International Journal of Research in Engineering and Applied Sciences(IJREAS)
Available online at http://euroasiapub.org/journals.php
Vol. 7 Issue 5, May-2017, pp. 208~217
ISSN (O): 2249-3905, ISSN(P): 2349-6525 | Impact Factor: 7.196 | Thomson Reuters Researcher ID: L-5236-2015

Self-embedding Steganography method using LSB replacement and XOR encryption

Er Rupinderjeet Singh[1]
Computer Engineering
ASRA College of Engg. And Tech.
Bhawanigarh, Punjab

Er.Inderjeet Singh[2]
Computer Engineering
ASRA College of Engg. And Tech.
Bhawanigarh, Punjab

Abstract
Development in internet and information sharing on it increases demand to keep the owner's rights from any manipulations or plagiarism. Instead of this, for some confidential data such as proof (in terms of video/images) needs content to be kept hide from public or to prevent it from leakages to the public. Hence need to provide the security and protection to these information'susing cryptography, steganography, or watermarking methods. Cryptography, steganography, and watermarking have similar application. Secret Messages are hidden is the main task of this work, send to other users and the receiver would be capable to know the secret message. As for cryptography, this method will transform the secret message into encrypted form to secure the transmission, and then use a 'key' to decrypt the message. The security has been providing by the method of encryption and decryption, but the contents have not been protected. On the other hand, steganography is to embed secret information perfectly secured with no visible change in the cover object. In this work, both cryptography and steganography has been merge in cover image by converting it into non-overlapping blocks hence results in more security for hidden message. XOR cryptography method has been used for encryption and decryption whereas two bit LSB placement based on maximum entropy blocks has been used for embedding. For selecting the secret information, Self-embedding approach has being used in which only MSB bits has been chosen hence cause with more region to be embedded. Algorithm is able to embed maximum of 50% region of the cover image MSB bits.

Keywords*: cryptography, steganography, LSB, blocks, XOR,*

1.1 Overview

The technique of hiding secret data in the cover image while hiding own existence is referred to as steganography. In other words, it involves hiding the information as if there is no hidden information at all. Text, audio, images, video etc. can be the secret information. In steganography, secret information needs to be converting into binary form. Later, it is inserted into the covering file which may be audio or image file. This output image is called as stego-image. If the output is an image file, then the technology is called as image steganography. Cryptography deals with constructing, the protocols named as analyzing protocols has been prevent the third party from reading secret information. When cryptography with steganography is combined, the output will in powerful process which allows the users to transfer the sensitive information over the geographical securely [1]. Any unauthorized user can just only view the stego image but only authorized users can extract the secret information.

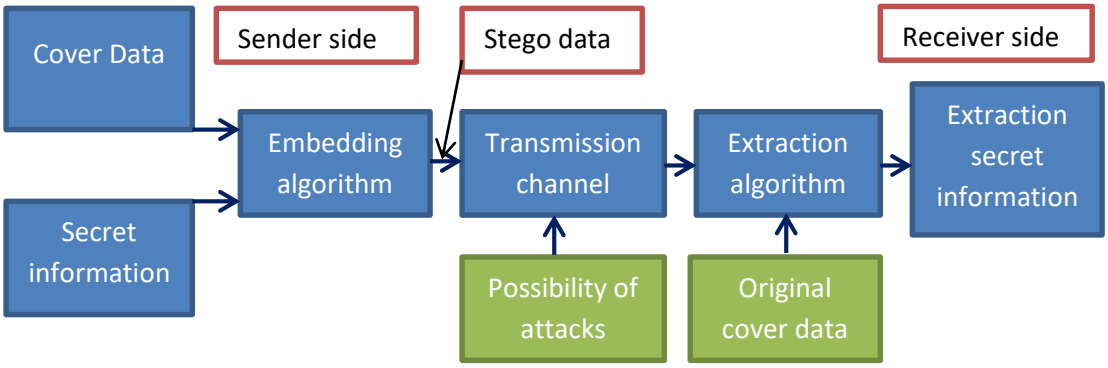

Figure 1: General model of a steganography system[2]

Note that Green boxes are not necessary in above block diagram [2].

