Image Steganography Based On Optimal LSB Pixel Adjustment Method

TVS Gowtham Prasad*, Dr. S Varadarajan**, Dr. S.A.K Jilani***, Dr. G N Kodandaramaiah****
*Assistant professor, Dept. of ECE, Kuppam Engineering College,
tvsgowtham@gmail.com.
** Professor, Dept. of ECE, SVUCE, S V University.
*** Professor, Dept. of ECE, MITS.
**** Professor, Dept. of ECE, KEC

ABSTRACT

Now a days, internet becomes major channel for communicating information one place to other such as text, image, audio, video data. Steganography is a technique in which information can to be communicating secretly by hiding in another such as secondary information with changing its significance. This paper presents a new approach of image steganography using polynomial based optimal LSB and pixel adjustment method. This method main focus on adaptiveness of LSB's replacement and pixel adjustment for improving the capacity of hiding data and robustness of steganography. Objective analysis is done over the proposed method using MSE, PSNR and Normalized correlation method.

General Terms

Image processing, Data Security, steganography

Keywords

LSB Steganography, polynomial equations, Normalized correlation, Data hiding capacity.

I LITERATURE SURVEY

In olden days different data hiding methods are used for communicating information secretly. For example, during the Second World War invisible ink was used to write the information on a paper so that paper looks like a plain paper to other people. When we apply liquids like urine, milk, vinegar etc., and heated then letters on the paper are visible [1]. Today internet becomes very popular medium for communicating data such as text, image, audio, video etc. But cyber crimes, information copying and thefting are increasing day by day. To achieve secured communication data hiding methods are needed. Data hiding are of three types cryptography, steganography, watermark-ing [3].

Cryptography is a technique that hides data in scrambled in an unintelligent manner. It is difficult to the malicious user to extract the original message. The main drawback of the cryptography is that encrypted can be arouse suspiciously by the un authorized recipient which may causes message to damage. After that intended recipient cannot recover the message data[4][6][3]. Steganography comes from the Greek words Steganos (Covered) and Graptos (Writing).Steganography is about concealing and hiding information and provides secured communication between sender and recipient[2][1]. The data which contains secret message is called cover image and type of steganography is depend on the type cover. If cover is a text or image it is called text or image steganography respectively. In general, Steganography are of two types fragile and robust [text][1]. In fragile, information is hiding in the cover without destroying or damaging the significance of cover image. If cover image is damaged during communication secret message cannot be recovered. In robust, message is hided with protection and detection capabilities. Again, fragile steganography are of two types adaptive and non adaptive. In non-adaptive, modifications due to embedded data are uncorrelated with the cover features. In adaptive, modifications are correlated with cover features.

Steganography can be done in two ways; they are spatial domain method[3][4] and frequency domain method[5][6][7]. In Frequency domain, carrier image is transformed to its frequency representation before embedding the secret image. This method is difficult and slower than spatial domain. In spatial domain, secret image is embedding directly into the pixels of the carrier image. This method is easy and fast but less tolerance to noise. Least significant bit(LSB) substitution method is most commonly used in spatial domain. It has less data hiding capacity and less tolerance to noise. Steganography Terms:Cover-Medium – The medium in which information is to be hidden, also sometimes called as Coverimage or carrier. Stego-Medium – A medium in which information is hidden. Message – The data to be hidden or extracted. Stego_medium= hidden_ message + carrier + stego_key.

In this paper, a new approach for image steganography is proposed using adaptive LSB replacement and pixel adjustment method. The adaptive LSB is referred from[2] and pixel adjustment method is reffered from [3]. In this paper we proposed by combining the the above together to implement image steganography using polynomial equations. The performance analysis is done based on the mse, psnr and normalized correlation methods. Experimental results demonstrate the image quality and improved storage capacity.

II SIMPLE LSB INSERTION METHOD

In this section general operations of data hiding by simple LSB insertion method is described . simple LSb method embeds fixed length secret bits in the same length LSBs of pixels. It causes distortion when number of bits exceeds three.

