Cryto Data Hiding using Modified Interpolation Method

Balkrishan Jindal[1], Veerpal Kaur [2]

[1]Assistant Professor, Yadavindra College of Engineering, Punjabi University Guru Kashi Campus, Talwandi Sabo-151302, District: Bathinda (Punjab) India.

[2] Research Student, Yadavindra College of Engineering, Punjabi University Guru Kashi Campus, Talwandi Sabo-151302, District: Bathinda (Punjab) India.

Abstract— In this paper, a crypto data hiding using interpolation method is proposed. The proposed method of data hiding is implemented in two-phases. In the first phase, secret data is encrypted using RSA algorithm to add additional layer of security to the embedded data. In the second phase, crypto data is hidden into the cover image using proposed method of data hiding algorithm. The receiver receives the stego image to extracts the encrypted data using the proposed data extraction algorithm. To receive the original data, decryption is performed by receiver on the encrypted data with the help of private key of RSA algorithm. To evaluate the performance of the proposed method various Image Quality Metrics (IQM) are measured in terms of Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), Data hiding capacity, Structure Similarity Index Matching (SSIM) and Correlation. From experimental results, it has been concluded that the proposed method is better than other non reversible data hiding methods such as Jung et al. method, MPD method in term of PSNR and as well as in security.

***Keywords* —** RSA, Data Hiding, Crypto Data, PSNR

INTRODUCTION

Due to rapid development of technology, data hiding plays an integral role for transmitting of confidential data. Both cryptography techniques [1-3] and steganography techniques [4-22] provide security to the confidential data. To achieve complete security of data and get best quality of stego image, it is better way to combine both methods for data hiding. Cryptography techniques convert the plain text into cipher text form. Cipher text is visible to everyone. Steganography is the art and science of embedding the secret data into the cover media without the existence of embedded data which overcomes the limitation of cryptography. Internet is not trustworthy due to existence of fraud and copyright. In order to provide security to the information send over the internet, data hiding become mandatory. Data hiding is also termed as information hiding. Presently, data hiding [4-22] is divided into two forms such as Reversible Data Hiding method [4, 5, 9, 10] and Non Reversible data hiding method [1, 6]. In reversible data hiding method, the distortion is completely removed from the original cover image. It is also defined as method in which the receiver gets both the original cover image and as well as original data. Interpolation based methods [4, 9] and histogram shifting based methods [7] are examples of reversible data hiding method. Whereas Non-Reversible data hiding method refers to in which the receiver extracts only the secret data without getting an original cover image such as Least Significant Bit [8] and Pixel Value Difference (PVD) [8] methods. The quality of stego image is better in Non- Reversible data hiding method as compared to reversible data hiding method. Interpolation methods are categorized into two categories as adaptive and non-adaptive method. In the adaptive method, they focus on the characteristic of the image such as an edge. Non- Adaptive methods are those methods of interpolation that deal all the pixels in equality. Neighbor Mean Interpolation (NMI) [10], Enhanced Neighbor Mean Interpolation (ENMI) [7], and Modified Neighbor Mean Interpolation [9] are examples of Non- Adaptive methods.

LITERATURE REVIEW

In this section, various methods of data hiding used by different author and their performance of work are described.

Jindal and Singh presented the data hiding method based upon both cryptography and steganography [1]. They use flexible matrix in combination with Pythagorean Theorem in order to encrypt the secret data. Then divide the cover image into two blocks such as lower pixel blocks and upper pixel block. They embedded the crypto data using moderate bit substitution method into the upper pixel block of the cover image and apply the pixel adjustment process on the lower block of the cover image. Then, combined both the blocks and apply the post pixel adjustment to generate the stego image. They also applied the T test for validation of their work. From the experimental results, it is clear that presented method achieves high security and robustness.

Malik et al. introduced the reversible data hiding based on Modified Neighbor Mean Interpolation (MNMI) method [4]. Firstly, they interpolate the original cover image using MNMI method to generate the modified cover image and embed the secret data into the modified cover image using two pass. In the first pass, secret data is hidden into the odd pixels of the modified cover image and in the second pass; embed the secret data into the even pixels of the interpolated image. They compared their results with Jung and Yoo's method and Chang et al.'s method in term of image quality and data hiding capacity.