The LSB is a widely used steganography algorithm that is based on converting characters of the secret text message into a string of binary bits [3]. The original algorithm needs to be used a gray-scale cover image, this is done by embedding the 3 or more than 3 bits from the secret text message into the least 3 significant bits of the cover image pixels. This algorithm was adapted to work on color images by using the three color channels. The eight bits are further categorized into two categories of MSB and LSB bits in which two LSB bits are used for embedding.Another adaptation of the LSB has to use it just on a crop from the cover picture. It depends on separating a crop from the cover picture and after that embedding the secret text message into this crop by using the LSB approach. The stego picture is gotten by reassembling the picture and the stego crop. The crop arranges must be known to the receiver to have the capacity to separate the message [3] Fig. 1 provides a general view of various stages existed in general steganography system.

choice to the user which portion one needs to sanitize has been proposed. The core difference between self-embedding techniques and the self-sanitization system, however, is the goals of the two technologies and how they are used. To authenticate images self-embedding techniques had been created [5] where the self-sanitization system was developed to remove information from unauthorized view. Additionally, self-embedding techniques need to be used to retrieve broken image data, whereas the self-sanitization system needs to be used to hide and restore intentionally removed information. One more feature of typical steganographic schemes is that they needs to be used the share secret key or password between the receiver and the sender. This shared key is needs to be used to run a pseudorandom number generation algorithm for defining the sequence of pixels needs to be used for embedding.Though, if there is a distance between the communicating parties,

1.2 Motivation

Most of the steganography algorithms had not been consider the image content whereas locating the message bearing pixels. Thus, in most cases, they are bound to defeat against visual and statistical attacks. In this work, the image content has been evaluated to identify suitable locations to keep the message hide, without compromising capacity or security. This has been done by categorizing the image into non-overlapping sections and then by selecting the blocks having maximum entropy. In this, self-sanitization for embedding has been also included as the message that is hidden has been used from the cover image and then MSB bits of hidden portion are used for embedding. High capacity embedding algorithm in which hidden portion can be selected manually by a user as it gives the

sharing the key turns into extra overhead, needs to be executing the key exchange/distribution protocols & thus extending cost in terms of bandwidth and time. So, this is a keyless scheme that is design to keep off this additional overhead. In any case, in the meantime, one must guarantee that absence of the key should not render the plan uncertain. In this work, the main focus is to appear this objective.

1.3 Existed work in LSB based steganography

Seethalakshmi et. al. [1] used neural networks to recognize the best locations with high energy coefficients where secret data embedding is done. AES encryption algorithm needs to be used to encode the secret information. By dividing cover image onto blocks, the energy co-efficient for each block are identified using IWT .The high energy coefficients in the cover image has been used to embed the secret information are identified using RBF function in neural networks. Then LSB embedding technique has been used to embed the secret information in the high energy positions of the cover image.In order to negate the effects of IWT, on the stego image, Inverse IWT has been applied. Later stego image is brought back to the original shape using data re-arrangement process.

Turán et. al. [2] presented an algorithm for image steganography, which uses principles of LSB steganography and Mojette transform. Method has high PSNR but also increases the computational difficulty. This is caused by processing of image with secret information as one block and the quantity of needed iterations rising with the resolution of the image.

Faragallah et. al. [3] proposed an approach based on cropping the cover image into a predefined number of crops with certain secret coordinate). The secret text message is categorized into sections with the same cover image crops. Every secret text message part is installed into a picture crop by a secret succession by using the LSB approach. Embedding is done in shading channels by the arrangement, 3 bits in the blue color channel, three bits in the green shading channel, and two bits in the blue color channel. Finally, the stego crops are assembled to get the stego image. However they need to keep the co-ordinates of crops in their method.

Kemouche et. al. [4] developed the basic LSB technique that allows hiding information in JPEG images by using the least significant bits of pixels. They added a metaheuristic approach to LSB technique and hybridized local search (LS) with LSB. LSB has been improved by combining it with a stochastic local search SLS. In their proposed methods: LSB, LSB + LS and LSB+ SLS, they decomposed both the secret message and the image in 4 bits blocks. However, by applying the guideline of every strategy embedded the private message in the image.

Pathak et. al. [6] presents another LSB based steganography. It utilizes an LSB method for image steganography. To hide the MSB bits of every pixel of information picture in the LSB bits of every pixel of cover picture 3-sets of PN groupings are produced. These PN sequences are generated using a key of length of 192-bits to secure the message. Then, before the transmission of image GCD transform has been used.It localizes the damaged area done during transmission. Here, 4-LSB bits, replacement of each pixels of the cover image is done by 4- MSB bits of every pixel of data image.

