ISSN No. 0976-5697

Volume 5, No. 5, May-June 2014

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Image Encryption for Separable Reversible Data Hiding

S.Lavanya
Assistant Professor, Computer Science and Engineering,
Anna University, Regional Centre, Coimbatore, India

Dr.S.Palaniswami
Principal, Government College of Engineering,
Bodinayakanur, Tamil Nadu, India

S.Rijutha
PG Student, Anna University, Regional Centre,
Coimbatore, India

Abstract— Separable reversible data hiding is a new methodology used for security and authentication in images. A technique that has been implemented in order to combine image cryptography, data hiding and LSB compression. In the first phase, a content owner encrypts the actual uncompressed image using a stream cipher algorithm. Then, a data hider may compress the least significant bits of the enciphered image using a data hiding key to create a sparse space to accommodate some additional data. With an enciphered image containing concealing data, if the receiver has the data hiding key, can extract the concealing data even though the receiver does not know the image. If the receiver has the encryption key, can change the enciphered image in to an understandable format in order to obtain an image similar to the actual one, but cannot extract the concealing data. If the receiver has both the data hiding key and the encryption key, can extract the concealing data and recover the actual content without any error by exploiting the spatial correlation in natural image when the amount of additional data is not too large.

Index Terms — LSB compression, reversible data hiding, stream cipher, image cryptography, data hiding.

I. INTRODUCTION

Today, in the digital age, The term digitization is often used when varied forms of information, such as manuscript, utterance, picture or articulate, are transformed into a single binary code, which is stored for an indefinite period, and transmitted at high speeds. In spite of these advantages, digital data also has a downside. It is easy to access illegally, tamper with, and copy for purposes of copyright violation. There is, therefore, a need to hide secret identification inside certain types of digital data. This information can be used to prove exclusive rights, to identify attempts to tamper with sensitive data. Storing, hiding, or embedding secret information in all types of digital data is one of the tasks of the field of the steganography.

Cryptography and Steganography are well known and widely used techniques that influence information in order to code or hide their existence. Cryptography scrambles a message so it cannot be understood; the Steganography hides the message so it cannot be seen. Even if both methods afford security, a study is made to unite both Cryptography and Steganography methods into one system for better privacy and security. Internet users required to accumulate, send or obtain the secret data. The common way to do this is to transform the secret data into another form, this process is called Encryption. Steganography and cryptography both are used for the purpose of sending the data securely. The comparable approach is followed in Steganography as in cryptography like encryption, decryption using secret key. In steganography the message is kept secret without any changes but in cryptography the actual content of the message is differed in different stages like encryption and decryption. Here, the drawback is if enough time is given the enemy is allowed to intercept and modify the messages. In order to avoid this steganography is used.

Steganography or stego means “covered writing”[16] which is derived from the Greek words. The art and science of hiding information by embedding messages inside, it seems to be risk-free messages. Steganography is a mechanism by replacing bits of ineffective or unused facts in accepted computer archive (such as graphics, utterance, manuscript, HTML, or even diskette) with bits of unrelated, untraceable information. This unseen information can be plain manuscript, cipher text, or even images. Steganography occasionally is used when encryption is not permissible. An enciphered file may still hide information by means of steganography, yet if the enciphered file is deciphered, the secret message is not seen.

Cryptography is the study of information conceal and authentication. It includes the protocols, algorithms and strategies to securely and constantly avoid or holdup an unauthorized access to sensitive information and enables verifiability of every component in a communication. Only users with the covert knowledge can convert the opaque information back into its useful form. The covert knowledge is generally called the key, though the covert knowledge may include the complete progression or algorithm that is used in the encipher/decipher. The information in its useful form is called clear text, in its enciphered form it is called cipher text. The technique used for enciphering and deciphering is called a cipher (or cipher).

Steganography is useful even in cases where cryptographic tools are available and provide adequate safety measures. Embedding data in a cover is technical challenge. The concealing data should not increase the size of the cover, because this would be manifest to an attacker familiar with the actual cover. Secret data ought to be concealing in holes in the steganography faces the additional challenge of embedding the secret data in a robust way to

make it impervious to lossy compression and other operations that may modify the cover.

