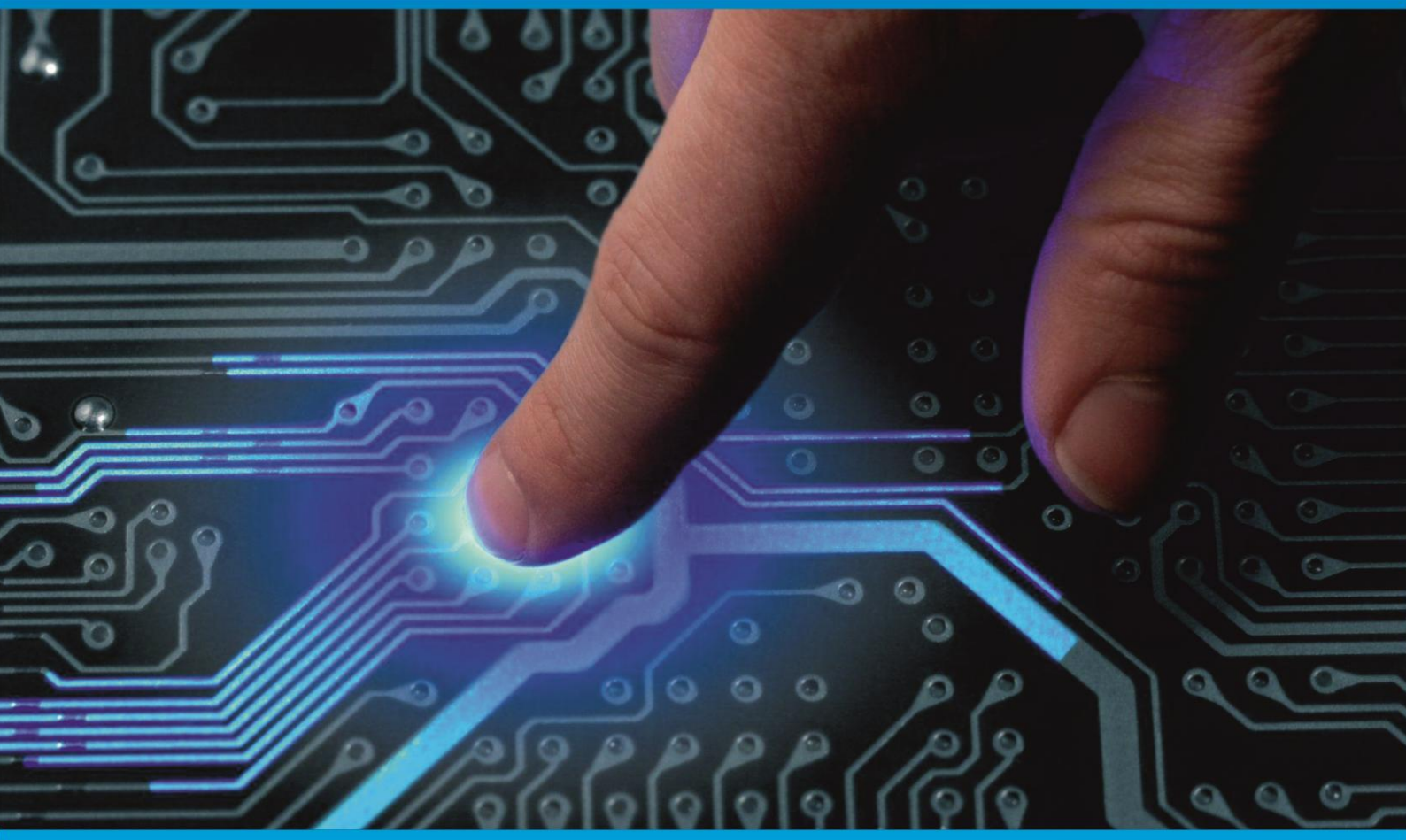
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 3, March 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 3, March 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0903045 |