Islam et. al. [7] proposed method in order to make it difficult to the unauthorized person to determine the existence of a secret cipher, but did not emphasis to raise the capability of the message. In ordinary LSB Steganography technique only message bit will be replaced with the LSB bit of the picture but the message bit has not been change in this algorithm but it would replace the status of the message bit. They also merge Cryptography with it so that the secret message can be secured by two security layers.

Davidson et. al. [8] propose multi-bit steganography in the high energetic pixels using appropriately defined energy functions. Since the location and intensity of these pixels differ from image to image, it doesn't impart a constant signature of change. Algorithms keep no signature in the stego images though the embedding capacities are very high as well as the embedding efficiencies. They have considered steganography by utilizing active pixels in spatial domain only. However, scheme is flexible and can be applied to other transform domain (DCT, DWT, etc.) as well as other cover media (e.g., video, audio, etc.).

Wang et. al. [9] proposed two visually impaired LSB steganography algorithms as quantum circuits are proposed in view of the novel enhanced quantum representation (NEQR) for quantum pictures. One algorithm is plain LSB which utilizes the message bits to additional for the pixels' LSB directly. The other is blocking LSB which installs a message bit into various pixels that have a place with one image block.

Chakraborty et. al. [10] Proposed a method to embed the secret message based on region selector. Edge predictor has been used to compute the edge image from the cover image. The method involves following phases.First, Region selector divides the edge image into non-overlapping Z × Z blocks then the predicted error greater than a particular threshold, are selected from each block for capacity estimation. Capacity of each block is measured by computing the total bits that should embedded into a particular block. In each block for a specific prescient error one, a few bits of the secret message can be embedded into the comparing grayscale of the first cover depending on the threshold. Capacity is calculated by adding the bits that can be embedded in a particular grayscale of a block.If the capability of the block is not sufficient to fulfill the secret data region selector re-processes the region for embedding. There are further information required for extraction of the secret data like block size (Z) and threshold (Tk) which are embedded in those regions which are not used for data embedding.

Nguyen et. al. [11] presented the MPBDH (multi bit-planes image steganography using block data-hiding) that obtains a large amount of embedding capacity while maintaining appreciable visual quality. In the proposed approach, more than one bit-plane of the block of pixels needs to be used to hide secret bits.As a result, the capacity is higher than that of the existing block complexity based data hiding approaches. Moreover, retaining the BDH, in which the necessary number of embedding changes is minimized in comparison with other methods, causes the distortions by the data hiding process to be reduced.Additionally, by selecting a high texture characteristic block of pixels in which to embed the given secret message, even at the high embedding rates, the smooth districts are kept the same as in the cover picture. This leads to a reduction in the possibility of being detected by visual attack methods.

Gowda et. al. [12] proposed an algorithm which uses two most popular cryptographic algorithms and combines them with an innovative advancement of the most used steganographic technique to develop a protected and effective algorithm. The algorithm provides 3 layers of security by first encrypting the data using AES encryption scheme. Then encrypting the key has been used for the encryption using RSA. Then further increasing the chaos factor by the random nature in which the images are sent. The three layers increase the time for sending the data; however the time needed to decrypt the information increases exponentially.

Sirisha et. al. [13] presents an method for LSB focused around image steganography .It upgrades the current Least Significant Bit (LSB) substitution systems to improve the security level of concealed information. In this work covered information is put away into distinctive position of Least Significant Bit of picture using block division method depending upon the secret key. Hence it is complex to

concentrate the concealed data knowing the recovery systems.

Dai et. al.[14] presents a general adaptive image steganographic scheme that is based on the selection of pixel, which can be integrated with majority texture definition and distortion profile. Based on linear texture complexity definition of image block, texture regions have been selected as the embedding area with the threshold. There exists a modification pattern which makes each selected image block still satisfies the selection criteria after modification, that ensures the achievement of information extraction. Then, with the modified distortion profile definition of HUGO algorithm, STCs has employed to embed secret message bits in the selected pixels. By retrieval the embedding regions, the receiver can separate the message.