In the existing system the content owner encrypts the actual image using stream cipher algorithm by generating an encryption key, and a data-hider be able to embed additional information into the encrypted image using a data-hiding key by LSB compressing techniques even though the receiver does not know the actual content. With an encrypted image containing extra data, a receiver might first decrypt it according to the encryption key, and then extort the concealed data and recover the actual image according to the data-hiding key. In this scheme, the data removal is not separable from the content decryption. In other words, the added data must be extracted from the decrypted image, so that the major content of actual image is exposed before data extraction, and, if receiver has the data-hiding key but not the encryption key, recipient cannot extort any information from the encrypted image containing extra data.

The planned method is made up of image enciphering, data concealing and data-extrication/image-recuperate phases. The content owner encrypts the actual uncompressed image using an encryption key to produce an enciphered image. Then, the data-hider compresses the least significant bits of the enciphered image using a data-hiding key to produce a sparse space to accommodate the extra data. At the receiver side, the data concealed in the created space can be easily retrieved from the encrypted image containing additional data according to the data-hiding key. Since the data concealing only affects the LSB, a decipher with the encryption key can have an end result in an image similar to the actual version. When using both of the encryption and data-hiding keys, the concealed added data can be effectively extracted and the actual image can be flawlessly recovered by exploiting the spatial correlation in natural image.

II. LITERATURE SURVEY

In the literature, many data hiding methods exploring the spatial domain and Frequency domain of images has been proposed. Bender et al. [12] proposed The technique of least significant-bit (LSB) replacement, in which a secret message is concealed in the least significant bits of image pixel values. Mielikainen [13] Proposed a modified LSB replacement method which embeds as many bits as the expected method, but alters less pixel values. Yang et al. [14] planned an Adaptive k-LSB substitution technique in which larger values of k are adopted in the Edge areas of the cover image and smaller ones are used for the smooth areas. Wang et al. [15] transformed image block contents into coefficients in the frequency domain By the discrete cosine transform (DCT) and concealed secret bits by modifying the Magnitude relations between the AC values of image blocks. Besides data embedding Techniques using the DCT, the discrete wavelet transforms (DWT) [17] and the discrete Fourier transform (DFT) [18-19] have also been used.

In recent years, several researchers have revealed a large form of image data hiding techniques in the literatures. These techniques are often classified roughly into 3 approaches, i.e., the spatial domain, the frequency domain, and also the compression domain. Within the spatial domain, the cover image is altered directly and undetectably to hide the secret message. Lee and Chen [18] proposed a steganographic algorithm applied within the spatial domain during which the smallest amount important bit (LSB) of every pixel within the cover image was replaced by secret data. Later, Chang et al.[19] found the best LSB substitution for embedding secret data by using a dynamic programming strategy. By applying each run-length coding and standard computation, Chang et al. [16] designed 2 efficient data hiding ways for icon files and grayscale files

A number of reversible data hiding methods have been proposed and investigated in recent years [8]. In difference expansion method [1], differences between two adjacent pixels are doubled to generate a new least significant bit (LSB) plane for accommodating extra data. A data hider can also execute reversible data hiding using a histogram shift mechanism, which effectively makes use of the zero and peak points of the histogram of an image and slightly modifies the pixel gray values to embed data into the image [2]. Another kind of method makes use of redundancy in a cover by performing lossless compression to create a spare space for data embed-ding [3]. Furthermore, various skills have been introduced into the typical reversible data hiding approaches to improve the performance [4]–[6]

Reversible data hiding (RDH) in images is a method, by which the actual cover can be losslessly recuperate after the concealed message is extricated. This significant method is extensively used in medical imaging, armed forces and law forensics, where no deformation of the actual cover is allowed. Since first introduced, RDH [9] has attracted considerable research interest. With regard to providing secrecy for images, enciphering is an efficient and accepted means as it converts the actual and meaningful content to indecipherable one. Even though few RDH techniques in encrypted images have been available yet, there are some hopeful applications if RDH [9] can be useful to enciphered images. To separate the data extraction from image decryption, the idea of compressing encrypted images and the space for data embedding; Compression of encrypted data [8] can be formulated as source coding with side information at the decoder, in which the distinctive method is to produce the compressed data in lossless approach by exploiting the syndromes of parity-check matrix of channel codes. The scheme used to compress the encrypted LSBs to memory space for extra data by finding syndromes of a parity-check Matrix [10] and the side information used at the receiver side is also the spatial correlation of decrypted images.

