CONDITIONAL ENTRENCH SPATIAL DOMAIN STEGANOGRAPHY

N Sathisha[1], Madhusudan G N[2], K Suresh Babu[3], K B Raja[3], K R Venugopal[4]

[1]Department of ECE, Govt. S K S J Technological Institute, Bangalore, India
[2]Analyst, Accenture Services Pvt. Ltd., Bangalore, India.
[3]Department of ECE, University Visvesvaraya College of Engineering,
Bangalore University, Bangalore, India.
[4]Principal, University Visvesvaraya College of Engineering,
Bangalore University, Bangalore, India.

ABSTRACT

*Steganography is a technique of concealing the secret information in a digital carrier media, so that only the authorized recipient can detect the presence of secret information. In this paper, we propose a spatial domain steganography method for embedding secret information on conditional basis using 1-Bit of Most Significant Bit (MSB). The cover image is decomposed into blocks of 8*8 matrix size. The first block of cover image is embedded with 8 bits of upper bound and lower bound values required for retrieving payload at the destination. The mean of median values and difference between consecutive pixels of each 8*8 block of cover image is determined to embed payload in 3 bits of Least Significant Bit (LSB) and 1 bit of MSB based on prefixed conditions. It is observed that the capacity and security is improved compared to the existing methods with reasonable PSNR.*

KEYWORDS

Cover image, MSB, Payload, PSNR, Steganography.

1. INTRODUCTION

The steganography is covered writing to embed secret information in a carrier media for secure communication through open channel such that it does not draw the attention of an unauthorized person. The outbreak of internet technology has led to increase in the data exchange with high integrity and confidentiality which can be achieved using steganography. The most important requirements for steganography are (i) Imperceptibility: is essential for the security of hidden communication (ii) Capacity: is the size of the secret information embedded into the cover media (iii) Robustness: the ability of the payload to withstand disturbances caused by the intruder or noise developed in the non-ideal communication channel. The steganography methods based on secret key are (i) pure steganography: does not involve any exchange of key. (ii) Secret key steganography: embeds the secret message into the cover media using secret key at the sending end and the secret information cannot be retrieved without the secret key at the destination. The secret key may be embedded in the cover image or it is known between the two parties in the beginning. (iii) Public key steganography: does not require exchange of secret key. Public key and secret key are the two different keys generated at transmitting and receiving ends. Public key is used in the embedding of secret information into the cover media and secret key is used for retrieving of secret information from the steganodata.

DOI : 10.5121/sipij.2014.5303

The steganography based on carrier media are classified as (i) Text steganography: text steganography refers to the hiding of information within text messages without bringing out a notable change to the structure of the document. Some of the text steganography techniques are line shifting method, word shifting method, syntactic method, semantic method and text abbreviation. (ii) Audio steganography: embeds the secret message into digitized audio signal which results in slight altering of binary sequence of the corresponding audio file. Some of the available audio steganography methods are LSB coding: sampling technique followed by quantization to convert analog audio signal to digital binary sequence. In this technique LSB of carrier binary sequence of digitized audio file is replaced by binary equivalent of the secret message. Phase coding: encodes the secret message bits as phase shifts in the phase spectrum of a carrier digital signal achieving an inaudible encoding. Spread Spectrum: the secret information is scattered throughout the cover media without changing the statistical properties of cover media. Echo hiding: the secret message is embedded into cover audio signal as an echo. (iii) Image steganography: the payload and the cover are two different images. The payload is embedded inside the cover image using a suitable embedding algorithm resulting in the stego image.

The most popular hiding methods are spatial domain based steganography, palette based steganography and transform domain based steganography. Spatial domain based steganography includes the LSB replacement and Bit Plane Complexity Steganography (BPCS). The LSB technique is the most significant example of spatial domain embedding wherein the LSBs of the cover image is substituted by the MSBs of the payload. The BPCS steganography hides secret data by means of block replacing. Each image plane is segmented into the same size pixel-blocks (a typical size of 8*8) which are classified into informative and noise like blocks. The noise like blocks is then replaced with the secret blocks. Palette based steganography is generally used for the color images which are represented in the color luminance model like Y Cb Cr. Images transformed into the palette based color representation can be widely used over the internet which involves hiding the stego message into the palettes or indices of cover image. In transform domain based steganography the cover image and payload are converted into frequency domain or wavelet domain. The payload is embedded into the corresponding transform domain coefficients of the cover image. The transform domain techniques are Discrete Cosine Transform (DCT) which is used in common image compression format such as Moving Photographic Experts Group (MPEG) or Joint Photographic Experts Group (JPEG) and Discrete Wavelet Transform (DWT) which is used for hiding the secret message into the higher frequency of the wavelet transform while leaving the lower frequency coefficient sub band unaltered. Steganography is employed in various applications like enhancing robustness of image search engines and smart identity cards, copy right control of materials, video-audio synchronization, protection of intellectual property, exchange of highly confidential data in a covert manner and bank transactions.

Contribution: In this paper we proposed Conditional Entrench Spatial Domain Steganography (CESS) which embeds secret information in the LSB and MSB of cover image based on prefixed conditions to increase the security and capacity.

Organization: This paper is organized into following sections. Section 2 is an overview of related work. The steganography model is described in section 3. Section 4 discusses the algorithms used for embedding and extracting process. Performance analysis is discussed in section 5 and conclusions are given in section 6.