Nilchi et. al. [15] used a combination of both of the MP and LSB algorithms. The MP method has been hidden the data in the 4th to 7th bit layers of the pixels of the blue layer of "Cover-Image", and the LSB method embeds the "Message" in the LSB of pixels. They used both algorithms concurrently because these two algorithms have no overlap in the bit layers that they need to be used during the embedding phase. Therefore, in this steganography system, 7 bit layers of every pixel are needs to be used for hiding information, and only the MSB bit of every pixel is not used in the embedding phase. The MP method can only hide "Message" in the form of text, while the 3-LSB method is suitable for hiding all kinds of digital media; therefore, this work has two entrances for the "Message". Among all, one is for text, and the other one is for other kinds of digital media.

1.4 Proposed work

As hidden message, the cover image has been used to select the region need to be embedded. This has been chosen for sanitization scenarios i.e. a classified image, needed in court appearances in which some content needed to be kept in hidden form as to prevent leakage to the public. However method can be adopted for external hidden data as well. At first an area has been cropped for embedding as secret message which has been localized by cropping tool. As MSB (most significant bits) contain the visual content, hence these are separated from LSB (Least significant bits) hence helps in more region to embed in the same image. The embedding has been done in LSB bits of the cover image, therefore the remaining LSB bits can be used for embedding purposes, hence deduction of secret MSB does not cause decrease in embedding capacity. After extraction of secret message, XOR encryption has been applied to the secret message to ensure security of the message. This has been used by creating random bits of same size as that of secret message and then XOR operation has been applied to one-to-one basis. Embedding has been done by dividing the cover image into non-overlapping blocks of size Z*Z and entropy has been evaluated for all the blocks. The reason behind this is to select the blocks on some unique basis, therefore only MSB bits are used for entropy calculation as there is no change in these bits after embedding. This helps in inverse extraction process of the secret data. As there is no need of secret key to generate however some overhead about the number of bits embedded and cropping region has been embedded along with the secret message as it needs to complete the extracted image by combining MSB and LSB of the cropped area. The steps in brief for embedding and extraction has been written below

1.4.1 Embedding process

1.) Resizing and cropping the ROI needed as secret message to embed
2.) Separation of MSB and concatenation of bits in one dimensional array.
3.) Generation of extrainformation i.e. coordinates of cropping region with secret message, area of secret message (i.e. no. of MSB bits).
4.) Encryption of secret data by using XOR encryption

5.) Dividing image by 64*64 non-overlapping blocks
6.) Evaluation of entropy of each block and sort the blocks according to maximum entropy.
7.) Selection of a block in order of entropy and Embedding process by selecting two bits per pixel by placing them in two LSB's.(In this first, extra information has been embedded and later the secret message).
8.) Recombine the image and mark it as stego image

1.4.2 Extraction process

1.) Divide stego image into 64*64 non-overlapping blocks
2.) Calculate entropy of blocks by using only MSB's
3.) Sorting the blocks according to entropy in descend manner
4.) Extraction of first 2 LSB bits in order to extract information
5.) Based on extra information run the extraction process unless bits extracted is equal to length of secret bits.
6.) Decrypt the extracted bits using XOR operation.
7.) Reassembling according to coordinates from extra information
8.) Evaluate performance in terms of accuracy of detected data.

1.5 Results

For experimental results, stego images are analyzed using LSB enhancement technique to determine the level of un-detectability of the hidden information[16]. Steganalysis is the practice or art of breaking a steganography algorithm by attempting to detect hidden information [16]. For evaluating quality of steg0 image, PSNR (peak signal to noise ratio) and MSE (mean squared error) indexes has been provided at different payload capacity.

- **LSB enhancement**

LSB enhancement is a visual analysis technique, which means that the image is modified and then requires a human to look at the modified image to try and detect a pattern [16]. LSB enhancement processes an image by extracting the least significant bit of each pixel (can also be more than one bit per pixel, depending on colour depth) [16]. To display the resulting image, each pixel in represented entirely by the least significant bit by setting the value of each pixel to the maximum if the least significant bit is 1 or 0 if the bit is 0. Once the image is in this state the steganalyst can visually study the image for anomalies or patterns. The successful detection of information through LSB enhancement decreases with an increase in perceived randomness of the hidden information [17]. In the self-sanitization system the hidden sanitized part of the image was spread out evenly over the remaining pixels, thus smaller payloads increased the perceived randomness of the hidden information since affected pixels are spaced further away from one another. The success of detecting information in the self-sanitization system using LSB enhancement is thus dependant on the amount of information that is hidden. An output image (see fig. 2) after LSB enhancement on stego image has been given below.