Lossy compression is a technique in which an enciphered grey image can be proficiently compressed by discarding the excessively rough and the information of coefficients generated. When having the compressed data, a recipient may renovate the primary content of actual image by recovering the values of coefficients. A pseudorandom transformation is used to encipher an actual image, and the enciphered data are proficiently compressed by removing the excessively rough and fine information of coefficients generated. After receiving the compressed data, with the support of spatial interaction in natural image, a recipient can restructure the primary content of the actual image by iteratively updating the values of coefficients [11]. This way, the higher the compression ratio and the smoother the actual image, the better the quality of the reconstructed image. The compression ratio and the quality of reconstructed image vary with different values of compression parameters.

III.PROPOSED METHODOLOGY

The proposed scheme is made up of image encryption, data concealing and data-extrication/image-recuperation phases. The content owner encrypts the actual uncompressed image using a standard stream cipher which generates an encryption key to produce an enciphered image. LSB embedding, we always lose some information from the cover image. This is an result of hiding directly into a pixel. To do this we must get rid of some of the cover's information and restore it with information from the data to hide hence the data-hider uses the LSB compression method to compresses the least significant bits of the enciphered image using a data-hiding key to generate a sparse space to accommodate the extra data. At the receiver side, the data concealing in the created space can be easily retrieved from the enciphered image containing additional data according to the data-hiding key. Since the data hiding only affects the LSB, a deciphering with the encryption key and the outcome is an image similar to the actual version. When using both of the encryption and data-hiding keys, the concealing additional data can be successfully extracted and the actual image can be perfectly recovered by exploiting the spatial correlation in natural image. Hence the higher embedding capacity & improved PSNR value indicates that the reconstruction of image is of higher quality and MSE value is estimated in order to qualify the difference between the initial and the distorted or noisy image.

The procedure of separable method is also made up of image encryption, data embedding and data-extrication/ image-recuperation phases which are shown in the Fig 1. Content owner can encrypt the image before transmission by using encryption key. And extra data can be further added using the data hiding key. At the recipient side if recipient has only data hiding key, can only extract the data from image. If the recipient has encryption key then the receiver can decrypt the image. But if the recipient has both, data hiding and encryption key then the receiver can extract the hidden data and as well as can recover image. Using encryption key content owner encrypt image. Then the data hider creates a sparse space for hiding data by replacing least significant bits (LSB) in encrypt image using data hiding key.

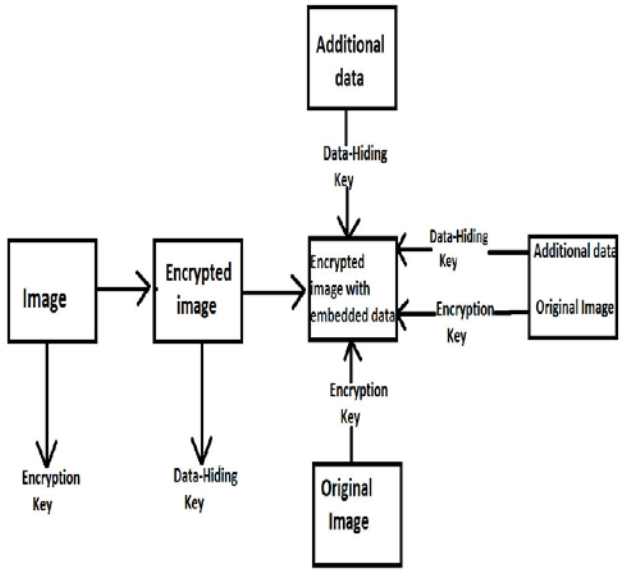


Figure.1. Separable reversible data-hiding

A. Image Encryption:

Take an actual uncompressed image from the database with a size N1*N2 each pixel with gray value falling into [0,255] is represented by 8 bits. Denote the bits of a pixel as bi,j,0, bi,j,1, …… bi,j,7, the gray value as bi, j and the number of pixels as N (N=N1*N2). Convert the actual image into grayscale image and resize it to a dimension 200*200. Image encryption involves generation of encryption key and generation of pseudo-random sequence.