2. RELATED WORK

Rong Jian Chen et al., [1] presented a multi bit and multi-image steganography system using adaptive embedding algorithms with minimum error. The algorithm evaluates the most similar value to replace the original value. The adaptive method is divided into three steps i) embed logo data into cover data ii) adaptively adjust LSB's of the cover data. iii) Adaptively adjust the MSB

of the cover data. Manoj Kumar et al., [2] proposed an image steganography based on the Data Encryption Standard (DES) using the S box mapping and secret key. The secret image is pre-processed by embedding function and the stego image is formed by replacing the embedding function values into the cover image. Prem Kumar and Narayanan [3] have proposed a new scheme for secure banking application based on visual cryptography. The work integrates both steganography and cryptography at the same time and considers maximum number of surrounding pixels to achieve capacity of every target pixel. Chao Wang et al., [4] proposed a method of fast matrix embedding by matrix extending to reduce the computational complexity of random linear code based matrix embedding. The fast algorithm is developed by appending some referential columns to the parity check matrix. The parameters considered for improvement are computational complexity and embedding efficiency which is more suitable for real time steganographic systems. Vladimar Banoci et al., [5] proposed a secure steganography system in JPEG file based on modulus function which is secure against histogram attacks. The modulo histogram fitting with dead zone method embeds the secret data in JPEG file format. JPEG image is used as cover image and embedding is performed in DCT domain in JPEG file, the data hiding is done by changing the selected quantized DCT transform coefficients according to modulus function. Before embedding, the secret message is encrypted by AES-128 bit cipher to increase security level of steganography system.

Raja et al., [6] proposed a robust image adaptive steganography using integer wavelet transforms to hide large volumes of data without causing any perceptual degradation of the cover image. The payload is embedded in non-principal diagonal coefficients of the low frequency band of cover image for better robustness. Chen Ming et al., [7] presented an overview of the definitions and advantages of different steganography tools and algorithms such as file structure based steganography, spatial domain steganography, transform domain steganography, document steganography and other categories. Wien Hong et al., [8] proposed a lossless steganography technique that hides data in Absolute Moment Block Truncation Coding (AMBTC) compressed images based on the interchange of two quantization levels. In this technique data extracting procedures are efficient which is applied to real time image processing and the stegoimage preserves the same image quality as the original compressed images. Neha Agrawal and Marios Savvides [9] proposed a steganography technique used for hiding biometric information like finger print or iris code templates in discrete cosine transform coefficients of cover image. The method is used to verify the authenticity of original and transmitted image. Mankun Xu et al., [10] presented Model Based (MB) steganography using least square method to estimate the embedding rates towards MB JPEG steganography. Kotaro Yamamoto and Munetoshi Iwakiri [11] proposed a steganography technique to hide information using Standard Musical Instrument Digital Interface (MIDI) File as cover media to increase embedding payload. The embedding technique improves the payload capacity compared to any other conventional method without deteriorating performance quality.Vladimir Banoci et al., [12] proposed two methods of steganography using Code Division Multiple Access (CDMA) techniques. One method is code book which improves the perceptibility of stego images, the second method is code book with CDMA creates highly variable and easily modifying steganography system which increases security, capacity and PSNR used in radio telecommunication.

Abbas Cheddad et al., [13] proposed an algorithm of skin tone detection which takes images or video files in RGB color as input and embed the data on the selected specific Region of Interest (ROI) in the cover image. Jin-Suk Kang et al., [14] proposed an adaptive steganography using complexity on bit planes of color image by fixing threshold and variable length. In order to improve the BPCS technique information is inserted depending on the color image using bit plane and multichannel features. Mei-Ching Chen et al., [15] presented an extension of collage steganography which improves the payload capacity. The messages are hidden in the smooth regions of the cover object. The capacity of cover images in the data base is analyzed in advance in order to select a proper cover image according to the secret message. Nicholas Hopper et al.,

[16] introduced a steganographic protocol based on rejection sampling from the channel that is provably secure and has nearly optimal bandwidth.

A. W. Naji et al., [17] presented an overview of the steganography approaches and its classifications and also the type of attacks on the hidden information. Shreelakshmi R et al., [18] proposed pre-processing technique for cover images, which increases the reliability of LSB replacement steganography in spatial domain. Saeed Sarreshbedari and Shahrokh Ghaemmaghami [19] developed a high capacity image steganography using wavelet transform coefficient of the cover image to embed the secret information. The method uses noisy bit planes over the whole block to embed the secret information. Mahdi Ramezani and Shahrokh Ghaemmaghami [20] improved the embedding capacity and imperceptibility of the stego images by embedding the secret data into contrast image parts with Mod-4 technique which decreases the effects of modifications caused by the embedding process. Hongmei Tang et al., [21] presented an image encryption and steganography scheme. The secret message is encrypted through the combination of a gray value substitution operation and position permutation using logistic map then the secret information is hidden in the cover image. Logistic map makes the encryption system strong. Chiew Kang Leng and Pieprzyk Josef [22] proposed a method for estimating the length of secret message embedded in a binary gray scale image. They have made use of the changes of some image statistics (inter pixel correlation) of the 512 patterns histogram from boundary pixels as the distinguishing statistics.

Zahra Toony and Mansour Jamzad [23] proposed a method to resize the secret image into an appropriate smaller size using seam carving method by retaining the important contents of secret image. The smaller secret image is embedded in a cover image which prevents the distortion in the stego image. Che-Wei Lee and Wen-Hsiang T Sai [24] use Shamir's secret sharing method to generate partial shares of secret data by using the coefficients of some polynomial functions as data carriers for computing the shares. The portable network graphics image is utilized to embed the partial shares. Hamid Izadinia et al., [25] developed a method to hide large amount of secret message in quantized error value. Quantization of pixel values is done by using quantization index modulation method. If the pixel quantized error value is odd the secret bit is one and if the pixel quantized error value is even the secret bit is zero.

3. MODEL

In this section the definitions related to steganography, proposed embedding and retrieval models are discussed.

3.1. Definitions

(i) Cover image*:* It is an object consisting of the signal stream or data file as a carrier of the embedded object. The cover image may be of any format and dimensions. The raw cover images are good for steganography.

(ii) Payload: Message to be transmitted confidentially by embedding into cover image. The payload can be image, text audio, video etc.

(iii) Stego image: It is a unified image obtained from the combination of the cover image and the payload.

(iv) Mean Square Error (MSE): It is defined as the square of error between cover image and stego image. The distortion in the image can be measured using MSE. It is calculated using Equation 1

$$MSE = \left[\frac{1}{N}\right]^2 \sum_{i=1}^{N}\sum_{j=1}^{N}\left(X_{ij} - \bar{X}_{ij}\right)^2 \qquad (1)$$

Where: X_{ij}: The value of the pixel in the cover image.
$\overline{X}_{ij}$: The value of the pixel in the stego image.
N: Size of Image.

