A Secure Steganographic Method Using Modified LSB (Least Significant Bit) Substitution

Suman, Dr. Sukhjeet Kaur Ranade

***Abstract*— In this paper a technique for hiding secret data into color images and grey images using [distance, in 4/8 neighbors, pixel wise] a secure steganographic method using modified LSB(Least Significant Bit) substitution. it ensure the quality of the image is not shattered. The work uses a set of few parameters like threshold value, lower limits, and upper limit values to decide the hiding blocks, and ensure that the extraction algorithm can read those particular blocks and fetch the required message. It is based purely on steganography without encryption. The additional ordering of Red, Green and Blue components in color images for the extraction data acts as key for the extraction algorithm.**

***Index Terms*— Steganography, Cover image, Stego-image, Modified LSB substitution , Error blocks,**

I. Introduction

Internet is the on the top of the demands of people in today’s era. It is the major source of sharing files, resources etc. Therefore, Internet Security is the main issue to provide security and authorization to the users and data. Encryption has been widely used for the safety of data that converts the plain text to cipher text using some encryption algorithms. However, it makes the text or message indecipherable but it makes the message suspicious as well. Encryption is not a very reliable method to secure data, as there are many algorithms to hack the cipher text. Any expert hacker can simply decode the cipher text by hit and trail method. The alternative to this method is Steganography, which provides a secure method to hide data. It do not attract the attention of any hacker and provide security. Steganography is way to conceal the secret message in some medium like audio image or video. The image, which embeds the secret message in it, is a cover image. After the embedding of secret message, Image formed is the stego image. The well-known approach of steganography technique is LSB substitution. It embeds the secret message by replacing n LSBs of the picture element with n bits of secret message. Then based on the LSB substitution technique, a genetic algorithm of optimal LSB substitution is now also available to improve the stego-image security of the simple LSB method.

II. Literature Survey

Wu and Tsai [1] the work in this paper shows that Secret data can be embedded in cover object. It is done by replacing the similar two – pixel blocks of cover object and the original text. This method is also useful for hiding small as well as large amount of data in the cover objects. It provides high security without imperceptions and it is easy to use. It is known as the best way to provide security.

Wu et al. [2] in this paper, to improve the capacity of hidden data two techniques known as LSB substitution and pixel-value differencing are combined with each other. It provides an imperceptible stego-image quality. The working of the combination of these two techniques is that firstly, by analysing the two consecutive pixels, a different value is obtained by using the PVD method. The smooth area is used to get a small difference value and the large one is located on an edged area. In the smooth areas, the secret data is hidden into the cover image by LSB method while using the PVD method in the edged areas. The combination of LSB or PVD method provide a great range of the variable, hence it is hard to guess the data hidden by using these techniques. The security level is the same as that of a single using the PVD method of the proposed method. The results of this method were compared with alone PVD method, and it shows that the combination provides better results than this alone method and it can hide a much larger data and maintains a good visual quality of stego-image.

Jung and Young [3] A new data hiding method based on the least significant bit (LSB) substitution and the multi-pixel differencing (MPD) method is presented on the proposed method to improve the capacity of hidden secret data and to provide an unperceivable visual quality. First, a sum of different values for a four-pixel sub-block is calculated. The low value of the sum is on the smooth block and the high value is on an edged block. The secret data are hidden into the cover image by the LSB method in the smooth block, while the MPD method is concealed in the edged block. The experimental results show that the proposed method has a higher capacity and maintains good visual quality.

Manuscript received Aug, 2017.

***Suman**, Department of Computer Science, Punjabi University Patiala, India.*

***Dr. Sukhjeet Kaur Ranade**,* Associate Professor, *Department of Computer Science, Punjabi University Patiala, India.*

Young et al. [4] a new data hiding method based on the least significant bit (LSB) substitution and the multi-pixel differencing (MPD) method is presented on the proposed method to improve the capacity of hidden secret data and to provide an unperceivable visual quality. First, a sum of different values for a four-pixel sub-block is calculated. The low value of the sum is on the smooth block and the high value is on an edged block. The secret data are hidden into the cover image by the LSB method in the smooth block, while the MPD method is concealed in the edged block. The experimental results show that the proposed method has a higher capacity and maintains good visual quality.