Tai et al described the separated reversible data hiding technique based on public key cryptography [5]. The presented method includes image encryption, data hiding, extraction of data and recovery of cover image. Image is encrypted using public key by the image owner. Secret data is hidden into the encrypted image using data hiding key by the data hider. After extraction of the secret data, image is decrypted using private key. Their method of data hiding is mostly used in cloud services.

Shahana presented the steganography technique based on Discrete Cosine Transform (DCT) and RSA algorithm [6]. Firstly, secret image is encrypted using RSA algorithm in order to provide more security to the hidden data. Then, divide the cover image into 8 by 8 blocks and apply DCT on each block of the cover image. After applying the DCT on each block, they embedded the crypto image into the cover image to get stego image. Experimental results of the presented method are better in term of image quality.

Chang et al. introduced the information hiding technique based on the Enhanced Neighbor Mean Interpolation (ENMI) method [7]. Cover image is scaled down using image processing tool and scaled up the cover image using ENMI method to get the modified cover image. Then data embedding is performed into the modified cover image. In order to gain the high payload, they apply the histogram modification method on the stego image. From their experimental results it is quite evident that presented method of data is better in term of image quality as compared to Jung and Yoo's method [10].

Jung et al presented the novel approach of data hiding by using both Least Significant Bit (LSB) and Multi Pixel Difference (MPD) [8]. According to the sum of pixel, they divide the cover image into two regions such as smooth blocks and edge block. For the smooth block, they applied the LSB method to embed the secret data and they applied the MPD method on edge block method to hide the secret data. They compared their results with the existing MPD, 2-Bit LSB and Pixel Value Difference (PVD).

Malik et al. describe the improved version of Neighbor Mean Interpolation method [9]. According to authors, NMI method requires more calculation and complexity. To reduce the calculation and complexity, they introduced the Modified Neighbor Mean interpolation [MNMI]. Firstly, input image is interpolated by using MNMI method so that enlarged image more resembles to the input image. Then, hide the data into the modified cover image. From their experimental results, it is clear that presented interpolation algorithm produce better quality of stego image as compared to other interpolation algorithm. They also show that the introduced data embedding method gain high data hiding capacity.

Jung and Yoo presented the reversible data hiding method using Neighbor Mean interpolation method [10]. They apply the NMI method on the cover image for interpolation of pixels. Then, divide the interpolated image into 2 by 2 non overlapping block and perform the data embedding into the modified cover image. They showed that NMI method is better than Bilinear Interpolation and Nearest Neighbor Interpolation. From their experimental results, it is quite evident that PSNR of the presented NMI method is more than 35 db.

Jindal and Singh introduced the novel approach of data hiding using moderate bit substitution method [11]. They encrypt the original data using double encryption method such as flexible matrix and magic square method to provide multi layer of security to the hidden data. After encryption, they performed crypto data embedding into the original cover image with the help of moderate bit substitution method. In this paper, they concluded that double encryption provides more security to the hidden data and it is less prone to attack. They also apply T test for the validation of work.

Yalman et al. described the data hiding method based on R-weighted coding [12]. Their method consists of two steps. In the first step, they enlarge the input cover image using NMI method of interpolation to get the modified cover image. In the second step, they hide the secret data using R- weighted coding method into the modified cover image. They showed their experimental results are better in term of PSNR than Jung and Yoo's method [9].

Chan and Cheng presented the non reversible data hiding technique based on simple Least Significant Bit (LSB) substitution [13]. In this paper, they hide the secret data into the cover image using LSB data hiding method to get the stego image. Then, they apply the optimal pixel adjustment process on the stego image in order to improve the quality of the stego image and as well as reduce the computational complexity. They compared their results in term of image quality with other non reversible methods of data hiding.

Rani and Sharma introduced the crypto data hiding technique [14].They performed encryption on the original data to get crypto data with the help of RSA algorithm. Then, they performed data hiding and embed the crypto data into the cover image. At the receiver side, receiver extracts the encrypted data from the stego image and performs decryption by using private key of RSA algorithm.

Kahlon and Bhardwaj presented non reversible data hiding scheme based on Modified LSB. In this paper, the original cover image is converted from spatial domain to frequency domain using Discrete Cosine Transform (DCT) [15]. Then, data is embedded into the modified cover image using Modified LSB (MLSB) method. The presented method is applied on any image such as Gray scale, binary and RGB images. They compared their results in terms of PSNR and MSE with 4LSB method of data hiding.