Implementing Novel Cryptography Technique in Image Encryption and Secure Data Hiding

R.Padmavathy, P.Alaguthai.,Msc,M.Phil

Student, Dept. of Computer Science, Sakthi College of Arts and Science for Women, Oddanchatram, TamilNadu, India

Assistant Professor, Dept. of Computer Science, Sakthi College of Arts and Science for Women, Oddanchatram, TamilNadu, India

ABSTRACT:Reversible data hiding technique in encrypted secret image and hiding the original image. The pixels of the image and a special encryption scheme are designed to encrypt the estimating errors. Without the encryption key, one cannot get access to the original image. The data hiding key only, it can embed in or extract from the encrypted image additional data without knowledge about the original image. The data extraction and image recovery are free of errors for all images. Experiments demonstrate the feasibility and efficiency of the proposed method. A bench- mark encryption algorithm (e.g. AES) is applied to the rest pixels of the image and a special encryption scheme is designed to encrypt the estimating errors. Without the encryption key, one cannot get access to the original image. However, provided with the data hiding key only, he can embed in or extract from the encrypted image additional data without knowledge about the original image. Moreover, the data extraction and image recovery are free of errors for all images. Experiments demonstrate the feasibility and efficiency of the proposed method, especially in aspect of embedding rate versus Peak Signal-to-Noise Ratio (PSNR). And also used LSB the least significant bit (lsb) is the bit position in a binary integer giving the units value, that is, determining whether the number is even or odd. The lsb is sometimes referred to as the right-most bit, due to the convention in positional notation of writing less significant digit further to the right.

1. INTRODUCTION

Reversible data hiding (RDH) has the capability to erase the distortion introduced by embedding step after cover restoration. It is an important property that can be applied to many scenarios, such as medical imagery, military imagery and law for entices. For this reason, RDH becomes a hot research topic and is extensively studied over the years. Until now, many RDH techniques have been proposed based on three fundamental strategies: lossless compression- appending scheme [difference expansion (DE) and histogram shift (HS)]. Some recent arts combined the three strategies to residuals of the image such as prediction errors (PE) to achieve better performance. Almost all state-of- the-art RDH algorithms consist of two steps. Generates a host sequence with small entropy, i.e., the host has a sharp histogram which usually can be realized by using PE combined with the sorting technique or pixel selection. The second step reversibly embeds the message in the host sequence by modifying its histogram with methods like HS and DE. On the other hand, some robust RDH methods have also been proposed. Least significant bit (LSB) technique has been proposed. HLSB technique where the secret information is embedded in the LSB of the cover frame. Hash function is used to select the position of insertion in LSB bits. In this technique has been used mean square error (MSE).

Its h help to error required in original image. The proposed technique is compared with existing LSB based secret message and the results are found to be encouraging. Level of information increased and LSB maintain the separate key. We can easily clear the secret image, so we can get in original image. Reversible data hiding in images is a technique that hides data in digital images for secret communication. It is a technique to hide additional message into cover media with a reversible manner so that the original cover content can be perfectly restored after extraction of the hidden message. In this paper has been used image encrypted and decrypted method. Encryption is an effective and popular means of privacy protection. In order to securely share a secret image with other person, a content owner may encrypt the image before transmission. “Selective encryption”. Secure multimedia distribution one part the data is encrypted.

There are two levels of security for digital image encryption: low level and high-level security encryption. In low-level security encryption, the encrypted image has degraded visual quality compared to that of the original one, but the content of the image is still visible and understandable to the viewers. In the high-level security case, the content is completely scrambled and the image just looks like random noise.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 3, March 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0903045 |

The content owner encrypts the signs of host discrete cosine transform (DCT) coefficients. Different fingerprints are generated at the receiver side by decrypting only a subset of the coefficients with different decryption keys. The intra-prediction mode, motion vector differences and DCT coefficients' signs are encrypted, while watermarking process proceed son the DCT coefficients' amplitudes adaptively. a commutative watermarking and encryption system is presented based on a layered scheme and a key dependent transform domain. However, the data embedding is not reversible with the above-mentioned techniques. This paper proposes a novel RDH method in encrypted spatial images based on estimation technique.