Let us consider C be the original 8 bit cover image of size $M_c X N_c$.

$$C = \{p_{ij}\}\ 0 < i \le M_c ; 0 < i \le N_c \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots 1$$

P_{ij} is the pixel values varies from 0 to 2^8-1.

Let 'm' be n-bit secret message represented as

$$m = \{m_i\}\ 0 < i \le n \quad m_i \in \{0,1\} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots .2$$

Let us say 'm' message is 6-bit binary data {1 0 1 0 0 1}.To embed this data using LSB insertion method, it requires six pixels. Say pixel values are {120 201 150 223 250 140}.The 8-bit binary equivalent of the pixels are

{0 1 1 1 1 0 0 $\underline{0}$, 1 1 0 0 1 0 0 $\underline{1}$,
1 0 0 1 0 1 1 $\underline{0}$, 1 1 0 1 1 1 1 $\underline{1}$,
1 1 1 1 1 0 1 $\underline{0}$, 1 0 0 0 1 1 0 $\underline{0}$ }

The underlined bits are LSB bits in each pixel intensity value. These bits are replaced with each message bits and the resultant binary form of pixels is as below.

{0 1 1 1 1 0 0 $\underline{1}$, 1 1 0 0 1 0 0 $\underline{0}$,
1 0 0 1 0 1 1 $\underline{1}$, 1 1 0 1 1 1 1 $\underline{0}$,
1 1 1 1 1 0 1 $\underline{0}$, 1 0 0 0 1 1 0 $\underline{1}$ }

and the decimal equivalents are {121 200 151 222 250 141}

When these hided pixels is compared with original pixel values ,the difference is either 0 or 1. Thus embedding each bit in lsb of pixel don't change the quality of the message.To embed the message data in 2-bit LSb , it require only three Pixels such as { 121 200 151 }.After hiding the binary and decimal equivalents are { 0 1 1 1 1 0 $\underline{1\ 0}$, 1 1 0 0 1 0 $\underline{1\ 0}$, 1 0 0 1 0 1 $\underline{0\ 1}$ } and {122,203, 151}.When these hided pixels is compared with original pixel values, the difference varies in between 0&2^2-1.

Thus bit replacement can be expressed mathe-matically as

$$p'_{ij} = p_{ij-}p_{ij} \bmod 2^k + mi \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots 3$$

where 'k' represents number of bits to be embed in each pixel.

III OPTIMAL LSB PIXEL ADJUSTMENT METHOD:

In this section an optimal technique for image steganography is proposed to enhance the quality of the stego image and to increase the data hiding capacity. The basic concepts are taken from [2][7][3]. In this approach number of bits to be hide will be vary from pixel to pixel. The selection of pixel in the cover image used is done based on polynomial equation.

Let us consider second order polynomial equation

$$p(x) = ax^2 + bx + c \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots 4$$

Where a, b, c are the coefficients of polynomial equation. $p(x)$ should be calculated for different values of 'x'. $p(x)$ represents the location of the pixel in the cover image to be used for hiding the message.$i.e, x \in \{1,2,3, \ldots\ldots .\}$.Once polynomial values are determined, pixel value in the location equal to the polynomial value is separated and compared such that the gray level value is greater than 32, the embed three bits of message in the 3 lsb's of the pixel in cover image.if not embed only 2 lsb's of pixel in the cover image. So that, the changes in the pixel may not affect the feature of the cover image.

If $p_{ij} > 32\ then\ k = 3,$

$$p'_{ij} = p_{ij-}p_{ij} \bmod 8 + mi \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots 5$$

Otherwise $k = 2$

$$p'_{ij} = p_{ij-}p_{ij} \bmod 4 + mi \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots 6$$

Here 'mi' is not a binary data. It is decimal equivalent of the 3bit or 2bit binary message depending on the pixel value of the cover image.