A stream cipher is a symmetric key cipher where plaintext digits are combined with a pseudorandom cipher digit stream (key stream). In a stream cipher each plaint manuscript digit is enciphered one at a time with the corresponding digit of the key stream, to give a digit of the cipher manuscript stream. The encryption of each digit is reliant on the current state. A digit is typically a bit and the combining function an exclusive-or (xor).

Encryption key is 128 bit value. It is generated randomly by using the random function. The random function generates the random key in a uniformly distributed function. Pseudo random sequence consists of random bits generated using the encryption key. The number of bytes generated should be equal to the number of pixels in the input image provided the pixels are represented as 8-bit values. If the pixels are represented as 16-bit values then the number bytes in Pseudo random sequence should be double the number of pixels. Perform xor operation between actual bits and pseudo-random bits to obtain the enciphered image.

$$B'_{i,j,k} = b'_{i,j,u} \oplus r_{i,j,u} \ldots \quad (1)$$

Where $r_{i,j,u}$ are determined by an encryption key using a standard stream cipher. Then, $B_{i,j,u}$ are concatenated orderly as the enciphered data. A number of protected stream cipher methods can be used here to make sure that anybody without the encryption key, such as a aggressor or the data hider, cannot gain any information about actual content from the enciphered data.

B. Data Embedding:

In data concealing phase, the extra data is concealing into the enciphered image using a data-hiding key though he does not know the actual content. Consider an enciphered

image as a input image. Some parameters are concealing into a small number of enciphered pixels, and the LSB of the other enciphered pixels are compressed to create a space for accommodating the additional data and the actual data at the positions occupied by the parameters [18]. According to a data-hiding key, data hider pseudo-randomly selects Np enciphered pixels that will be used to carry the parameters for data concealing. Here, Np is a small positive numeral, for example, Np=20.The other (N-Np) enciphered pixels are pseudo-randomly permuted and divided into an amount of groups, each of which contains L pixels. The transformation way is also regulated by the data-hiding key. For each pixel-type, gather the M least significant bits of the L pixels, and represent them as B(k,1),B(k,2)…B(k, M. L) where k is a group index within[1,(N-Np)/L]. Here, S is a small positive integer. Then, hide the values of the variables M, L and S into the LSB of NP chosen enciphered pixels. For the example of NP=20 the data-hider may represent the values of M,L and S as 2,14 and 4 bits, respectively and replace the LSB of selected enciphered pixels with the 20 bits

$$R = (((N-Np).S/L-Np))/N \approx S/L \quad \ldots \quad (2)$$

Where, R is enciphered data concealing rate, N is Number of pixels present in the enciphered image, NP is Number of pixels which carries the parameters, S is Small positive integer and L is Number of pixels in each pixels group. Construct the fixed point numeric object for the enciphered image. Generate data hiding key using pseudo-random generator and randomly selects the enciphered pixel. Determine the LSB bit of the image using the function getlsb(). Compress the LSB bits using LSB compression technique. Data is concealing to the spare space created.

C. Data Extrication And Image Recuperation:

When having an enciphered image containing concealing data, the three cases which is shown in Fig 2. depicts that a recipient have merely the data-hiding key, merely the encryption key, and together the data-hiding and encryption keys, respectively. At the receiver side the receiver can receive the information based on their requirements in 3 cases. The three cases include, first case receiver has only the data-hiding key for extracting only the concealing data so that the image is not revealed, second case only the encryption key where the enciphered image is deciphered without revealing the hidden data, and third case where both the data-hiding key and encryption keys, are used in order to extract the hidden data and to recover the actual image respectively. PSNR and MSE value is calculated in order to check the reconstructed image quality