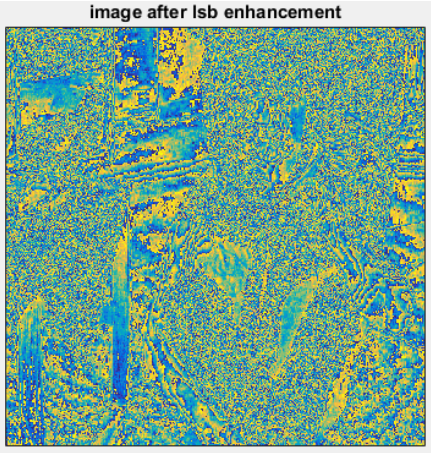

Figure 2: Visual inspection using LSB enhancement

As seen in above image, one cannot judge the changes happened in the image after LSB enhancement method.

- **PSNR and MSE**

Peak Signal to noise ratio (PSNR)

This parameter provides the quality of image in terms of powers of the original and stego images.

$$PSNR = 10log_{10}\frac{(2^n-1)^n}{MSE} = 10log_{10}\left(\frac{255^2}{MSE}\right) \quad (1)$$

Here MSE is mean square error value and n is number of bits i.e. 8 for uint8 image.

Mean square error (MSE)

This parameter quantifies the amount of modifications between the original and stego image.

$$MSE = \frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}|(f_{x,y} - g_{x,y})|^2 \quad (2)$$

Wherethe pixel of original image is$f_{x,y}$, and $g_{x,y}$ is the stego image pixel and M and N are rows and columns in the image. For RGB images, psnr and mse values has been evaluated using individual channels however matlab functions “immse” and “psnr” gives values for whole image.

- **Payload**

The payload of an image relates to embedding intensity. As only MSB bits have been chosen for embedding, payload percentage has been selected depending upon MSB bits in the image. Formula for calculating payload percentage has been written in eq(3)

Payload (%)=(MSB bits embedded/ Total MSB bits in the image)*100…..(3)

The results in visual output has been shown below at different stages of the algorithm

Figure 3: Cropping window

Fig. 3 shows square box used for cropping the region needed as secret image. In this work, square window has been used but rectangular sizes can be chosen.

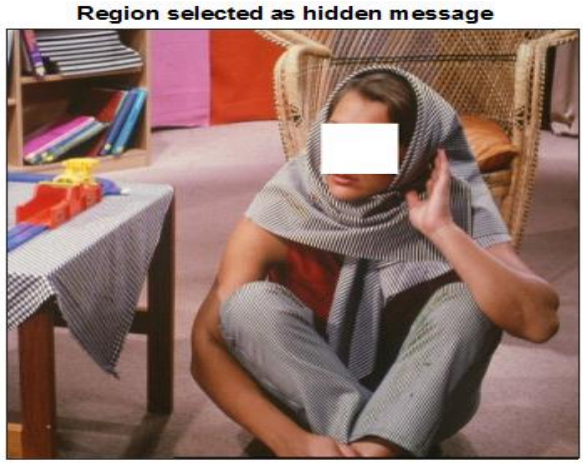

Figure 4:White square as MSB selected for embedding

Fig. 4 shows white region from which MSB bits need to be extracted or sanitized area in the image.

Figure 5:XOR encryption of secret information to be embedded.

Fig.5 shows MSB bits after encryption using XOR operation. Random bits has been generated by a secret key in which an integer or message can be used to get the initial points for generating random numbers as same secret message can be used in extraction process.

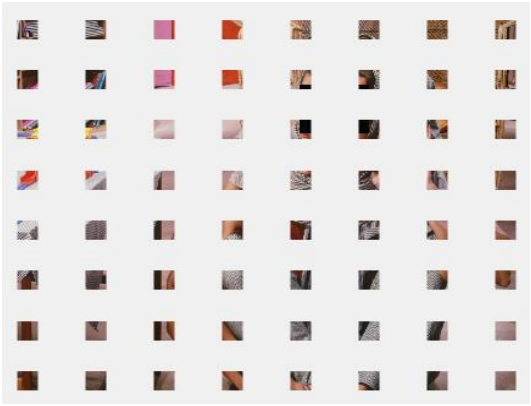

Figure 6: Non-overlapping blocks of size 64*64

Fig.6 shows the block making process in which 512*512*3 image has been divided into 64*64*3 non-overlapping blocks. Smaller sizes can be used for block making as it provides more scrambling to embedded regions.