Patel et al. described the data hiding method based on LSB and blowfish algorithm. Initially, they encrypt the original data using blowfish algorithm to provide security to the embedded data [16]. Then, hide this crypto data into the original cover image using simple LSB method. At the receiver end, receiver gets the stego image and extracts the encrypted data using LSB method and as well as decrypts the data using blowfish algorithm.

RESEARCH METHODOLOGY

In this method, Cryptography is combined with the steganography to provide high security and robustness. Proposed method consists of two steps. In the first step, original secret data is converted from plain text to cipher text using RSA algorithm. In the second step, encrypted data is embedded into the original cover image using proposed data hiding algorithm. The size of original cover image is 512 × 512 pixels. Whereas, receiver receives the stego image and extracts the encrypted data using data extraction algorithm. In order to get the original data, decryption is performed with the help RSA algorithm. The proposed method of crypto data hiding is shown in Figure 1.

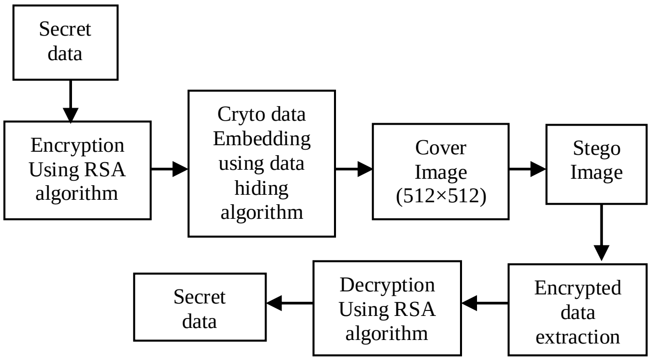

Secret data
Encryption Using RSA algorithm
Cryto data Embedding using data hiding algorithm
Cover Image (512×512)
Stego Image
Encrypted data extraction
Decryption Using RSA algorithm
Secret data

Figure1. Block diagram of the proposed data hiding method

RSA algorithm [14] is invented in 1977 by three scholars' such as Ron Rivest, Adi Shamir and Leonard Adleman. It is most popular algorithm of an asymmetric cryptography and as well as provides more security to the data because it requires factoring of very large two prime numbers. RSA algorithm uses two key pairs for data encryption and decryption. Secret data is encrypted using public key of RSA which is known to everyone and decryption of data is performed with the help private key. The size of public key and private key of RSA algorithm is usually 1024- 2048 bits long. Secure Socket Layer also uses the RSA algorithm for encryption. It consists of three steps as Generation of key pairs, Encryption and Decryption. All steps are given as below.

Step1: Select any two dissimilar large random prime number such that p and q where p ≠ q.

Step2: Calculate the value of n such as n = p × q.

Step3: Compute Eular's totient function such as: ϕ(n) = (p-1)× (q-1)

Step4: Choose an integer e such that 1<e< (n) for encryption.

Step5: Calculate d to satisfy the congruence relation d × e = 1 mod (n) for decryption.

Step6: The public key pair is (e, n) whereas (d, n) is private key pair.

Step7: Cipher text: C= P ^{e} mod n

Step8: Plain text: P= C ^{d} mod n

IV. PROPOSED CRYTO DATA HIDING ALGORITHM

In this algorithm, secret data is encrypted using RSA algorithm and then cover image is sub-divided into 1 × 4 non-overlapping blocks (Row wise). Finally, crypto data is embedded into the cover image using proposed data hiding algorithm. All steps of embedding algorithm are given as below and repeat all the steps until all the crypto bits are not embedded into the cover image.

Cover image C_O , Crypto data: C_d Stego image S

Step1: Perform separation on the cover image C_O into 1 × 4 non-over-lapping blocks (Row wise).