(v) Peak Signal to Noise Ratio (PSNR): It is the measure of quality of the stego image by comparing with the cover image in terms of signal and noise. PSNR is calculated using Equation 2.

$$PSNR = 10\log_{10}(255^2/\ MSE)\ dB \qquad (2)$$

(vi) Capacity: It is the size of the data in a cover image that can be modified without deteriorating the integrity of the cover image. The steganographic embedding operation needs to preserve the statistical properties of the cover image in addition to its perceptual quality. Capacity is represented by bits per pixel (bpp) and is computed using Equation 3.

$$Capacity = \frac{\text{number of bits of payload embedded}}{\text{total number of bits in the cover image}} \qquad (3)$$

(vii) Entropy: Entropy is a measure of security for a steganography system. A system is perfectly secure when the Relative Entropy (RE) tends to zero.

3.2. Proposed Embedding Model

The payload is embedded chaotically into the cover image based on the number of one's in three MSB bits of each pixel of cover image matrix to generate stego image. The high security steganography model is shown in Figure 1.

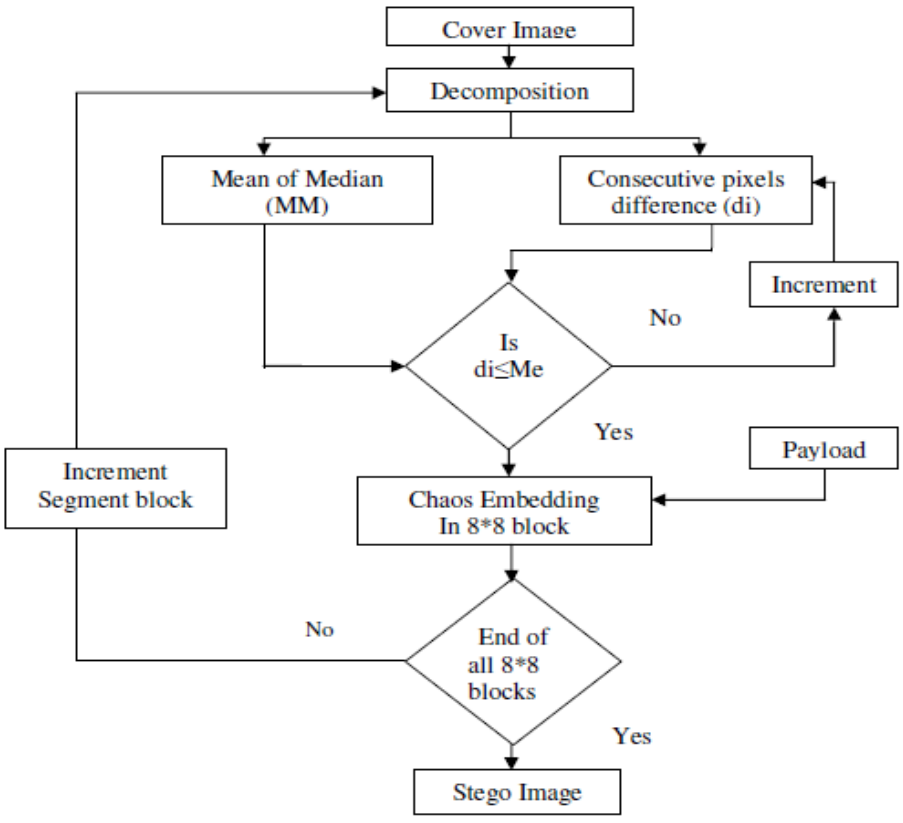


Figure.1. Embedding Model

(i) Cover Image Decomposition: The cover image of JPG, BMP, TIF, PNG formats with different dimensions are considered to verify the algorithm. The cover image is decomposed into 8*8 blocks, to increase security and capacity of steganography technique.

(ii) Upper and Lower Bound: Set the Upper Bound (UB) and Lower Bound (LB) values with maximum Range (R) of 200 to get optimum PSNR. Embed the bits of Upper and Lower Bound alternatively in the fifth bit of a pixel in the first block of the cover image using the Equations 4 and 5.

Upper Bound Embedding Position (UBEP)

$$UBEP=p_{(n,1)} \quad (4)$$

Lower Bound Embedding Position (LBEP)

$$LBEP=p_{(n,5)} \quad (5)$$

Where $n = 1,2, \ldots 8$ (x-coordinate in 8*8 matrix block)
p is the pixel intensity value in the cover image

The range (R) is calculated using the equation 6

$$R=UB-LB \quad (6)$$

(iii) Mean of Median (MM): Consider from second 8*8 block onwards and Compute the median values of all columns in each block using Equation 7.

$$M=\frac{1}{2}\{p_{(4,n)}+p_{(5,n)}\} \quad (7)$$

Where $n = 1,2, \ldots 8$ (y-coordinate of 8*8 matrix block)

Mean of Median (MM) values in each block is computed using the Equation 8.

$$MM=\frac{1}{8}\{\sum_{i=1}^{8} M(i)\} \quad (8)$$

(iv) The difference between the consecutive pixels *(d_i):* The difference between consecutive pixels from second block of cover image for embedding payload is computed using Equation 9.

$$d_i = |p_i - p_{i+1}| \quad (9)$$

Where *i* is the index of a pixel in 8*8 matrix block

(v) Chaos embedding: The values of MM and d_i are compared, if d_i is lesser than the MM, then embed the payload in adjacent pixels p_i and p_{i+1} of cover image using following steps.

1) Split each pixel into two parts, say most part and least part as shown in Figure. 2.

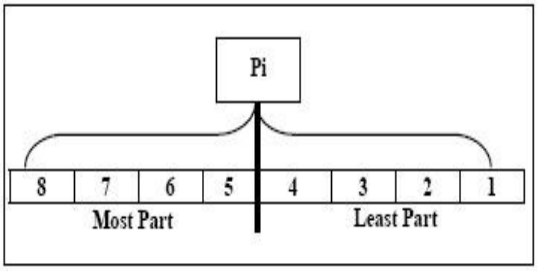


Figure 2. Splitting of Pixel

2) Count the number of ones in the first three bits of most part i.e., 8th, 7th and 6th positions in the pixel and embed payload into the cover image as per Table 1.