After the LSB substitution, the gray level value of the original pixel is changed to some other value in the stego which might be affect the features of the cover image. To improve the quality of the stego image, it is necessary to bring the values of pixels to its original values. This can be done by using pixel adjustment method.Consider '$d1$' be the decimal equivalent of the message. '$d2$' be the decimal equivalent of the k-lsb bits in the pixel of a cover image. Let 'd' be decimal equivalent of the pixel in the stego image. If '$d1$' is greater than '$d2$' the substract the $2^k/2$ from the stego pixel 'd'. If '$d1$'is less than '$d2$' then add $2^k/2$ from the stego pixel 'd'.

$$if\ d1 > d2\ then\ d = d - (2^k/2) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots 7$$

$$otherwise\ d = d - (2^k/2) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots 8$$

As a result, pixel value of the stego image is estimated to the absolute value of the cover imaqge. Thus the error between stego pixel and original cover pixel may vary in between [0, 2^{k-1}].

IV Algorithm of the Proposed Method

Step 1*: Select The Secret Message to be embed.*

Step 2*: Select the Cover image.*

Step 3*: Check the size of the secret and cover images.*

Step 4*: If cover image > 8times of the secret data.*

Step 5*: Define polynomial equation and determine the polynomial values.*

Step 6*: If secret data size > cover image size.*

Step 7*: Select the cover image such that size should be large and go to step 5.*

Step 8*: Based on polynomial value, separate pixel in cover image.*

Step 9*: check the intensity of pixel.*

If pixel value>32

Embed three lsb in cover pixel

Else

Embed three lsb in cover pixel

Step 10*: estimate the pixel values based on pixel adjustment method.*

V IMAGE QUALITY METRICS:

In the image steganography, High quality stego image to be utilized so that unintended recipient couldn't identify the secret data embedded in it. Basically there are two approaches for image quality assessment. They are objective and subjective measuring method. Subjective measuring method is based in the visual capabilities of the human. Object measuring method is based the mathematical method. Objective methods are of three types a) Full -Reference b) No-Reference and c) Reduced-Reference[10],[13].In full Reference, reference image to be known. Full Reference is basically of two types

1. Simple statistics error metrics
2. HVS feature based metrics.

In this paper, simple statistic error metrics such as Mean Square Error, Peak Signal to Noise Ratio and Normalized correlation methods[10] are taken to analyze the quality of the stego image. Let us consider $x(i,j)$ represents the cover (reference) image and $y(i,j)$represents the distorted (modified) stego image due to the embedding of the secret data. Where i and j are the pixel position of the M×N image.

***Mean Square Error*:** The mean-squared-error (MSE) is the simplest, and the most widely used, full -reference image quality measurement. Similarity is determined by computing the error between the stego image and the reference cover image.

$$\mathrm{MSE} = \frac{1}{\mathrm{MN}} \sum_{i=1}^{M} \sum_{j=}^{N} (x(i,j) - y(i,j))^2 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots 9$$

MSE is zero when $x(i,j) = y(i,j)$.

Peak Signal to Noise Ratio (PSNR): The PSNR is evaluated in decibels and is inversely proportional the Mean Squared Error.

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{(2^n - 1)^2}{\sqrt{\mathrm{MSE}}}\right) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots .10$$