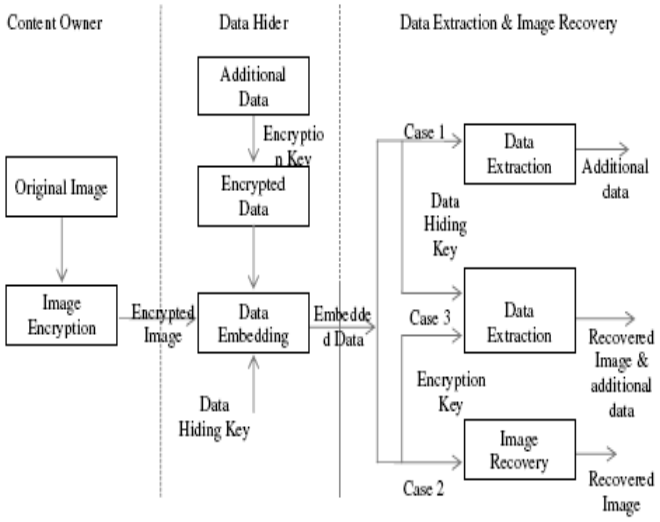


Figure.2. Three cases at receiver side of the proposed method CASE 1: Only Data-Hiding Key

With an enciphered image containing concealing data, if the receiver has only the data-hiding key, can first obtain the values of the parameters M, L, S from the LSB of the Np selected enciphered pixels. (N-NP) pixels into (N-NP)/L groups and extracts the S concealing bits from the M LSB-planes of each group. When having the total (N-NP).S/L extracted bits, the receiver can divide them into NP actual LSB of selected enciphered pixels and (N-NP).S/L-NP additional bits. Note that because of the pseudo-random pixel selection and transformation, any aggressor without the data-hiding key cannot gain the parameter values and the pixel-groups, therefore cannot haul out the concealing data. Furthermore, the recipient having the data-hiding key can effectively extract the concealing data.

CASE 2: Only Encryption Key

Consider the case that the receiver has the encryption key but does not know the data-hiding key. Obviously, recipient cannot find the values of parameters and cannot extract the concealing data. However, the actual image content can be approximately recovered. The receiver can decrypt the received data,

$$b'_{i,j,k} = B'_{i,j,k} \oplus r_{i,j,u} \quad \ldots \quad (3)$$

Where $r_{i,j,u}$ are derived from the encryption key. The gray values ofdeciphered pixels are

$$p'_{i,j} = \sum_{u=0}^{7} b'_{i,j,k} \quad \ldots \quad (4)$$

Since the data-embedding operation does not alter any MSB of enciphered image, the deciphered MSB must be same as the actual MSB. The value of PSNR in the directly deciphered image is calculates using MSE which is given as,

$$PSNR = 20 * \log10 (MSE) \quad \ldots \quad (5)$$

The mean squared error is defined as,

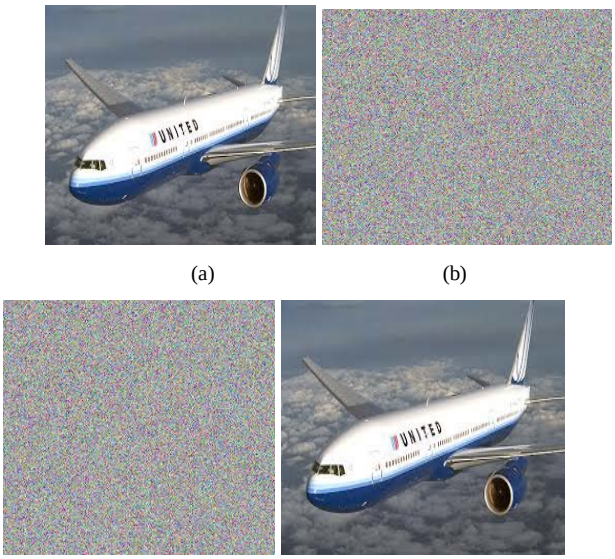
$$MSE = \frac{1}{MN} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i,j) - K(i,j)]^2 \ldots \quad (6)$$

Where, M and N are the dimensions of the pictures I and K are the two pictures to be compared.