Table 1. Payload embedding cases

Number of ones in the three bits of most part	Cases	Number of bits to be embedded
0	Case 0	1 bit
1	Case 1	3 bits
2	Case 2	2 bits
3	Case 3	3 bits

3) *Case 0*:- Embed 1 bit of payload pixel in the 5th position of the cover image pixel.
4) *Case 1:*- Embed 3 bits of payload pixel into the 1st, 2nd and 3rd positions of the cover image pixel.
5) *Case 2:*- the two bits of Payload are embedded into the cover image. The one bit of payload is embedded into the first position of cover image pixel and increment counter A. The second bit of payload is embedded into either second or fifth position of cover image pixel based on the following conditions
   (a) The fifth position of the cover image pixel is used for embedding if Counter A > LB, Counter C > 5, and Counter B < R, increment counter B and reset Counter C to 0. Else
   (b) Embed in second position of the cover image pixel and increment Counter C.
6) *Case 3:*- the three bits of Payload are embedded into the cover image. The two bits of payload are embedded into the first and second positions of cover image pixel and increment counter A and counter C. The third bit of payload is embedded into either third or fifth position of cover image pixel based on the following conditions
   (a) The fifth position of the cover image pixel is used for embedding if Counter A > LB, Counter D > 5, and Counter B < R, increment counter B and reset Counter D to 0. Else
   (b) Embed in third position of the cover image pixel and Increment Counter D.

The counters used in the embedding process are

Counter A: - Total number of bits embedded in the 1st position of cover image pixel in case 2 and case 3.
Counter B: - Total number of bits embedded in the 5th position of cover image pixel in case 2 and case 3.
Counter C: - Number of bits embedded in the 2nd position of cover image pixel in case 2.
Counter D: - Number of bits embedded in the 3rd position of cover image pixel in case 3.

3.2. Proposed Retrieval Model

The payload is extracted by adapting reverse process of embedding and the block diagram is shown in Figure. 3. The stego image is segmented into blocks of 8*8 matrix. The values of upper bound and lower bound are extracted from the 5th bit of the pixel from the first block of the stego image and range is calculated. The MM and consecutive pixel difference di is calculated from 2nd block onwards. If di<MM the payload bits are extracted as per the Table 1 with different cases.

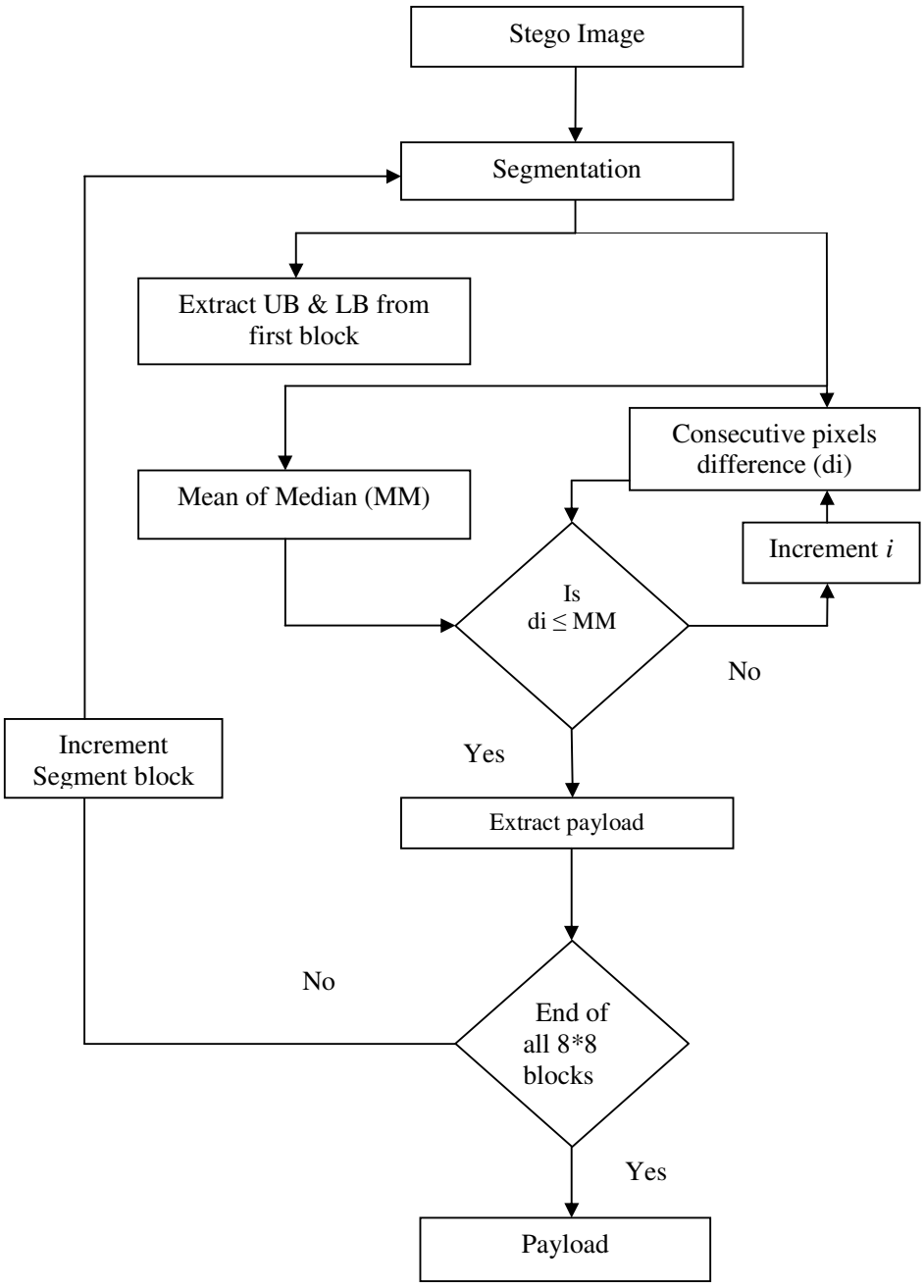


Figure 3. Retrieval Model

4. ALGORITHM

Problem definition: Given a cover image and payload images of gray scale or colour images, the payload is to be embedded into the cover image to derive stego image using LSB's and 1 bit of MSB replacement technique with chaotic manner.