Step2: Calculate Absolute Difference (AD1 and AD2) value using equation (1)

$$AD1_{(i,1)} = |O_i(1,4) - O_i(1,3)| \; And \; AD2_{(i,2)} = |O_i(1,4) - O_i(1,2)| \quad (1)$$

Step3: Compute the number of embedding bits using (2) and (3) equations. Where $eb_{(i,1)}$ and $eb_{(i,2)}$represents the embedding bits. Upper limit and lower ranges of the designed range table are represented as $ul_{(i,1)}$and$lr_{(i,2)}$.

$$eb_{(i,1)} = log_2\left(ul_{(i,1)} - lr_{(i,1)} + 1\right) \quad (2)$$
$$eb_{(i,2)} = log_2\left(ul_{(i,2)} - lr_{(i,2)} + 1\right) \quad (3)$$

Step4: Compute two new differences(D1 & D2) using equation (4) and (5)

$$D1_{(i,1)} = \left|lr_{(i,1)} + Sb_{(i,1)}\right| \quad (4)$$
$$D2_{(i,2)} = \left|lr_{(i,2)} + Sb_{(i,2)}\right| \quad (5)$$

Such as, $Sb_{(i,1)}$ and $S_{b(i,2)}$ are the two integer values of number hiding crypto data bits

$eb_{(i,1)}$ and $eb_{(i,2)}$ correspondingly.

Step5: Compute the new pixel pairs of values using below equations

Let $L_{(i,1)} = \left|AD1_{(i,1)} - D1_{(i,1)}\right|$ and $L_{(i,2)} = \left|AD2_{(i,2)} - D2_{(i,2)}\right|$ are the new pairs of pixel are gained using these equations.

$$\left(O_i'(1,4), O_i'(1,3)\right) = \begin{cases} \left(O_i(1,4) - \left\lceil \frac{L_{(i,1)}}{2} \right\rceil, O_i(1,3) + \left\lfloor \frac{L_{(i,1)}}{2} \right\rfloor\right) for\ D1_{i,1} = 1\ (mod2) & (6) \\ \left(O_i(1,4) - \left\lceil \frac{k_{(i,1)}}{2} \right\rceil, O_i(1,3) + \left\lfloor \frac{k_{(i,1)}}{2} \right\rfloor\right) for\ D2_{i,1} = 0\ (mod2) & (7) \end{cases}$$

$$\left(O_i'(1,4), O_i'(1,2)\right) = \begin{cases} \left(O_i(1,4) - \left\lceil \frac{L_{(i,1)}}{2} \right\rceil, O(1,2) - \left\lfloor \frac{L_{(i,1)}}{2} \right\rfloor + L_{(i,2)}\right) for\ D1_{i,2} = 1\ (mod2) & (7) \\ \left(O_i(1,4) - \left\lfloor \frac{L_{(i,1)}}{2} \right\rfloor, O_i(1,2) - \left\lfloor \frac{L_{(i,1)}}{2} \right\rfloor + L_{(i,2)}\right) for\ D2_{i,2} = 0\ (mod2) & (8) \end{cases}$$

Step6: In order to provide the consistency to the hidden data adjust the $o_i^{'}(1,4)$ pixel for the both pairs.

Step7: Back to step 2 and replicate the same process until all the 1×4 non-overlapping (Row wise) sub blocks are not proceed and get the stego image S.

V. PROPOSED DATA EXTRACTION ALGORITHM

At the receiver side, receiver receives the stego image and extracts the crypto data using proposed data extraction algorithm. After the extraction of encrypted data, decryption is performed using private key of RSA algorithm in order to get the original data.

Stego Image S; Crypto Data E_s

Step1: Perform separation on the stego image S into 1 × 4 non-over-lapping blocks (Row wise).

Step2: Determine the Absolute Differences (AD1' and AD2') between the two pixel values using equation (9)

$$AD1'_{(i,1)} = |O_i(1,4) - O_i(1,3)| \; and \; AD2'_{(i,2)} = |O_i(1,4) - O_i(1,2)| \quad (9)$$

Step3: Extract the integer values, by using equation (10) and (11) which belongs to the encrypted data bit stream where lr represents the lower range of the range table.

$$Sb_{(i,1)} = \left|AD1'_{(i,1)} - lr_{(i,1)}\right| \quad (10)$$
$$Sb_{(i,2)} = \left|AD2'_{(i,2)} - lr_{(i,2)}\right| \quad (11)$$

Step4: Calculate the number of hiding crypto data bits by using equation (12) and (13) in order to translate $Sb_{(i,1)}$ and $Sb_{(i,2)}$ integer values into $eb_{(i,1)}$ and $eb_{(i,2)}$bit binary representation.

$$nb_{(i,1)} = log_2\left(ur_{(i,1)} - lr_{(i,1)} + 1\right) \quad (12)$$
$$nb_{(i,2)} = log_2\left(ur_{(i,2)} - lr_{(i,2)} + 1\right) \quad (13)$$

Step5: Combine all the extracted crypto data bits in order to obtain complete crypto data bit stream C_d .