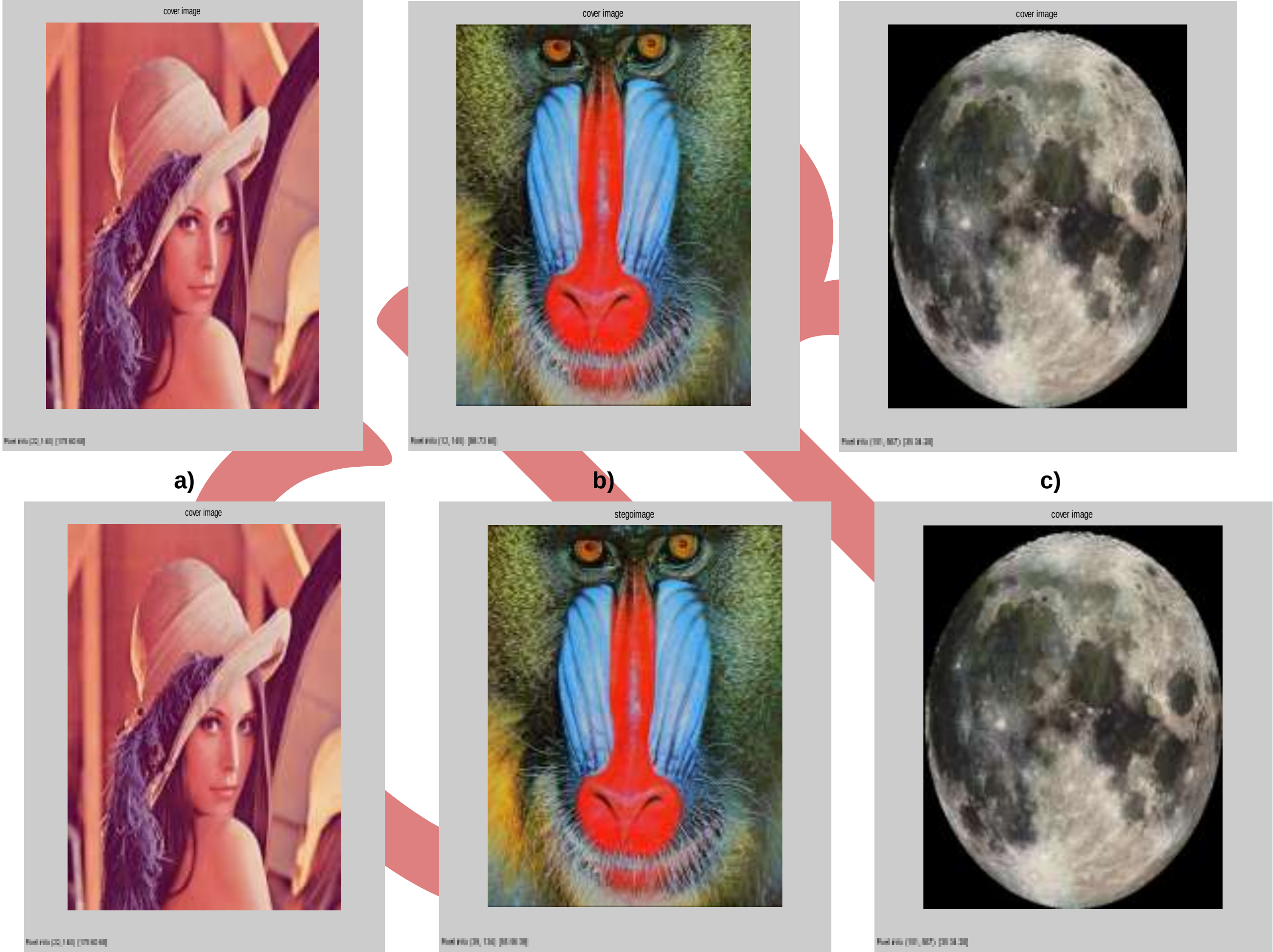
Where n is the number of bits to represent image.

Normalized Cross-Correlation (Nc): The closeness between two digital images can also be quantified in terms of correlation function. Normalized Cross-Correlation (NK) measures the similarity between two images and is given by the equation.

$$NC = \frac{\sum_{i=1}^{M}\sum_{j=}^{N}(x(i,j) * y(i,j))}{\sum_{i=1}^{M}\sum_{j=}^{N}x(i,j)^{2}} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots .11$$

VI RESULTS AND DISCUSSIONS

The algorithm explained in the above is coded in the MATLab and results are verified by considering different cover images such as lenna, baboon and moon. *Figure 1&2* shows the cover and stego images using the proposed method. In the below *Tabulation 1,2 and 3* estimated parameters such as MSE, PSNR, Normalized correlation and the required number of pixels for the hiding process are mentioned for LSB substitution method and the proposed method. In