Assumptions:

(i) The cover and payload scale images are different dimensions.

(ii) The stego image is transmitted over an ideal channel.

The embedding algorithm using chaotic technique in the spatial domain is given in Table 2. The payload is embedded into the cover image based on MM and di. The UB, LB and R are acting as keys and are embedded into fifth position of cover image pixels of first 8*8 block.

Table 2. Embedding algorithm of CESS

Input: Cover image

Output: Stego image

1. The cover image is segmented into blocks of 8*8.
2. The lower bound and upper bound with max range of 200 is set to use fifth bit of cover image pixel for embedding.
3. Embed lower bound and upper bound values in the first block of the cover image.
4. Determine Median (M) values for each block from second block onwards.
5. Determine the Mean of Median values of cover image.
6. The difference between consecutive pixel values in each block are computed.
   $d_i = |p_i - p_{i+1}|$
7. If $d_i \leq MM$, then embed payload in the cover image pixels p_i and p_{i+1}. in a chaotic manner.
8. The number of one's present in most bits of cover image pixel are counted and payload bits are embedded based on modified cases.
9. The one bit of payload is embedded into the fifth position of the cover image pixel in the case 0
10. The three bits of payload are embedded into the first, second and third position of the cover image pixel in the case 1
11. The two bits of payload are embedded into the first position and second or fifth position of the cover image pixel in the case 2
12. The three bits of payload are embedded into the first, second position and third or fifth position of the cover image pixel in the case 3.

The embedded payload is extracted at the destination from stego image by adapting reverse process of embedding is given in Table 3. The stego image is segmented into 8x8 matrix blocks. The UB and LB key values are extracted from first 8*8 block. The payload bits are extracted from second block onwards based on key values, MM and ***di***.

Table 3. Retrieving algorithm of CESS

Input: Stego image

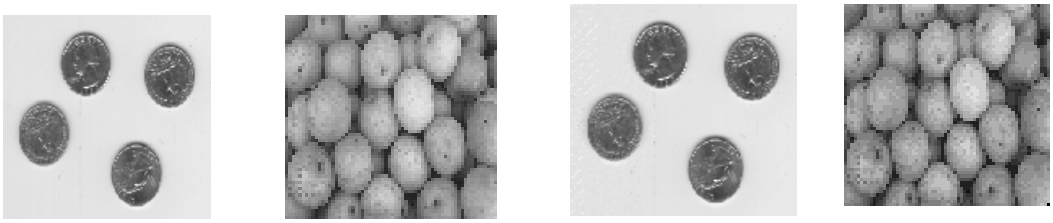
Output: Payload

1. The stegoimage is segmented into blocks of 8*8.
2. The lower bound and upper bound values from the first 8x8 block are extracted
3. Median (M) values for each block from second block onwards are computed.
4. The mean of median values of stego image is computed.
5. The difference between consecutive pixel values in each block are computed.
   $d_i - |\mu_i - \mu_{i+1}|$
6. If $d_i \leq MM$, then retrieve payload from the pixels p_i and p_{i+1} based on keys.
7. Arrange payload bits to construct payload image.

5. PERFORMANCE ANALYSIS

The cover images viz., Lena, Eight, Child, Blue hills and payload images such as Pears, Baboon and Lena are considered for performance analysis. The payload viz., Baboon, Pears, Baboon and Lena are embedded into the cover images such as Lena, Eight, Child and Blue hills respectively to generate stego images are shown in the Figure 4. It is observed that, the perceptual quality of stego images compared to respective cover images and also the perceptual quality of retrieved payloads compared to respective original payloads are very good.

a) Cover image Lena b) Payload image Baboon c) Stego image d) Retrieved payload



a) Cover image Eight b) Payload image Pears c) Stego image d) Retrieved payload

a) Cover image Child b) Payload image Baboon c) Stego image d) Retrieved payload

a) Cover image Blue hills b) Payload image Lena c) Stego image d) Retrieved payload

Figure. 4. The payloads Baboon, Pears, Baboon and Lena are embedded into Lena, Eight, Child and Blue hills cover image respectively

5.1. Performance analysis using PSNR and Relative Entropy (RE)

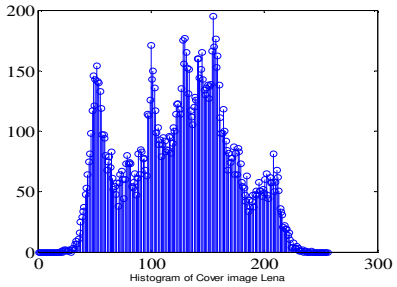
The Variation of PSNR and Relative Entropy for different formats of images with a Capacity of 0.25 bpp are tabulated in Table 4. The values of RE varies between 0.0011 to 0.3996 with an average PSNR value of around 43 dB. The very low value of RE represents more secure of Payload (P.L). The PSNR values of 43 dB indicate, the quality of stego image is almost equivalent to original Cover Image (C.I). Hence the proposed algorithm is more secure.