Step6: Decryption of crypto data is performed with the help of RSA algorithm with a view to getting the original data.

VI. EXPERIMENTAL RESULTS

This section exhibits the experimental results and discussion of the proposed crypto data method. The four gray scale cover images (Lena, Airplane, Man and pepper) using standard images of size 512 × 512 are used in the experimental work are shown in Figure 2 (a), respectively. The proposed crypto data hiding scheme is implemented in MATLAB (2017a). The main objective of the proposed method is to attain the high security to the hidden data and to improve the quality of the stego image. The stego image obtained with the proposed crypto data hiding is depicted in Figure 2(b). From Figure 2, it is lucid that both the cover images and stego images obtained with the proposed method are looking like similar to each other.

Various Image Quality Measuring (IQM) parameters in terms of Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), Data Hiding capacity, Correlation and Structure Similarity Index Matching (SSIM) are used in order to measure the performance of the proposed method. PSNR is very critical parameter used to find the visual quality of image. PSNR more than 35 db is considered as good quality image. From the Table I, it is clear that Structure Similarity Index Matching (SSIM) of the cover and stego image is almost near to 1 because changes are small. The standard formulas for calculating the PSNR [17] and MSE [17] are given in equation (14) and (15).

$$\text{PSNR} = 10\log_{10}\left(\frac{255^2}{\text{MSE}}\right) \quad (14)$$

$$MSE = \frac{1}{512 \times 512}\sum_{i=1}^{512}\sum_{j=1}^{512}(C(i,j) - S(i,j))^2 \quad (15)$$

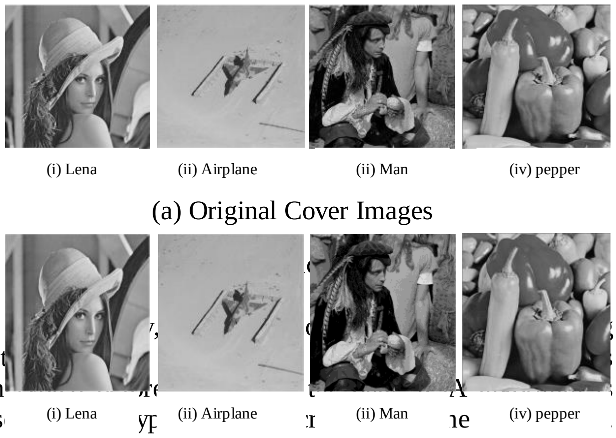
Where $C(i,j)$ and $S(i,j)$ are the pixels that are situated on the i^{th} row and j^{th} column of the original cover image C and stego image S. 512 × 512 pixels is the size of both cover and stego image. PSNR, MSE, Data hiding capacity, Correlation and SSIM using proposed method are summaries in Table I. Comparison of the proposed method with Jung et al.'s method [8] and Multi-Pixel Differencing (MPD) in term of Peak Signal to Noise Ratio (PSNR) using different images is shown in Table II.

Table I
Experimental results of the proposed method in term of Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), Data Hiding Capacity, Correlation, and Structure Similarity Index Matching (SSIM).

Image	PSNR	MSE	Data Hiding Capacity	Correlation	SSIM
Lena	39.64	7.05	279173	0.9985	0.9563
Airplane	44.26	2.43	199165	0.9975	0.9503
Man	37.72	10.97	324063	0.9983	0.9726
Pepper	40.61	5.64	284185	0.9990	0.9727

Table II
Comparison of the proposed algorithm with Jung et al.'s method and Multi-Pixel Differencing (MPD) in term of Peak Signal to Noise Ratio (PSNR) using different images.

Image	MPD Method	Jung et al.'s Method [8]	Proposed Method
Lena	36.92	35.95	39.64
Airplane	35.05	34.46	44.26
Man	33.73	33.11	37.72
Pepper	35.90	33.91	40.61



(a) Original Cover Images

(b) Stego Images obtained with proposed method

Figure 2 (a) Original Cover Images (b) Stego Images obtained with proposed method order to obtain the stego image. The embedded data is extracted correctly from the stego image. Original image is not required to extract the data. Experimental results show that the proposed crypto data hiding method gives high data hiding capacity and visual quality image as compared to other non reversible data hiding methods. The result of this work is quite promises.