CASE 3: Both Encryption Key and Data-Hiding Key

If the receiver has both the data-hiding and the encryption keys, the receiver may aim to extract the concealing data and recover the actual image. According to the data-hiding key, the values, the actual LSB of the chosen enciphered pixels, and the extra bits can be extracted from the enciphered image containing concealing data. By putting the LSB into their actual positions, the enciphered data of the selected pixels are retrieved, and their actual gray values

can be correctly deciphered using the encryption keys. In the following, we will recover the actual gray values of the other pixels. Considering a pixel-group, must be one of the vectors meeting As long as the number of pixels in a group is sufficiently large and there are not too many bits concealing into each group, the actual content can be perfectly recovered by the spatial correlation criterion. Since the different must be calculated in each group, the calculation complexity of the content recuperation. On the other hand, if more neighbouring pixels and a smarter prediction method are used to estimate the gray values, the performance of content recuperation will be improved, but the estimated complexity is higher. To keep a low estimated complexity, we let be fewer than ten and use only the four neighbouring pixels to calculate the estimated values.



(a) (b)

(c) (d)

Fig.3. (a) Actual plane, (b) its enciphered version, (c) enciphered version containing concealing data with embedding rate 0.0516bpp, and (d) directly deciphered version with PSNR 46.9534 dB and MSE 0.7637.

Table I Quality metrics for various standard test images

TEST IMAGES	PERFORMANCE METRICS			
	PSNR	MSE	BPP	TIME
SHIP	46.9225	0.7614	0.0562	1.153774
PLANE	46.9534	0.7637	0.0516	1.176137
CHILD	47.3169	0.8306	0.0492	1.020845
FLOWER	47.9610	0.9629	0.0800	1.090821

IV. PERFORMANCE EVALUATION

The test image Plane sized 200×200 shown in Fig.3 (a), used as the input images in the experiment. After image encryption using the standard stream cipher method, the eight enciphered bits of each pixel are converted into a gray value to generate an enciphered image shown in Fig 3(b). Embed 2064 additional bits into the enciphered image using LSB compression technique to create a sparse space to accommodate some additional data. The enciphered image containing the concealing data is shown in Fig. 3(c), and the embedding rate 0.05165 bit per pixel (bpp). With an enciphered image containing concealing data we could extract the concealing data using the data-hiding key. If we directly deciphered the enciphered image containing concealing data using the encryption key, the value of PSNR in the deciphered image was 47.0 dB, which verifies the theoretical value 46.9534 dB calculated by (12) and MSE is 0.7631. The directly deciphered image is given as Fig. 3(d). By using together the data-hiding and the encryption keys, the concealing data could be successfully extracted and the actual image could be perfectly recovered from the enciphered image containing concealing data. Hence the higher embedding capacity & improved PSNR value indicates that the reconstruction of image is of higher quality and MSE value is estimated in order to qualify the difference between the initial and the distorted or noisy image.

Table I depicts the quality metrics for various standard images. PSNR (dB) indicates the energy of distortion caused by data hiding, the MSE measures the average of the squares of the errors and the Bit Per Pixel (bpp), which specifies the number of bits used and Elapsed time id duration of image enciphered with concealing data. . The average value of PSNR is observed to be quite good and MSE is fairly close to zero.

Table 2 Performance Metrics - BPP & Elapsed Time

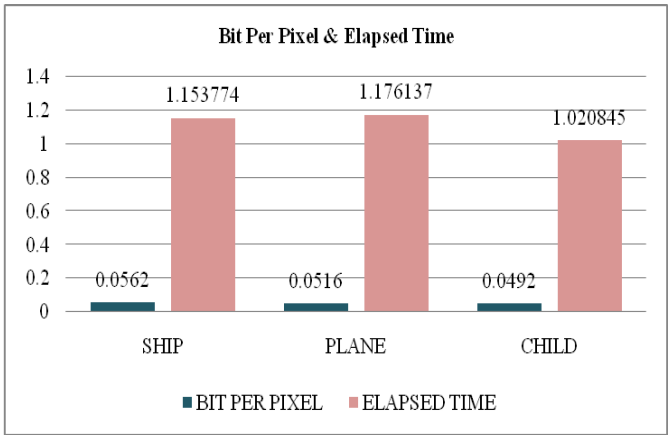


Table II depicts the quality metrics of Bit per Pixel and Elapsed Time of the images. BPP is the number of bits of information stored per pixel of an image or displayed by a graphics adapter. Elapsed time is the time taken to encrypt and to embed additional data into an image.