Table. 4. Variation of PSNR and RE with 0.25 bpp Capacity

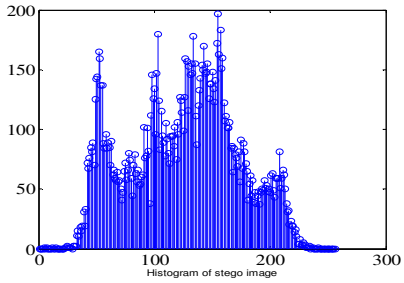
Combination	PSNR (dB)	RE
C.I:-Eight.tif, P.L:-Pears.png	42.532	0.3996
C.I:-Cell.tif, P.L:-Child.tif	43.827	0.0453
C.I:-Child.tif, P.L:-Baboon.jpg	42.126	0.3122
C.I:-Blue hills.jpg, P.L:-Pears.png	41.367	0.0302
C.I:-Lena.jpg, P.L:-Baboon.jpg	43.70	0.0011

a) Cover Image Lena

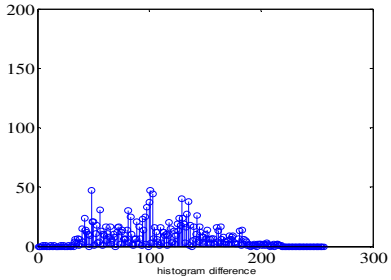
b) Stego image



c) Histogram of Cover image Lena



d) Histogram of stego image



e) Histogram difference

Figure.5. Histograms of Cover image Lena, Stego image and Difference.

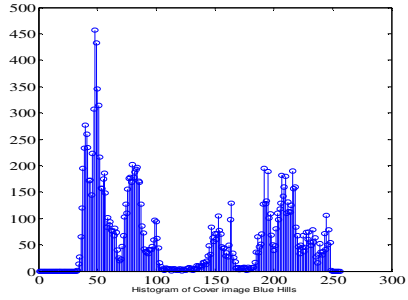
5.2. Performance analysis using histograms

The cover images Lena, Eight, Child and Blue hills are used to generate stego images with Baboon, Pears, Baboon and Lena payload. The payload Baboon is embedded into cover image Lena to generate stego image and the corresponding histograms of cover image and stego image with difference in histograms of cover image and stego image are shown in Figure 5.

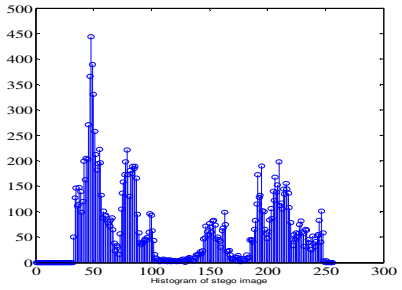
The payload Lena is embedded into cover image Blue hills to generate stego image and the corresponding histograms of cover image and stego image with difference in histograms of cover image and stego image are shown in Figure 6.

a) Cover Image Blue hills

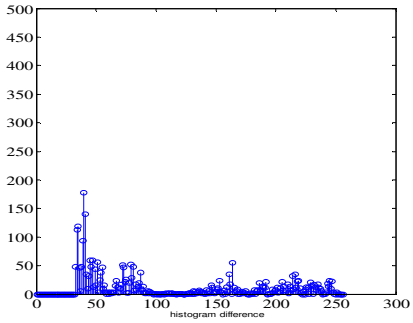
b) Stego image



c) Histogram of Cover image Blue hills



d) Histogram of stego image



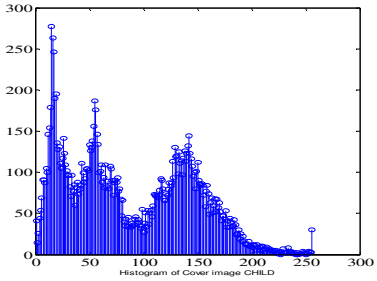
e) Histogram differnce

Figure.6. Histograms of Cover image Blue hills, Stego image and Difference

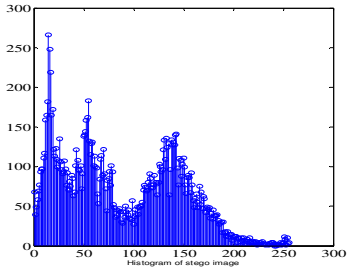
The payload Baboon is embedded into cover image Child to generate stego image and the corresponding histograms of cover image and stego image with difference in histograms of cover image and stego image are shown in Figure 7.

a) Cover Image Child

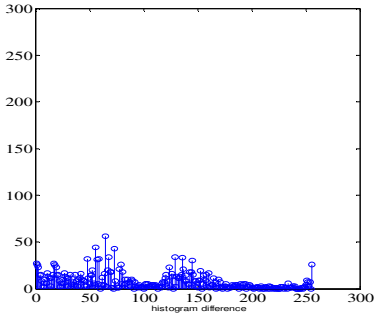
b) Stego image



c) Histogram of Cover image Child



d) Histogram of stego image



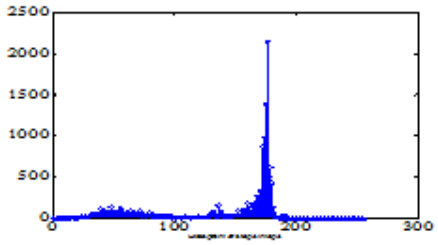
e) Histogram differnce

Figure.7. Histograms of Cover image Child, Stego image and Difference

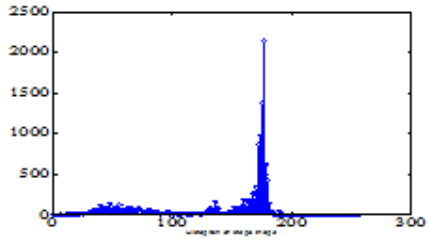
The payload Pears is embedded into cover image Eight to generate stego image and the corresponding histograms of cover image and stego image with difference in histograms of cover image and stego image are shown in Figure 8. It is noticed that the histogram patterns of all cover images and stego images are almost same. Hence difference in histograms of cover images and stego images are almost zero. The steganalysis tool based on statistical analysis of histogram difference cannot detect the proposed algorithm as histograms difference is almost zero. Hence the proposed algorithm is secure.

a) Cover Image Eight

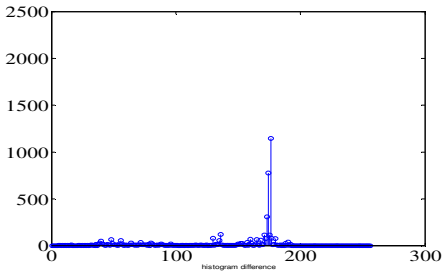
b) Stego image



c) Histogram of Cover image Eight



d) Histogram of stego image



e) Histogram differnce

Figure.8. Histogram of Cover image Eight, Stego image and Difference

5.3. Performance comparison of proposed method with existing methods.

The Table 5 shows the comparison of PSNR of the existing Steganographic Methods presented by Wen-Chung Kuo and Shao-Hung Kuo [26] Cheng-Ta Huang et al., [27] Rengarajan Amirtharajan et al., [28] Khodai and Faez [29] and the proposed CESS algorithm. It is observed that the PSNR is higher in the case of proposed method compared to the existing algorithms as the quality of stego image is better with moderate capacity.