Figure 7:Output stego image

Fig.7 shows the stego image produced after embedding the secret data in the image. Here black portion shows the pixel that has been used for embedding purposes and only LSB bits are present at these locations.

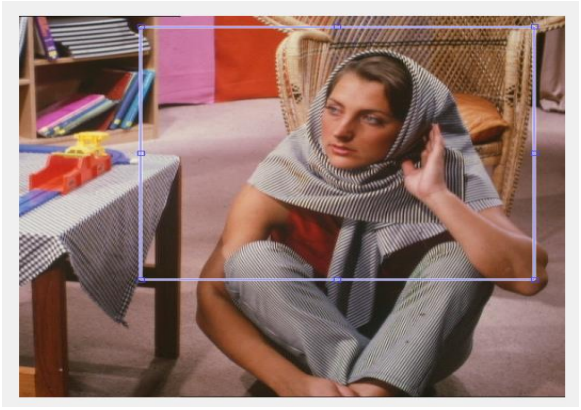

Figure 8: Cropping window with payload 47.9889 % of total MSB bits in the image

Fig. 8 shows a patch with size 47.99 % of total MSB bits. Algorithm can use maximum of 50% payload as two bits are altered among four LSB bits. Below is a table showing PSNR and MSE quality indices which can analyze clearly using bar graphs.

Table 1: MSE and PSNR indexes at different payloads

MSE	PSNR (DB)	Payload %
0.5650	50.6100	1.89360
1.0584	47.8842	3.08950
0.3063	53.2700	6.09970
0.4104	51.9988	8.18480
0.6074	50.2961	12.0804
0.7471	49.3973	14.9364
1.1224	47.6293	22.4319
1.4980	46.3758	29.9038
2.4046	44.3203	47.9889

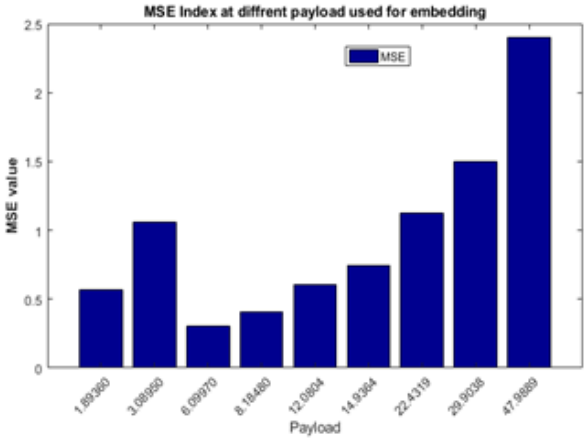

Figure 9:Bar graph showing MSE index at different payload

Fig.9 shows the bar graph for MSE parameter. As seen above the MSE values increases along with increase in payload. However at first two payloads, there is a high value of MSE index. The reason behind this is the reason to be selected and the block chosen for embedding as high entropy reason i.e. face region has been selected in first two patches.

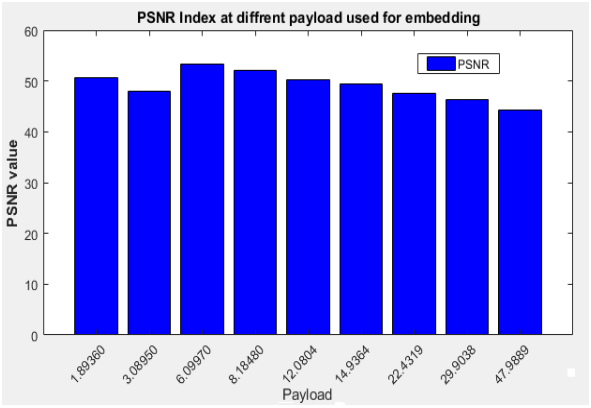

Figure 10: Bar graph showing PSNR index at different payload

Fig. 10 shows PSNR values. It has been found that there is not much difference in PSNR, MSE indexes as bits to be altered can found similar values in many pixels. However slight decrease has been found with the increase in payload.

1.6 Conclusion

The proposed methods used self-embedding technique in which an MSB patch of pixels can be selected as secret information. As MSB contains the most visual content it is enough for self –sanitization applications hence caused the embedding capacity increased to almost double as compared to whole bit embedding. In this work, two LSB bits has been replaced as these does not affect in large changes while visual examinations. To secure the content, XOR encryption has been applied to the secret content. For embedding first image is divided into non-overlapping blocks and then blocks are selected with maximum entropy first basis. This provides more security as random blocks are chosen from all over image content. Steganalysis has been carried out using LSB enhancement technique and there is no detection of secret embedded pixels in the stego image. High PSNR at all payload shows that there are not much alterations after embedding the secret information when compare the original image pixels and stego image pixels.