A large portion of pixels are utilized to estimate the rest before encryption, and then encrypted with a standard encryption algorithm. After that we encrypt the estimating errors with a special encryption scheme. By concatenating encrypted estimating errors and the large group of encrypted pixels, the ultimate version of encrypted image is formulated. The additional data can be embedded in the encrypted image by modifying the estimating errors. In general, the excellent performance can be achieved in three different prospects. The proposed method is completely reversible. The extraction and decryption steps are independent, which are more natural and applicable.

II. LITERATURE REVIEW

2.1 DATA HIDING IN ENCRYPTED IMAGES USING DCT

Reversible data hiding in images is a technique that hides data in digital images for secret communication. It is a technique to hide additional message into cover media with a reversible manner so that the original cover content can be perfectly restored after extraction of the hidden message. In this paper has been used image encrypted and decrypted method. Encryption is an effective and popular means of privacy protection. In order to securely share a secret image with other person, a content owner may encrypt the image before transmission. “Selective encryption”. Secure multimedia distribution one part the data is encrypted. There are two levels of security for digital image encryption: low level and high-level security encryption. In low-level security encryption, the encrypted image has degraded visual quality compared to that of the original one, but the content of the image is still visible and understandable to the viewers. In the high-level security case, the content is completely scrambled and the image just looks like random noise.

Encryption

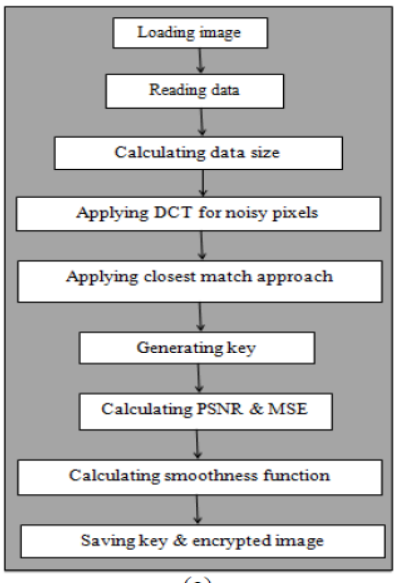


Fig 2.1 Block diagram for Encryption

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 3, March 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0903045 |