Wang et al. [5] have proposed a novel hiding data scheme with distortion tolerance. The proposed scheme not only can prevent the quality of the processed image from being seriously degraded, but also can simultaneously achieve distortion tolerance. They show that the proposed scheme indeed can obtain a good image quality and is superior to the other schemes in terms of its distortion tolerance.

Zhang et al. [6] this paper is based on four-pixel differencing and modified least significant bit (LSB) substitution, used to improve the embedding capacity and provide an imperceptible visual quality. The common difference value of a four-pixel block is exploited to classify the block as a smooth area. By the k-bit modified LSB substitution method is used to hide the secret data into each pixel and we can readjust the work to manage the perceptual distortion. This will provide a suitable image quality as well as a wide embedding capacity. But this method does not give a stronger security.

Gutte et al. [7] the secret communication system has two layered security levels. First level is through encryption of the text using Extended substitution algorithm and second one is through embedding the encrypted text into LSBs variably. The verification of both the Steganography schemes along with Extended Substitution Algorithm has been done and it is clear from the experimentation that inserting the data at three LSB positions does not change image parameters like PSNR, Mean, Standard deviation, Entropy in much extent. Therefore, it retains the image quality similar to two LSB scheme. It can be used to secure all type of data like alphabets (small as well as capital), special characters and mathematical symbols. The variable *y* takes values as 0, 1, 2, 3. Embedding the cipher at LSBs is decided by variable *y*. As the LSB in each pixel are not same but decided according to variable value, it is stronger approach and helps in minimizing the error.

Juneja and Sandhu [8] this paper defines an approach for Information Security in RGB Color Images using a Hybrid Feature detection technique; Two Component based Least Significant Bit (LSB) Substitution Technique and Adaptive LSB substitution technique for data hiding. Advanced Encryption Standard (AES) is used to provide Two Tier Security; Random Pixel Embedding imparts resistant to attacks and Hybrid Filtering makes it immune to various disturbances like noise. An image is combination of edge and smooth areas, which gives a good opportunity to hide information in it. It implements the idea that edge areas being high in contrast, color, density and frequency can tolerate more changes in their pixel values than smooth areas, so we can embed with a large number of secret data while retaining the original characteristics of image. The proposed approach achieved Improved Imperceptibility, Capacity than the various existing techniques along with Better Resistance to various Steganalysis attacks like Histogram Analysis, Chi-Square and RS Analysis as proven experimentally.

Bhardwaja and Khanna [9] have offered two levels of security through a process of two steps, rather than hidden the message bits directly in cover image, they were twisted in a random regulates and generated by 2D Arnold Cat Map after that encrypted message is hidden behind a cover image using basic LSB method. MSE (Mean Square Error) and PSNR (Peak Signal to Noise Ratio) are two common quality measurements to measure the difference between the cover-image and the stego image. Results showed that the projected method gave better results than simple LSB with higher PSNR and lower MSE.

III. Proposed Method

In this work the embedding and extraction sequence of secret message in algorithm can be pre-fixed to work with the order for colour components, like R, G, B for colour images, for extraction and embedding to add more security. For example, instead of embedding chunks of secret data sequentially in the order: R>>G>>B, the order can be shuffled to G>>R>>B or B>>R>>G. Correspondingly the Extraction order should be known to the Receiving end for proper retrieval. The R_G_B component combination will work as the KEY, as any improper order different that the order used at Embedding time will restrict the full message extraction. So it adds to the security of the algorithm without encryption/decryption. The work uses the Distance Algorithm mention by Liao, Zhang [6]

The embedding and extraction procedure is described in detail as follow:

Embedding procedure:

Step 1: Initialization: Separate the colour image into arrays (images-like) of same resolution, for all different colour components. (Note: For grayscale, images there will be only one component)

Step 2: For each colour-component image, follow the steps below:

a) The average difference value Diff is calculated by given equation:

$$\text{Diff} = \frac{1}{3}\sum_{i=1}^{4}(y_i - y_{min})$$

b) This method adaptively embeds messages using two levels and threshold value T is used to partition the range of Diff into two levels. If Diff ≤ T, Diff belongs to ‘‘lower-level”(the block belongs to a smooth area), then $k = k_l$. Otherwise, Diff belongs to ‘‘higher-level” (the block belongs to an edge area), then k = k_h. In order to succeed in the readjusting procedure, we apply the restrictions $2^{ki} \le T \le 2^{kh}$ and $1 \le k_i, k_h \le 5$.

c) Firstly, verify the block belongs to ‘‘Error Block”. If not continue to next step. Otherwise, restart from Step 1.

d) Convert y_i to be y_i' by the k-bit common LSB substitution method (1≤ i ≤ 4), respectively.

e) Apply the k-bit modified LSB substitution method to y_i' and let y_i'' be the result (1≤ i ≤ 4), respectively.

f) This step is described as “readjusting procedure”. Let $\hat{y}_i = y_i'' + l \times 2^k$, 1≤ i ≤ 4, 1 € {0, 1, -1}, and search $(\widehat{y_1}, \widehat{y_2}, \widehat{y_3}, \widehat{y_4})$such that

i. $\widehat{diff}$ and diff belong to the same level , where $\widehat{diff} = \frac{1}{3}\sum_{i=0}^{3}(\hat{y}_i - \hat{y}_{min})$, $\hat{y}_{min}$ = min $\{\widehat{y_1}, \widehat{y_2}, \widehat{y_3}, \widehat{y_4}\}$.

ii. The final stego block $(\widehat{y_1}, \widehat{y_2}, \widehat{y_3}, \widehat{y_4})$ does not belong to “Error Block”.

iii. The value of $\sum_{i=0}^{3}(\hat{y}_i - y_i)^2$ is minimized.

STEP 3: Final: Re-join the colour components images into single colour image with proper order for R-G-B components.

Extracting algorithm:

Step 1: The average difference value diff by the eq. (1).

Step 2: use the threshold value T to find out the level which diff belongs to, If diff belongs to the “lower level”, k = k_l, otherwise k =k^h.

Step 3: Verify whether the blocks to “Error Blocks “. If not, extract 4k-bit secret data from the k-bit LSB of y_i (1< I < 4). Otherwise, restart from step 1.

IV. EXPERIMENTATION AND RESULT

All the experiments are performed in MATLAB 7.10.0.499 (R2010a) on a PC with 2.50 GHz Intel(R) Core(TM)i5-3210M CPU, 4.00 GB RAM and 500 GB HDD under windows 8 environment. All the images are of size 512×512 and are in bmp format. The performance evaluation metrics used are Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), and embedding time. In this work, threshold (T) values = 7, 12, 15, 18 and k_l-k_h= 2-3, 2-4, 3-4, 2-5 have been considered to calculate PSNR, MSE and Embedded time for various images. PSNR of cover and stego image less than 30 is perceptible to human eyes. Image quality is better when PSNR value is higher.

PSNR is measured in decibels. peak signal to noise ratio (PSNR), applied to image as a quality metric by scaling the MSE according to the image range and is given by following equation:

$$PSNR = 10\log_{10}\frac{(255^2)}{MSE} \qquad (1)$$

Where MSE is mean square error and is given by:

$$MSE = \frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}(S_{xy} - C_{xy})^2 \qquad (2)$$

Where M and N are length and width of the 2D image Y respectively

(a) (b) (c)

Figure 1. Three cover images with size 512×512: (a) Lena (b) Peppers (c) Baboon.