VIII. References

[1] B. Jindal and A. P. Singh, "Concealing data in digital image with multilayer security," Multimed Tools Appl., Volume 75, Issue 12, pp.7045-7063, 2016.

[2] B. A. Forouzan, "Cryptography and Network Security," 3rd edition, McGraw-Higher Ed, India, 2016.

[3] W. Stallllings, "Cryptography and Network Security," 6th Ed., Pearson Education, India. 2013.

[4] A. Malik, and G. Sikka, "An image interpolation based reversible data hiding scheme using pixel value adjusting feature," Multimed Tools Appl.76 (11), pp.13025-13046, 2016.

[5] W. L. Tai and Y. F. Chang, "Separate Reversible Data Hiding in Encrypted Signals with Public Key Cryptography," MDPI, pp. 1-8.

[6] T. Shahana, "An Enhanced Security Technique for Steganography Using DCT & RSA, International Journal of Advance Research in Computer Science & Software Engineering," Volume 3, Issue 7, pp. 943-949, 2013.

[7] Y. T Chang, C.T. Huang, C.F. Lee and S. J. Wang, "Image Interpolation based data hiding in conjunction with pixel-shifting of histogram," J Supercomput 66, pp.1093-1110, 2013.

[8] K. H. Jung, K. J. Ha and K. Y. Yoo, "Image data hiding method based on MPD and LSB Substitution Methods," IEEE, International Conference on Convergence and Hybrid Information Technology, pp. 355-358, 2008.

[9] A. Malik, G. Sikka, and H. K. Verma, "Image interpolation based high capacity reversible data hiding scheme," Journal of Multimed Tools Appl. 76(22), pp. 24107-24123, 2016.

[10] K. H. Jung and K.Y. Yoo, "Data hiding method using image interpolation," Computer Standards and Interface 31(2), pp. 465 – 470, 2009.

[11] Jindal and A. P. Singh, "Image steganography with multilayer security using moderate bit substitution," Applied Science 14(8), ISSN 1812-5654, pp. 738-747, 2014.

[12] Y. Yalman, I. Erturk, and F. Akar, "An image interpolation based reversible data hiding method using R-Weighted coding," IEEE International Conference on Computational Science and Engineering, pp. 346-350, 2013.

[13] C. K. Chan and L. M. Cheng, "Hiding data in image by simple LSB substitution," Pattern Recognition 37(3), pp. 469-474, 2004.

[14] P. Rani, and P. Sharma, "Cryptography using image steganography," International Journals of Computer Science and Mobile Computing (IJCSMC), Volume 5, Issue 7, pp. 451-456, 2016.

[15] R. Kahlon and Bhardwaj, "Secure image steganography using bit shift encryption and MLSB approach," International Journal of Science and Research (IJSR), Volume 5, Issue 7, pp. 408-412, 2016.

[16] K. Patel, S. Utareja and H. Gupta, "Information Hiding using Least Significant Bit Steganography and blowfish algorithm," International Journal of Computer applications, Volume 63, pp. 24-28, 2013.

[17] R. C. Gonzalez and R. E. Woods, "Digital Image Processing," 3rd edition, Pearson Education, India. 2016.

[18] C.F. Lee and H. L. Chen, "A novel data hiding scheme based on modulus function," J Syst Softw 83, pp. 832- 843, 2010.

[19] S. L Li, K. C. Leung, L. M. Cheng, and C. K. Chan, "A novel image-hiding scheme based on block difference," Pattern Recognition 39, pp. 1168-1176, 2005.

[20] A. Cheddad, J. Condell, K. Curran and P. Kevitt, "Digital image Steganography: Survey and analyses of current methods," Signal Processing 90: pp.727-752, 2010.

[21] A. Malik, G. Sikka and H. K. Verma, "A modified Pixel-Value differencing image steganographic scheme with least significant bit substitution method," I. J. Image, Graphics and Signal Processing, pp. 68-74, 2015.

[22] C. H. Yang, C. Y. Weng, S. J. Wang, and H. M. Sun, "Adaptive data hiding in edge areas of images with spatial LSB Domain Systems," Transaction on Information Forensics and Security, Volume 3, pp. 488-497, 2008.