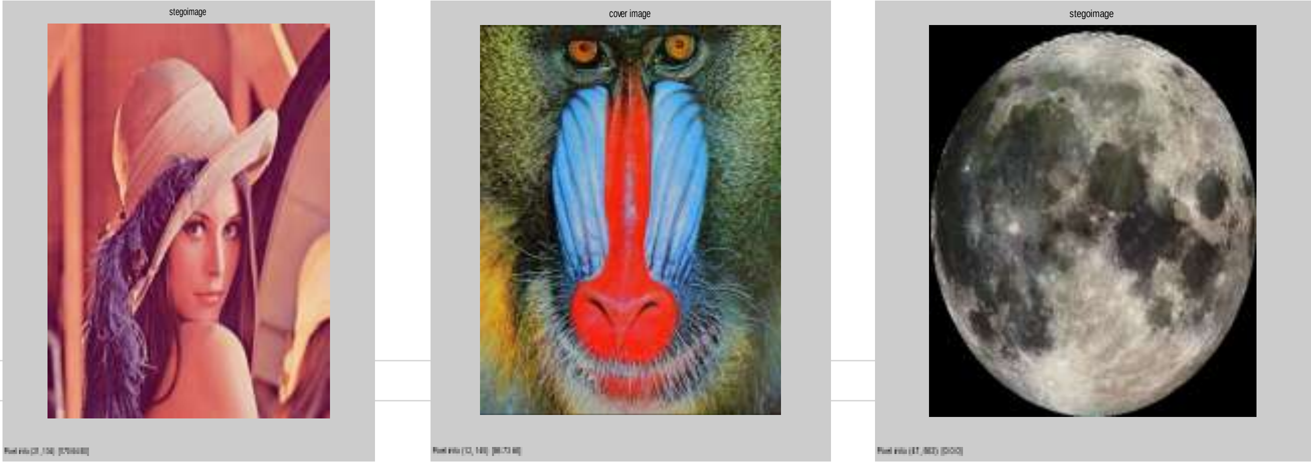


a) **b)** **c)**

Figure1: Cover images of the test images a) Lenna b) Baboon c) Moon

a) ***b)*** ***c)***

Figure2: Stego images of the test images a) Lenna b) Baboon c) Moon for 16KB Secret message



a) b) c)

Figure3: Stego images of the test images a) Lenna b) Baboon c) Moon for 150KB Secret message

omparison with the LSB Substitution method better PSNR and Less MSE values. But Normalized correlation values are differed in the second and third decimal values. Even the total number of pixels required for hiding the secrete message in proposed method is less than the pixels required in the LSB substitution method. We tested by taking two different sizes of secret message i.e, 16KB, 150KB.

Table 1: Analysis based on MSE, PSNR, and Normalized correlation for optimal LSB pixel Adjustment method for 150KB of secret data.

Coverimage	MSE	PSNR	Normalized correlation
Lenna	0.0163	88.0023	0.998
Baboon	4.5029	79.7375	0.991
Moon	0.0392	90.6584	1.000

Table 2: analysis based on MSE, PSNR, and Normalized correlation for LSB substitution method for 150KB of secret data.

Coverimage	MSE	PSNR	Normalized correlation
Lenna	0.0195	70.4018	0.996
Baboon	5.4035	63.7900	0.988
Moon	0.0470	72.5267	1.000

Table 3: Hiding capacity analysis for proposed optimal LSB Pixel Adjustment Method.

Hiding data size	No. of pixels required in Proposed method			2-LSB Method
	Lenna	Baboon	Moon	
16KB	5.657KB	6.093KB	5.355KB	5.3KB
150 KB	58.672KB	64.711KB	56.62KB	50KB

CONCLUSION

In this paper optimal LSB pixel Adjustment method has been implemented successfully and results based on different test images over various parameters such as MSE, PSNR, Normalized correlation and the required number of pixels for the hiding process are tabulated. Extensive work shows the effectiveness of the proposed method and the obtained results also proves the significant improvement than the LSB substitution method.

REFERENCES:

[1] M.Naseem, Ibrahim M hussain, M Kamran Khan, Aisha Ajmal, "*An optimum modified Bit Plane Slicing LSB Algorithm for secret data Hiding*", International Journal of computer applications(0974 – 8887), Vol-29, No.12, September 2011.