(a) (b) (c)

Figure 2. Three stego images (T = 7, kl = 2, kh = 3) (a) Lena (embedded 101712 bits, PSNR = 51.87 dB) (b) Peppers (embedded 203424 bits, PSNR = 46.72 dB) (c) Baboon (embedded 406848 bits, PSNR = 41.48dB).

(a) (b) (c)

Figure 3. Three cover images with size 512×512: (a) Lena (b) Peppers (c) Baboon.

(a) (b) (c)

Figure 4. Three stego images (T = 7, kl = 2, kh = 3) (a) Lena (embedded 101712 bits, PSNR = 57.09 dB) (b) Peppers (embedded 203424 bits, PSNR = 51.33 dB) (c) Baboon (embedded 406848 bits, PSNR = 45.74 dB).

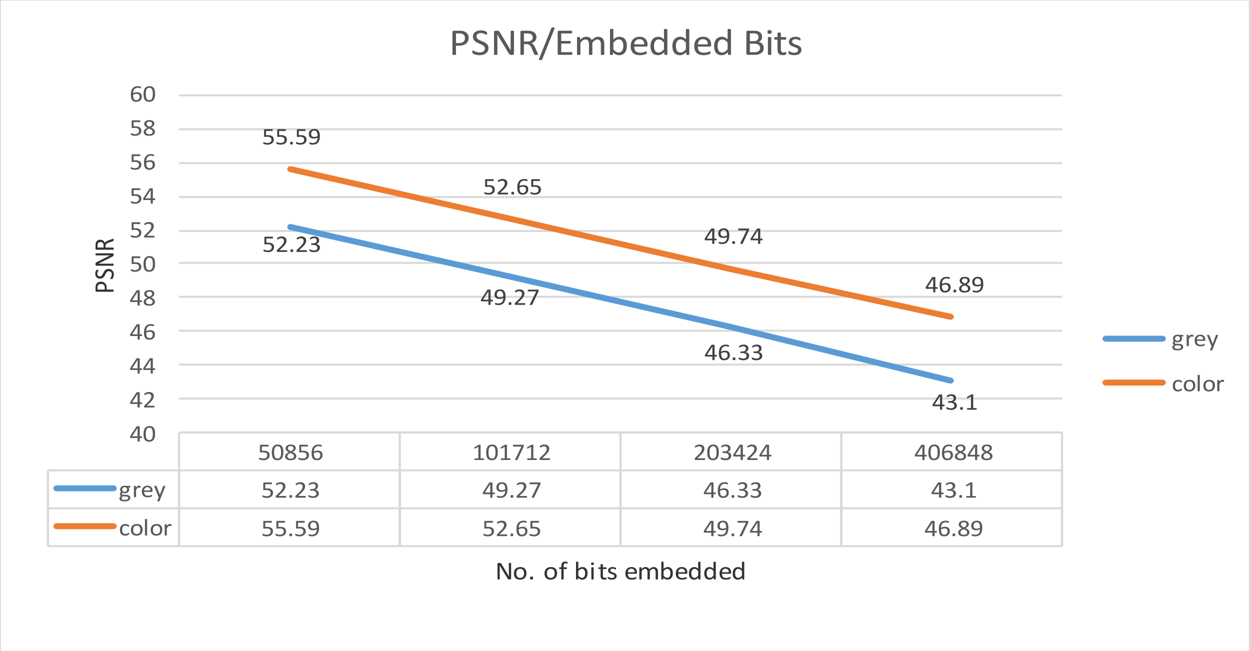
Experimental results have calculated on nine grey scale images (Baboon, Barbara, Goldhill, House, Jetplane, Lena, Peppers, Sailboat and splash) and same nine color images. Average PSNR values for grey scale and color images with different values of threshold (T) have shown in table1 and table 2 respectively. Figure1 depicts results are better in case of color images with higher PSNR (Peak Signal Noise Ratio) values as compared to grey scale images. In color images, PSNR values are increased by 4db to 5db. Figure 2 depicts as we increase the no of bits to be embedded the embedding time also increases. And it also shows when the difference between the lower and higher bit is more (k_l-k_h= 2-5, difference = 3) the embedding time decreases because it will enter the loop less no of times (as per the step 2 in algorithm) as compare to lower difference (k_l-k_h = 3-4, difference =1).