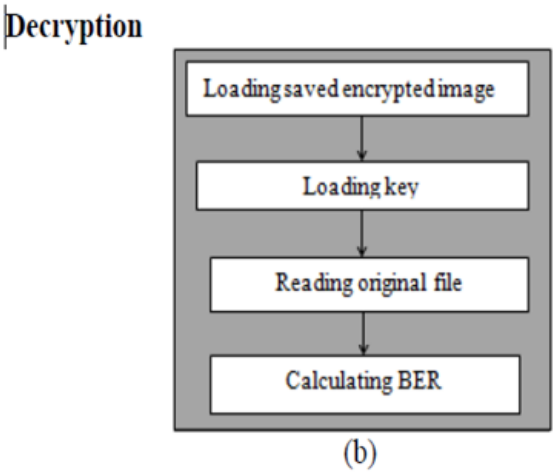


Fig 2.2 Block diagram for decryption

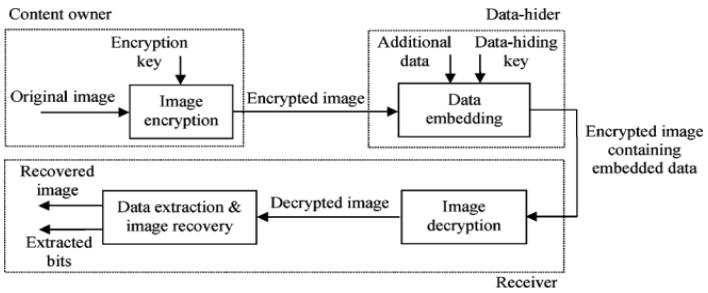
III. SYSTEM ANALYSIS

3.1 EXISTING SYSTEM:

In the existing system reversible data hiding technique the image is encrypted by using the without encryption key and the data to hide is embedded in to the image by using the data hiding. At the receiver side he first need to extract the image using the encrypted image in order to extract the data and after that he'll use data extraction process to extract the embedded data. It is a serial process and is not a separable process. The PSNR values of marked decrypted image are much higher than those previous method can achieve under given embedding rates. The extraction and decryption steps are independent, which are more natural and applicable

3.2 Proposed Scheme:

The proposed scheme is made up of image encryption, data embedding and data extraction/image-recovery phases. The content owner encrypts the original uncompressed image using an encryption key to produce an encrypted image. Then, the data-hider compresses the least significant bits (LSB) of the encrypted image using a data-hiding key to create a sparse space to accommodate the additional data. At the receiver side, the data embedded in the created space can be easily retrieved from the encrypted image containing additional data according to the data-hiding key. Since the data embedding only affects the LSB, a decryption with the encryption key can result in an image similar to the original version. When using both of the encryption and data-hiding keys, the embedded additional data can be successfully extracted and the original image can be perfectly recovered by exploiting the spatial correlation in natural image.



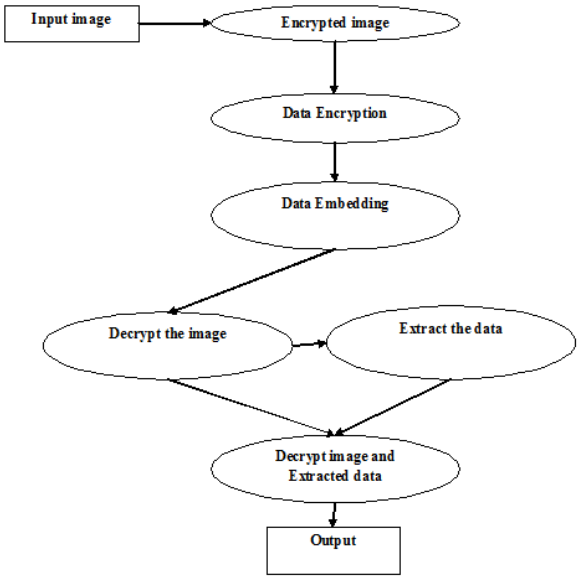
In this paper, hash based least significant bit (LSB) technique has been proposed. HLSB technique where the secret information is embedded in the LSB of the cover frame. Hash function is used to select the position of insertion in LSB bits. In this a technique has been used, mean square error (MSE).

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 3, March 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0903045 |

3.3 ARCHITECTURE:



IV. SYSTEM IMPLEMENTATION

4.1 Image Encryption:

Assume each pixel with gray value of the original image is falling into [0, 255] represented by 8 bits.

1 Denote the gray value as $p_{i,j}$,where (i , j) indicates the pixel position, and bits of a pixel as $b_{i,j,0}$, $b_{i,j,1}$,…, $b_{i,i,7}$

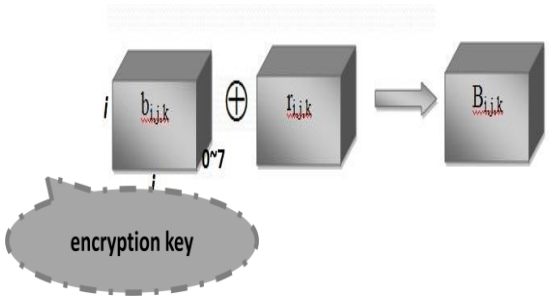
$$b_{i,j,k} = \left\lfloor \frac{p_{i,j}}{2^k} \right\rfloor \bmod 2 \quad k=0,1,\ldots,7 \quad \text{and} \quad p_{i,j} = \sum_{u=0}^{7} b_{i,j,k} \cdot 2^k$$