Table 5: Comparison of PSNR values with Lena as cover image

Authors	Technique	Capacity	PSNR (dB)
Wen-Chung Kuo and Shao-Hung Kuo [26]	Reversible data hiding based on EMD	0.0058	28.0
Cheng-Ta Huang et al., [27]	LSB & Vector quantizing	0.20	33.83
Rengarajan Amirtharajan et al., [28]	Standard Deviation converges for Random Image Steganography	0.28	35.00
M Khodai and K Faez [29]	Adaptive steganography using LSB substitution and PVD	0.379	38.18
Proposed Method	CESS	0.25	43.82

5.4. Security aspects of proposed method

The aim of steganography is to embed secret information into a carrier without disturbing much of statistical characteristics of carrier and evade steganalytic detection. It is apparent that, the measure of MSE and PSNR are not good measure for security against steganalysis detection. The proposed algorithm is more secure since (a) The MSB bit of cover image is used for embedding and (b) the bits of cover image are replaced by payload bits chaotically.

6. CONCLUSION AND FUTURE WORK

In this paper CESS algorithm is proposed in which the payload bit stream is embedded in both MSB and LSBs of gray scale cover image. The cover image is decomposed into 8*8 blocks. The key is embedded in the first block, which is used to retrieve the payload at the destination. The remaining 8*8 blocks are used to embed payload on conditional manner to safeguard the secret information. The difference between neighbour pixels *di* is computed and compared with the computed values of mean of median of each 8*8 matrix block. If $di < MM$ then the payload is embedded chaotically by using one MSB bit of cover image. The algorithm has better capacity and security with high PSNR compared to the existing algorithm. In future the same technique can be extended to the transform domain and robustness of algorithm can be verified.

REFERENCES

[1] Rong-Jian Chen, Jui-Lin Lai and Shi-Jinn Horng, "Novel Multi-bit and Multi-image Steganography Using Adaptive Embedding Algorithms with Minimum Error," Fifth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, pp. 221 – 228, 2011.

[2] Manoj Kumar Ramaiya, Naveen Hemrajani and Anil Kishore Saxena, "Security Improvisation in Image Steganography using DES," Third International Advance Computing Conference, pp. 1094 – 1099. 2013.

[3] S Prem Kumar and A E Narayanan, "New Visual Steganography Scheme for Secure Banking Application," IEEE International Conference on Computing Electronics and Electrical Technologies, pp.1013-1016, 2012.

[4] Chao Wang, Welming Zhang, Jiufen Liu and Nenghai Yu, "Fast Matrix Embedding By Matrix Extending," IEEE Transactions on Information Forensics and Security, Vol. 7, No 1, pp.346-350, February 2012.

[5] Vladimir BANOCI, Gabriel BUGAR, Dusan LEVICKY and Zita KLENOVICOVA, "Histogram Secure Steganography System In JPEG File Based on Modulus Function," Twenty Second International Conference Radioelectronika, pp. 1 – 4, 2012.

[6] K B Raja, S Sindhu, T D Mahalakshmi, S Akshatha, B K Nithin, M Sarvajith, K R Venugopal and L M Patnaik, "Robust Image Adaptive Steganography using Integer Wavelets," IEEE International Conference on Communication systems, Software and Workshops COMSWARE 2008, pp. 614-621, January 2008.

[7] Chen Ming, Zhang Ru, Niu Xinxin and Yang Yixian, "Analysis of Current Steganography Tools: Classifications and Features," International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 384-387, December 2006.

[8] Wien Hong, Tung-Shou Chen and Chih-Wei, Shiu, "Lossless Steganography for AMBTC-Compressed Images," Congress on Image and Signal Processing, pp. 13 – 17, May 2008.

[9] Neha Agrawal and Marios Savvides, "Biometric Data Hiding: A 3 Factor Authentication Approach to Verify Identity with a Single Image using Steganography, Encryption and Matching," IEEE Conference on Computer Vision and Pattern Recognition, pp. 85 – 92, June 2009.

[10] Mankun Xu, Tianyun Li and Xijian Ping, "Estimation of MB Steganography Based on Least Square Method," IEEE International Conference on Acoustics, Speech and Signal Processing, pp. 1509 – 1512, April 2009.

[11] Kotaro Yamamoto and Munetoshi Iwakiri, "A Standard MIDI File Steganography Based on Fluctuation of Duration," International Conference on Availability, Reliability and Security, pp. 774 – 779, March 2009.