Table 1: Average value of PSNR and MSE for all grey images.

No. of embedded bit	T=7, 2-3		T=12, 2-4		T=15, 3-4		T=18, 2-5	
	Average							
	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE
50856	54.74	0.2335	53.69	0.3312	52.23	0.4188	50.91	0.8247
101712	51.72	0.4631	50.62	0.6441	49.27	0.8248	47.80	1.5595
203424	48.67	0.9315	47.42	1.3552	46.33	1.6502	44.02	3.3237
406848	45.51	1.9090	43.97	2.8113	43.10	3.3519	40.75	6.8882

Table 2: Average value of PSNR and MSE for all color images.

No. of embedded bit	T=7, 2-3		T=12, 2-4		T=15, 3-4		T=18, 2-5	
	Average							
	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE
50856	58.31	0.1301	57.13	0.2030	55.59	0.2387	53.87	0.5934
101712	52.89	0.4710	54.09	0.3920	52.65	0.4653	51.94	1.0202
203424	49.97	0.8433	51.02	0.9472	49.74	0.836	47.77	1.7175
406848	46.71	1.4929	47.74	1.1906	46.89	1.4031	43.98	3.1514



	50856	101712	203424	406848
grey	52.23	49.27	46.33	43.1
color	55.59	52.65	49.74	46.89

Figure 5 Comparison of grey and color images with respect to PSNR values

Table 3: Average value Embedding time of all color images

No. of embedded bit	T=7, 2-3	T=12, 2-4	T=15, 5-4	T=18, 2-5
	Average			
	Embedding time	Embedding time	Embedding time	Embedding time
50856	9.40871	10.82611	7.6206	11.2326
101712	19.06	21.14244	15.17922	22.81755
203424	37.94088	41.98055	30.39011	44.45811
406848	75.33648	81.88575	60.42807	87.35293