2 exclusive-or results of the original bits and pseudo-random bits

$r_{i,j,k}$, determined by an encryption

$B_{i,j,k}$, concatenated orderly as the encrypted data

$$B_{i,j,k} = b_{i,j,k} \oplus r_{i,j,k}$$



4.2 Data Encryption

Here we are implementing data encryption method for secure data transmission. In Existing Algorithm have many drawbacks like key value is limited, because here we are using DES Algorithm.

4.2.1Data Encryption Standard (DES) is also known as Data Encryption Algorithm (DEA). DEA takes 64 bits of plain text and 56 bits of key to produce 64 bits cipher text block. The DES algorithm always functions on blocks of equal size and uses the permutations and substitutions in algorithm.

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 3, March 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0903045 |

4.2.2 Triple DES:

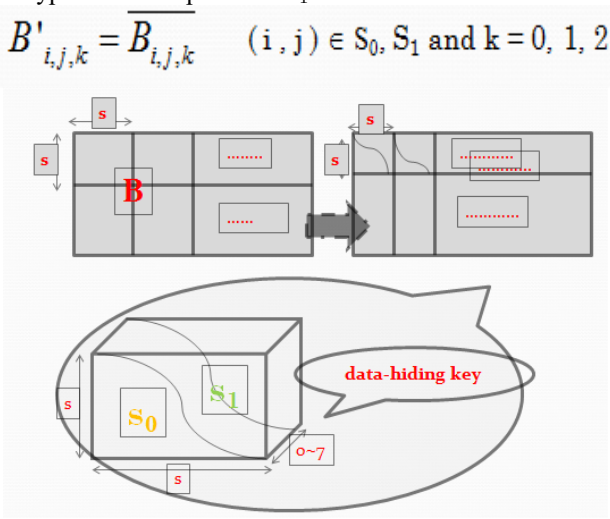
Triple DES is an extension to the DES algorithm. Triple DES uses the same approach for encryption as DES. 3DES takes three 64 bit keys which has a total length of 192 bits. We can give more than one key that is two or three keys for encryption as well as for decryption such that the security will be stronger.

4.3 Embedding Process

1. segment the encrypted image into non overlapping blocks sized by s × s
   - $B_{i,j,k}$, satisfying
     - $(m-1) \cdot s + 1 \le i \le m \cdot s$
     - $(n-1) \cdot s + 1 \le j \le n \cdot s$
     - $0 \le k \le 7$
   - pseudo-randomly divide the s^2 pixels into two sets S_0 and S_1
     - probability that a pixel belongs to S_0 or S_1 is ½
2. check the additional bit to be embedded is 0 or 1

   - 0 , flip the 3 LSB of each encrypted pixel in S_0
   - 1 , flip the 3 encrypted LSB of pixels in S_1

$$B'_{i,j,k} = \overline{B_{i,j,k}} \qquad (i,j) \in S_0, S_1 \text{ and } k = 0, 1, 2$$



4.4 Data revealing and Image recovery

1 Generate $r_{i,i,k}$ (by encryption key)

2 Calculates the exclusive-or of the received data and $r_{i,i,k}$
   - decrpted bits as $b'_{i,i,k}$

$$b'_{i,j,k} = r_{i,j,k} \oplus B'_{i,j,k} = r_{i,j,k} \oplus \overline{B_{i,j,k}} = r_{i,j,k} \oplus \overline{b_{i,j,k} \oplus r_{i,j,k}} = \overline{b_{i,j,k}} \quad k = 0, 1, 2$$