[12] Vladimir Banoci, Gabriel Bugar and Dusan Levicky, "Steganography Systems by using CDMA Techniques," Nineteenth International Conference Radioelektronika, pp. 183 – 186, April 2009.
[13] Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt, "Enhancing Steganography in Digital Images," Canadian Conference on Computer and Robot Vision, pp. 326 – 332, May 2008.
[14] Jin-Suk Kang, Yonghee You and Mee Young Sung, "Steganography using Block-Based Adaptive Threshold," Twenty Second International Symposium on Computer and Information Sciences, pp.1 - 7, November 2007.
[15] Mei-Ching Chen, Sos S Agaian and C.L.Philip Chen, "Generalized Collage Steganography on Images," IEEE International Conference on Systems, Man and Cybernetics, pp. 1043 – 1047, October 2008.
[16] Nicholas Hopper Luis von Ahn and John Langford, "Provably Secure Steganography," IEEE Transactions on Computers, pp. 662 – 676, May 2009.
[17] A W Naji, Teddy S Gunawan, Shihab A Hameed, B B Zaidan and A A Zaidan, "Stego-Analysis Chain, Session One Investigations on Steganography Weakness vs Stego-Analysis System for Multimedia File," International Association of Computer Science and Information Technology, pp. 405 – 409, April 2009.
[18] Shreelekshmi R, Wilscy M Madhavan and C E Veni, "Cover Image Preprocessing for More Reliable LSB Replacement Steganography," International Conference on Signal Acquisition and Processing, pp. 153 – 156, 2010.
[19] Sarreshtedari S and Ghaemmaghami S, "High Capacity Image Steganography in Wavelet Domain," Consumer Communications and Networking Conference, pp. 1 – 5, 2010.
[20] Ramezani M and Ghaemmaghami S, "Adaptive Image Steganography with Mod-4 Embedding Using Image Contrast," Consumer Communications and Networking Conference, pp. 1 – 4, 2010.
[21] Hongmei Tang, Gaochan Jin, Cuixia Wu and Peijiao Song, "A New Image Encryption and Steganography Scheme," International Conference on Computer and Communications Security, pp. 60 – 63. 2010
[22] Chiew Kang Leng and Pieprzyk Josef, "Estimating Hidden Message Length in Binary Image Embedded by Using Boundary Pixels Steganography," International Conference on Availability, Reliability and Security, pp. 683 – 688, 2010.
[23] Toony Z and Jamzad M, "A Novel Image Hiding Scheme Using Content Aware Seam Carving Method," International Conference on Availability, Reliability and Security, pp. 702 – 707, 2010.
[24] Ch-Wei Lee and Wen-Hsiang Tsai, "A New Steganographic Method Based on Information Sharing Via PNG Images," International Conference on Computer and Automation Engineering, pp. 807 – 811, 2010.
[25] Hamid Izadinia, Fereshteh Sadeghi and Mohammad Rahmati, "A new Steganographic Method Using Quantization Index Modulation," International Conference on Computer and Automation Engineering, pp. 181 – 185, 2010.
[26] Wen-chung Kuo and Shao-hung Kuo, "Reversible Data Hiding for JPEG Based on EMD," Seventh Asia Joint Conference on Information Security, pp. 1 – 4, 2012.
[27] Cheng-Ta Huang, Wei-Jen Wang, Min-Yi Tsai and Chin-feng Lee, "Employing LSB and VQ for Undetectable Secret Data Hiding," Ninth International Conference on Ubiquitous Intelligence and Computing and Ninth International Conference on Autonomic and Trusted Computing, pp. 644-649, 2012.
[28] Rengarajan Amirtharajan, P. Archana, V. Rajesh, G. Devipriya and J. B. B. Rayappan, "Standard Deviation Converges for Random Image Steganography," IEEE Conference on Information and Communication Technologies, pp. 1064 – 1069, 2013.
[29] M Khodaei and K Faez, "New Adaptive Steganographic Method using Least Significant Bit Substitution and Pixel value Differencing," IET Image Processing, Vol. 6, pp. 677 -686, 2012.

AUTHORS

N Sathisha received the BE degree in Electronics and Communication Engineering from Bangalore University and the M. Tech degree in Digital Communication and Networking from Visvesvaraya Technological University, Belgaum. He is pursuing Ph.D. in Computer Science and Engineering of Bangalore University under the guidance of Dr. K Suresh Babu, Assistant Professor, Department of Electronics and Communication Engineering, University Visvesvaraya College of Engineering. He is currently an Assistant Professor, Dept. of Electronics and Communication Engineering, Govt. SKSJ Technological Institute, Bangalore. He has over 8 research publications in refereed International Journals and Conference Proceedings. His research interests include Computer and Information Security, Computer Networks, Image Processing and Communication Engineering. He is a life member of Indian Society for Technical Education, New Delhi. He is a life member of Institute of Electronics and Telecommunication Engineers, New Delhi.

Madhusudan G N received the BE degree in Electronics and Communication Engineering from R L Jalappa Institute of Technology, Doddaballapur. Under Visvesvaraya Technological University. His areas of interests include Computer and information security, computer networks, Image processing and Communication Engineering. He is currently an analyst Accenture Services Pvt. Ltd, Bangalore.

K Suresh Babu is an Associate Professor, Dept. of Electronics and Communication Engineering, University Visvesvaraya College of Engineering, Bangalore University, Bangalore. He obtained his BE and ME in Electronics and Communication Engineering from University Visvesvaraya College of Engineering, Bangalore. He was awarded Ph.D. in Computer Science and Engineering from Bangalore University. He has over 20 research publications in refereed International Journals and Conference Proceedings. His research interests include Image Processing, Biometrics, Signal Processing,

K B Raja is an Associate Professor, Dept. of Electronics and Communication Engineering, University Visvesvaraya College of Engineering, Bangalore University, Bangalore. He obtained his BE and ME in Electronics and Communication Engineering from University Visvesvaraya College of Engineering, Bangalore. He was awarded Ph.D. in Computer Science and Engineering from Bangalore University. He has over 120 research publications in refereed International Journals and Conference Proceedings. His research interests include Image Processing, Biometrics, VLSI Signal Processing, Computer Networks

K R Venugopal is currently the Principal, University Visvesvaraya College of Engineering, Bangalore University, Bangalore. He obtained his Bachelor of Engineering from University Visvesvaraya College of Engineering. He received his Master's degree in Computer Science and Automation from Indian Institute of Science, Bangalore. He was awarded Ph.D. in Economics from Bangalore University and Ph.D. in Computer Science from Indian Institute of Technology, Madras. He has a distinguished academic career and has degrees in Electronics, Economics, Law, Business Finance, Public Relations, Communications, Industrial Relations, Computer Science and Journalism. He has authored 27 books on Computer Science and Economics, which include Petrodollar and the World Economy, C Aptitude, Mastering C, Microprocessor Programming, Mastering C++ etc. He has been serving as the Professor and Chairman, Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bangalore University, Bangalore. During his three decades of service at UVCE he has over 275 research papers to his credit. His research interests include computer networks, parallel and distributed systems, digital signal processing and data mining.