Table III Performance Metrics – PSNR & MSE

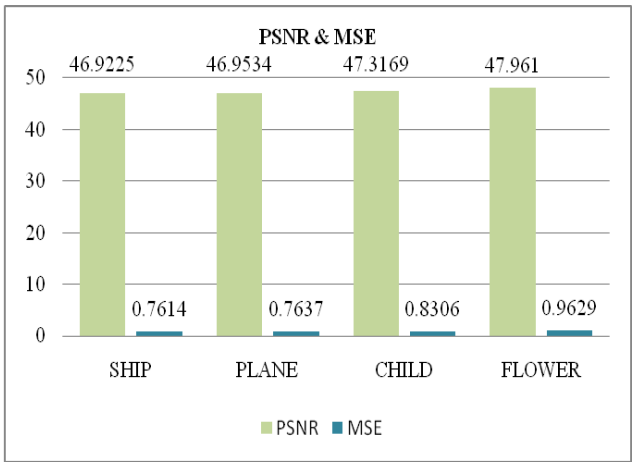


Table III depicts the quality metrics of PSNR and MSE. PSNR (dB) indicates the energy of distortion caused by data hiding, the MSE measures the average of the squares of the errors and the Bit per Pixel (bpp), which specifies the number of bits used and Elapsed time id duration of image encrypted with embedded data. . The average value of

PSNR is observed to be quite good and MSE is fairly close to zero.

V. CONCLUSION AND FUTURE WORK

Reversible data hiding scheme for enciphered image with a low computation difficulty is projected, which consists of image encryption, data concealing and data-extrication/image-recuperation phases. The data of actual image are entirely enciphered by a stream cipher. Even though a data hider does not familiar with the actual content, recipient can embed additional data into the enciphered image by modifying a part of enciphered data. With an enciphered image containing concealing data, a receiver may firstly decrypt it using the encryption key, and the deciphered version is similar to the actual image. According to the data hiding key, with the help of spatial connection in natural image, the concealing data can be correctly extracted while the actual image can be flawlessly recovered. Even if someone with the knowledge of encryption key can obtain a deciphered image and sense the presence of hidden data using LSB steganalytic methods, if receiver does not know the data hiding key, it is still not possible to haul out the extra data and recover the actual image. The implemented a reversible method can be enhanced in future by using the following provisions and MLSB technique can also be applied after embedding when there is lot of change in the pixel to retain nearest to the actual value. It can be applied in networking and the keys are sent and received securely. The image produced by the reversible data hiding using two key has alteration. In order to remove alteration and to generate the image in a high eminence using 3 key. In future we can use audio, video in case of image as cover for hiding the data.

VI. REFERENCES

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

[2]. Z.Ni ,Y.-Q .Shi, N.Ansari,and W.Su,"Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, 2006.\

[3]. U. Celik, G.Sharma,A.M.Tekalp , E .Saber, `"Lossless generalized-LSB data embedding," IEEE Trans. Image Process. ,vol.14, no. 2, pp. 253–266, Feb. 2005.

[4]. L. Luo, Z. Chen, M. Chen, X. Zeng, and Z. Xiong, "Reversible image watermarking using interpolation technique,"IEEE Trans. Inf. Foren- sics Secur., vol. 5, no. 1, pp. 187–193, 2010.

[5]. W. Hong, T.-S. Chen, Y.-P. Chang, and C.-W. Shiu, "A high International Journal of Emerging Science and Engineering (IJESE) ISSN: 2319–6378, Volume-2, Issue-3, January 2013 21 capacity reversible data hiding scheme using orthogonal projection and prediction error modification, "Signal Process., vol.90, pp.2911–2922,2010.