   - the original five most significant bits (MSB) are retrieved

3 The three decrypted LSB must be different from the original LSB, in this case

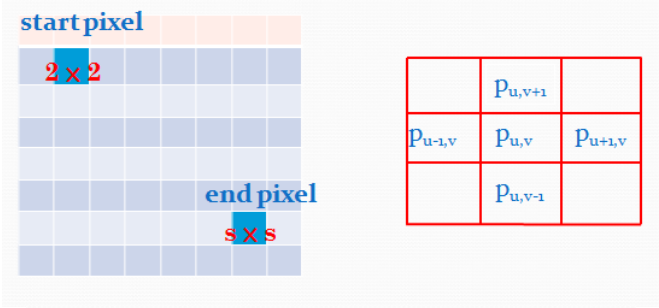
   - segment the decrypted image into blocks with the data-hiding key
   - divide the pixels in each block into two sets .

4 Concatenate the extracted bits and collect the recovered blocks

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 3, March 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0903045 |



$$f=\sum_{u=2}^{s-1}\sum_{v=2}^{s-1}\left| p_{u,v}-\frac{p_{u-1,v}+p_{u,v-1}+p_{u+1,v}+p_{u,v+1}}{4}\right.$$

4.4.1 The average energy of errors between the decrypted and original gray values is

- The sum of decimal values of three decrypted LSB and three original LSB must be seven.

$$E_A=\frac{1}{8}\cdot\sum_{u=0}^{7}[u-(7-u)]^2=21$$

4.5 Deriving PSNR and MSE value from the image

4.5.1 PEAK SIGNAL-TO-NOISE RATIO (PSNR)

The term peak signal-to-noise ratio (PSNR) is an expression for the ratio between the maximum possible value (power) of a signal and the power of distorting noise that affects the quality of its representation. Because many signals have a very wide dynamic range, (ratio between the largest and smallest possible values of a changeable quantity) the PSNR is usually expressed in terms of the logarithmic decibel scale.

4.5.1 PSNR and MSE Calculation

For the following implementation, let us assume we are dealing with a standard 2D array of data or matrix. The dimensions of the correct image matrix and the dimensions of the degraded image matrix must be identical. The mathematical representation of the PSNR is as follows:

$$PSNR = 20\log_{10}\left(\frac{MAX_f}{\sqrt{MSE}}\right)$$

Figure 1 - Peak Signal-to-Noise Equation

where the MSE (Mean Squared Error) is:

$$MSE=\frac{1}{mn}\sum_{0}^{m-1}\sum_{0}^{n-1}\|f(i,j)-g(i,j)\|^2$$

Figure 2 - Mean Squared Error Equation

This can also be represented in a text based format as:

MSE = (1/(m*n))*sum(sum((f-g).^2))

PSNR = 20*log(max(max(f)))/((MSE)^0.5)

Legend:

f represents the matrix data of our original image

g represents the matrix data of our degraded image in question

m represents the numbers of rows of pixels of the images and i represents the index of that row

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 3, March 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0903045 |

n represents the number of columns of pixels of the image and j represents the index of that column
$\mathbf{MAX_f}$ is the maximum signal value that exists in our original "known to be good" image

V. CONCLUSION

In this paper, a new method is proposed to map secret data to the gray-levels of the carrier image by utilising the concepts of transposition, bitxoring, bits shuffling, secret key, and cryptography with high imperceptibility and security. An average PSNR of 58dB, RMSE with 0.6673, and NCC with 0.9917 is achieved using the proposed method which are better than the existing method in the literature with PSNR=40, MSE=0.8115. The proposed method improved the security as well as the quality of stego images and provided promising results in terms of high PSNR, and less histogram changeability as compared to existing methods. The distinguishing properties of the proposed algorithm include transposition, bitxoring, and bits shuffling, adding multiple security levels to the proposed method. These different security levels create multiple barriers in the way of an attacker. Therefore, it is difficult for a malicious user to extract the actual secret data.