References:

[1] K. S. Seethalakshmi, Usha B A and Sangeetha K N, "Security enhancement in image steganography using neural networks and visual cryptography," 2016 International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS), Bangalore, 2016, pp. 396-403.

[2] J. Oravec, J. Turán and Ľ. Ovseník, "LSB steganography with usage of Mojette Transform for secret image scrambling," 2016 International Conference on Systems, Signals and Image Processing (IWSSIP), Bratislava, 2016, pp. 1-4.

[3] K. A. Al-Afandy, O. S. Faragallah, A. Elmhalawy, E. S. M. El-Rabaie and G. M. El-Banby, "High security data hiding using image cropping and LSB least significant bit steganography," 2016 4th IEEE International Colloquium on Information Science and Technology (CiSt), Tangier, 2016, pp. 400-404.

[4] D. Boughaci, A. Kemouche and H. Lachibi, "Stochastic local search combined with LSB technique for image steganography," 2016 13th Learning and Technology Conference (L&T), Jeddah, 2016, pp. 1-9.

[5] C. Rey and J.L Dugelay, "A survey of watermarking algorithms for image authentication", EURASIP Journal on Applied Signal Processing, vol 6 pp. 613-621, 2002

[6] R. K. Pathak and S. Meena, "LSB based image steganography using PN sequence & GCD transform," 2015 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Madurai, 2015, pp. 1-5.

[7] M. R. Islam, A. Siddiqa, Md. Palash Uddin, A. K. Mandal and M. D. Hossain, "An efficient filtering based approach improving LSB image steganography using status bit along with AES cryptography," 2014 International Conference on Informatics, Electronics & Vision (ICIEV), Dhaka, 2014, pp. 1-6.

[8] Goutam Paul, Ian Davidson, Imon Mukherjee, S. S. Ravi, "Keyless dynamic optimal multi-bit image steganography using energetic pixels" Published in: Multimedia Tools and Applications March 2017, Volume 76, Issue 5, pp 7445–7471

[9] Nan Jiang, Na Zhao, Luo Wang, "LSB Based Quantum Image Steganography Algorithm" Published in: International Journal of Theoretical Physics January 2016, Volume 55, Issue 1, pp 107–123

[10] Soumendu Chakraborty, Anand Singh Jalal, Charul Bhatnagar , "LSB based non blind predictive edge adaptive image steganography" Published in: Multimedia Tools and Applications March 2017, Volume 76, Issue 6, pp 7973–7987

[11] Tuan Duc Nguyen, Somjit Arch-int, Ngamnij Arch, "An adaptive multi bit-plane image steganography using block data-hiding" Published in:Multimedia Tools and Applications July 2016, Volume 75, Issue 14, pp 8319–8345

[12] S. N. Gowda, "Advanced dual layered encryption for block based approach to image steganography," 2016 International Conference on Computing, Analytics and Security Trends (CAST), Pune, India, 2016, pp. 250-254.

[13] M. Tulasidasu, B. L. Sirisha and K. R. Reddy, "Steganography Based Secret Image Sharing Using Block Division Technique," 2015 International Conference on Computational Intelligence and Communication Networks (CICN), Jabalpur, 2015, pp. 1173-1176.

[14] Qingqing Shen, Guangjie Liu, Weiwei Liu and Yuewei Dai, "Adaptive image steganography based on pixel selection," 2015 IEEE International Conference on Progress in Informatics and Computing (PIC), Nanjing, 2015, pp. 623-627

[15] A. Nilizadeh and A. R. N. Nilchi, "A novel steganography method based on matrix pattern and LSB algorithms in RGB images,"

2016 1st Conference on Swarm Intelligence and Evolutionary Computation (CSIEC), Bam, 2016, pp. 154-159

[16] T. Morkel, "Self-sanitization of digital images using steganography," *2015 Information Security for South Africa (ISSA)*, Johannesburg, 2015, pp. 1-6

[17] H.G Schaathun; P. Bateman "Image steganography and steganalysis"Department of Computing, Faculty of Engineering and Physical Sciences, University of Surrey, 2008