[6]. C.-C. Chang, C.-C. Lin, and Y.-H. Chen, "Reversible data embedding scheme using differences between actual and predicted pixel values, "Inform. Secure. , vol. 2, no. 2, pp. 35–46, 2008.

[7]. W. Zeng, "Digital watermarking and data hiding: technologies.

[8]. M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, "On compressing enciphered data," IEEE Trans. Signal Process., vol. 52, no.10, pp. 2992-3006, Oct. 2004.

[9]. Kede Ma, Weiming Zhang, "Reversible Data Hiding in Enciphered Images by Reserving Room Before Encryption" IEEE Trans. VOL. 8, no. 3, Mar 2013.

[10]. X. Zhang, "Lossy compression and iterative reconstruction for enciphered image," IEEE Trans. Inform. Forensics Security, vol. 6, no.1, pp. 53-58, Feb. 2011.

[11]. W. Liu , W. Zen g L. Don g and Q. Yao, — Efficient compression of enciphered grayscale images,‖ IEEE Trans. Image Process., vol. 19, no. 4, pp. 1097–1102, Apr. 2010.

[12]. W. Bender, D. Gruhl, N. Morimoto and A. Lu, Techniques for data hiding, IBM Systems Journal 35 (3-4) (1996) 313-336

[13]. J. Mielikainen, LSB matching revisited, IEEE Signal Processing Letters 13 (5) (2006) 285-287.

[14]. C. H. Yang, C. Y. Weng, S. Wang and H. M. Sun, Adaptive data hiding in edge areas of images with spatial LSB domain systems, IEEE Transactions on Information Forensics and Security 3 (3) (2008) 488-497

[15]. Y. N. Wang and A. Pearmain, Blind image data hiding based on self reference,Pattern Recognition Letters 25 (15) (2004) 1681-1689.

[16]. L. S. T. Chen, S. J. Lin and J. C. Lin, Reversible JPEG based hiding method with high hiding-ratio, Int. Journal of Pattern Recog. and Artificial Intelligence, 24 (2010) 1-23.

[17]. S. H. Wang and Y. P. Lin, Wavelet tree quantization for copyright protection watermarking, IEEE Trans. Image Processing, 13 (2) (2004) 154-165.

[18]. C. M. Pun, A novel DFT-based digital watermarking system for images, Proceedings of 8th Int. Conf. on Signal Processing, Guilin, Yunnan, China, 2006, pp. 1245-1248.

[19]. S. Pereira and T. Pun, Robust template matching for affine resistant image watermarks, IEEE Trans. on Image Process. 9 (6) (2000) 1123-1129.

Short Bio Data for the Author

Lavanya S has received her B.Tech degree in Information Technology from Mohamed Sathack Engineering College in 2006, Kilakarai, and M.Tech degree in Information Technology from Anna University Coimbatore in 2009 and MBA degree in Information System Management from Bharathiyar University in 2012. She is currently pursuing her Ph.D from Anna University, Regional Centre Coimbatore. She is currently working as Assistant Professor in the Department of Computer Science and Engineering, Regional Centre Anna University, Coimbatore, India. She has published more than 8 research papers in various journals and conferences. She has organized 3 national level workshops. She is a student member of IEEE.

Dr. S. Palaniswami, has received his B.E degree in Electrical and Electronics Engineering from University of Madras, Chennai and M.E degree in Applied Electronics from Government College of Technology, Coimbatore, in 1981 and 1986 respectively. He has received his Ph.D from the faculty of Electrical and Electronics Engineering, Anna University, Chennai in 2003. He has more than 33 years of academic and research experience and currently he holds the post of Principal, Government College of Engineering, Bodinayakanur, India. He has published more than 65 research papers in various journals and conferences. He has organized more than 10 workshops.

S. Rijutha has completed her B.Tech degree in Information Technology from Avinashilingam University, Faculty of Engineering, Coimbatore in 2011, and currently she is a PG scholar at Anna University Regional Centre, Coimbatore with a specialization of Software Engineering. She is currently working as Lecturer in the Department of Information Technology, Tejaa Shakthi Institute of Technology for Women, Coimbatore, India.