VI. FUTURE ENHANCEMENT

The main objective of this study is to provide an overall idea about the popular as well as emerging data hiding techniques in spatial and transform domains. This study deals with both reversible and non-reversible data hiding methods. Also, this study briefly discusses some common steganalytic techniques and concludes with an idea of the future scope of Secure data transmission. The wide range of these techniques will provide a good overview about current trends in transform domain steganography to the researchers who are interested in steganography.

REFERENCES

[1] M. K. I. Rahmani and N. P. Kamiya Arora, "A crypto-steganography: A survey," International Journal of Advanced Computer Science and Application, vol. 5, pp. 149–154, 2014. [2] J. V. Karthik and B. V. Reddy, "Authentication of secret information in image stenography," International Journal of Computer Science and Network Security (IJCSNS), vol. 14, no. 6, p. 58, 2014.
[3] M. H. Rajyaguru, "Crystography-combination of cryptography and steganography with rapidly changing keys," International Journal of Emerging Technology and Advanced Engineering, ISSN, pp. 2250–2459, 2012.
[4] D. Seth, L. Ramanathan, and A. Pandey, "Security enhancement: Combining cryptography and steganography," International Journal of Computer Applications (0975–8887) Volume, 2010.
[5] H. Abdulzahra, R. AHMAD, and N. M. NOOR, "Combining cryptography and steganography for data hiding in images," ACACOS, Applied Computational Science, pp. 978–960, 2014.
[6] P. R. Ekatpure and R. N. Benkar, "A comparative study of steganography & cryptography," 2013.
[7] N. Khan and K. S. Gorde, "Data security by video steganography and cryptography techniques," 2015.
[8] M. K. I. Rahmani and M. A. K. G. M. Mudgal, "Study of cryptography and steganography system," 2015.
[9] C. P. Shukla, R. S. Chadha, and A. Kumar, "Enhance security in steganography with cryptography," 2014.
[10] P. Kumar and V. K. Sharma, "Information security based on steganography & cryptography techniques: A review," International Journal, vol. 4, no. 10, 2014.
[11] J. K. Saini and H. K. Verma, "A hybrid approach for image security by combining encryption and steganography," in Image Information Processing (ICIIP), 2013 IEEE Second International Conference on. IEEE, 2013, pp. 607–61.1
[12] H. Sharma, K. K. Sharma, and S. Chauhan, "Steganography techniques using cryptography-a review paper," 2014.
[13] A. Dhamija and V. Dhaka, "A novel cryptographic and steganographic approach for secure cloud data migration," in Green Computing and Internet of Things (ICGCIoT), 2015 International Conference on. IEEE, 2015, pp. 346–351.
[14] P. Vijayakumar, V. Vijayalakshmi, and G. Zayaraz, "An improved level of security for dna steganography using hyperelliptic curve cryptography," Wireless Personal Communications, pp. 1–22, 2016.
[15] S. S. Patil and S. Goud, "Enhanced multi level secret data hiding," 2016.
[16] B. Karthikeyan, A. C. Kosaraju, and S. Gupta, "Enhanced security in steganography using encryption and quick response code," in Wireless Communications, Signal Processing and Networking (WiSPNET), International Conference on. IEEE, 2016, pp. 2308–2312.
[17] B. Pillai, M. Mounika, P. J. Rao, and P. Sriram, "Image steganography method using k-means clustering and encryption techniques," in Advances in Computing, Communications and Informatics (ICACCI), 2016 International Conference on. IEEE, 2016, pp. 1206–1211.
[18] A. Hingmire, S. Ojha, C. Jain, and K. Thombare, "Image steganography using adaptive b45 algorithm combined with pre-processing by twofish encryption," International Educational Scientific Research Journal, vol. 2, no. 4, 2016.
[19] F. Joseph and A. P. S. Sivakumar, "Advanced security enhancement of data before distribution," 2015.

INNO SPACE

SJIF Scientific Journal Impact Factor

Impact Factor:
7.488

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details