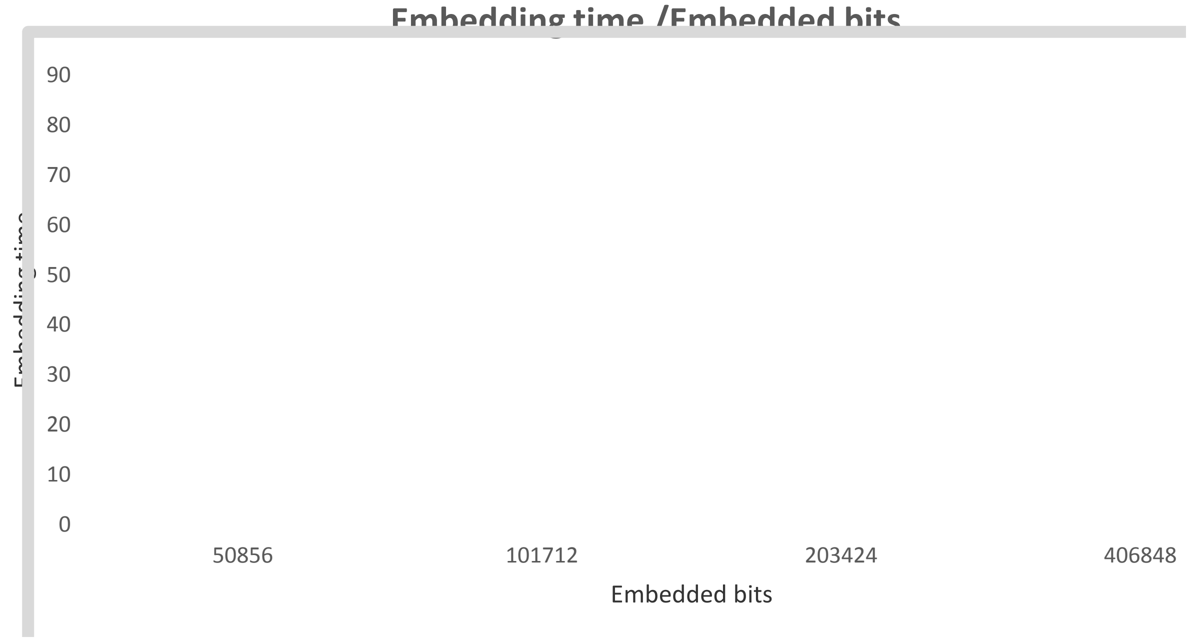


Figure 6 Embedding time Vs Embedded bits for color images at the different values of T= 7, 12, 15, 18

V. CONCLUSION

In this paper, we proposed a steganographic method based on modified LSB substitution. The result in table 2, show that the proposed method is able to achieve high PSNR values in color images as compared to grey scale images even after embedding 50856, 101712, 203424 and 406848 bits of secret data. The embedding time increases with the increase in no of bits embedded. The proposed method for shuffling the R, G, B component while embedding and the same for extraction, so one can prioritize which color blocks should be used first for embedding (usually the least important in the picture), like blue component can be used for hiding data in an image of flying birds with clear sky in background of image.

ACKNOWLEGDEMENT

With profound appreciation and due respect, I whole heartedly and sincerely acknowledge the initiatives, encouragement and proper direction by Dr. Sukhjeet Kaur Ranade Associate Professor, Department of Computer Science, Punjabi University, Patiala .

REFERENCES

[1] D.C. Wu and W.H. Tsai. “A steganographic method for images by pixel-value differencing.” Pattern Recognition Letters 24.9 (2003): 1613-1626.

[2] H.C. Wu, N.I. Wu, C.S. Tsai, M.S. Hwang. “Image steganographic scheme based on pixel-value differencing and LSB replacement methods.” Proc. Inst. Elect. Eng., Vis. Images Signal Process 152.5 (2005): 611-615.

[3] K.H. Jung, K.J. Ha, K.Y. Yoo. "Image data hiding method based on multi-pixel differencing and LSB substitution methods." in: International Conference on Convergence and Hybrid Information Technology 28 (2008): 355–358.

[4] C.M. Wang, N.I. Wu, C.S. Tsai, M.S. Hwang. "A high quality steganography method with pixel-value differencing and modulus function." J. Syst. Softw. 81 (2008): 150–158.

[5] Y.B. Lin, C.M. Wang and I.C. Lin. "Hiding data in spatial domain images with distortion tolerance." Computer Standards & Interfaces 31(2009): 458-464.

[6] X. Liao, Q.y. Wen, and J. Zhang. "A steganographic method for digital images with four-pixel differencing and modified LSB substitution." Journal of Visual Communication and Image Representation 22.1 (2011): 1-8

[7] R. S. Gutte, Y. D. Chincholkar, and P. U. Lahane. "Steganography for two and three LSBs using extended substitution algorithm." ICTACT Journal on communication technology 4.01 (2013): 685-690.

[8] M. Juneja and P. S. Sandhu. "Improved LSB based Steganography Techniques for Color Images in Spatial Domain." IJ Network Security 16.6 (2014): 452-46

[9] R. Bhardwaja and D. Khanna. "Enhanced the security of image steganography through image encryption." India Conference (INDICON) 17 (2015):1-4.

Suman is a student of M.Tech (CSE) in Department of Computer Science, Punjabi University, Patiala carrying out her research work under the guidance of Dr. Sukhjeet Kaur Ranade.

Dr. Sukhjeet Kaur Ranade is presently serving as Associate Professor in Department of Computer Science, Punjabi University, Patiala. Her key research areas are image processing and information hiding. She has published more than 50 papers in various journals and conferences of international and national repute.