[2] Chi KWong Chan, L M Cheng, "*Hiding data in images by Simple LSB substitution*", The journal of the pattern recognition society, Elsevier Computer Science, Vol 37, no.3 Pages 469-474, 2004.

[3] R. Amirtharajan, R Akila, P Deepika chowdavarapu, "*A Comparative analysis of image steganography*",International Journal of computer applications (0975– 8887), Vol-2, No.3, May 2010.

[4]. Chang, C. C. and Tseng, H. W. "*A Steganographic method for digital images using side match*", Pattern Recognition Letters, 25: 1431-1437, 2004..

[5]. Chen, T. S., Chang, C. C., and Hwang, M. S, "*A virtual image cryptosystem based upon vector quantization*", IEEE Transactions on Image Processing, 7, 10: 1485-1488, 1998.

[6]. Chung, K. L., Shen, C. H. and Chang, L.C, "*A novel SVD- and VQ-based image hiding scheme",* Pattern Recognition Letters, 22: 1051-1058, 2001.

[7]. Iwata, M., Miyake, K., and Shiozaki, A, "*Digital Steganography Utilizing Features of JPEG Images*", IEICE Transfusion Fundamentals, E87-A, 4:929-936, 2004.

[8] Bruic Schneier, "*Applied Cryptography Protocals, Algorithm and source code in C*", 2nd Edition, Wiley India edition, 2007.

[9] W.Diffie and M E Hellman, "*Exhaustive Cryptanalysis of NBS Data Encryption Standards*", IEEE Computer, Vol-10, pages 74-84, 1977.

[10] Ahmet M. Eskicioglu, Paul S. Fisher, "*Image Quality Measures and Their Performance*" IEEE Transactions on Communication, Vol. 43, No. 12, pp. 2959-2965, December 1995.

[11] Zhou Wang, Alan C. Bovik , "*A Universal Image Quality Index*", IEEE Signal Processing Letters, Vol. 9, No. 3, pp.81-84, March 2002.

[12] Z. Wang, A. C. Bovik, L. Lu, "*Why is image quality assessment so difficult*", in Proc. IEEE Int. Conf. Acoustics, Speech, andSignal Processing, Vol. 4, pp. 3313–3316, May 2002.

[13] Carnec M., Le Callet P., Barba D., "*An image quality assessment method based on perception of structural information"*, IEEE International Conference on Image Processing (ICIP 2003), Vol. 3, No.3, pp. 14-17, Sept 2003.

Mr. T V S Gowtham Prasad received B.Tech in Electronics and Communication Engineering from Sree Vidyanikethan Engineering College, A.rangampet, Tirupati and M.Tech received from S V University college of Engineering, Tirupati. Pursuing Ph.D from JNTU, Anantapur in the field of signal processing as ECE faculty.

Dr. S Varadarajan received his B.Tech in Electronics and Communication Engineering from S V University in 1987 and he received M.Tech degree from NIT Warngal. He did his Ph.D in the area of Radar Signal Processing. He is Currently Chairman for Institute of Electronics and Telecommunication Engineering (IETE), Tirupati Center. Currently he is working as Associate professor in the department of Electronics and communication Engineering, S V U College of Engineering, Tirupati.

Dr.S.A.K.Jilani was obtained Ph.D from SK University, Anantapur. A.P. He is working as professor in the department of Electronics and Communications Engineering, Madanapalle Institute of Technology, Madanapalle. He has 12 years of experience. He has published more than 50 research papers in various journals.

Dr. G.N. Kodandaramaiah, Obtained B.E. degree from SJC College of Engineering, Mysore and M.Tech degree from VTU. He did Ph.D in the area of Vocal Tract under JNTU, Hyderabad. He is working as HOD in the Department of Electronics and Communications Engineering, Kuppam Engineering College,Kuppam. He has more than 15 years of experience in teaching field. He has published more than 30 research papers in various journals.