Steganography Based on Payload Transformation

K B Shiva Kumar [1], K B Raja[2], R K Chhotaray[3], Sabyasachi Pattnaik[4]

**[1]Department of TC, Sri Siddhartha Institute of Technology,
Tumkur, Karnataka, India**

**[2]Department of ECE, University Visvesvaraya College of Engineering, Bangalore University,
Bangalore, India**

**[3]Department of CSE, Seemanta Engineering College,
Mayurbhanj, Orissa, India**

**[4]Department of Computer Science˒,
FM University, Balasore, Orissa, India**

Abstract

Steganography is meant for covert communication of confidential data through internet. In this paper, we propose Steganography based on Payload Transformation (SPT) which is non LSB and non transform domain technique where the cover image is segmented into 2*2 matrices and the matrix for payload embedding is considered based on the threshold value fixed by computing adjacent pixel intensity differences. The transformation matrix is obtained based on identity matrix and the payload bit pair. Then the stego image 2*2 matrices are derived from 2*2 cover image matrices and the transformation matrix. A key generated with first bit of payload matrix at the sending end is used to extract the payload from the stego image. It is observed that proposed algorithm is more secure and robust with reasonable PSNR in comparison with existing algorithms.

Keywords: Steganography, Cover Image, Payload, Stego Image.
.

1. Introduction

A technique to hide messages in an unsuspicious manner to hackers is known as steganography. The term being derived from *Greek* words *Steganos* and graphia. In the present scenario with the aid of computers and internet, the multimedia files are used as a medium to hide information in digital steganography. For secure communication from eavesdroppers both cryptography and steganography techniques can be used even though their approaches are different. Cryptography has a strong mathematical base in number theory as it is a well researched area. The data encrypted using cryptographic technique cannot be decrypted without the knowledge of the key. The modern digital steganographic techniques are classified as text based steganography, audio steganography and image steganography.

In text based steganography the message to be sent is embedded in a text file by formatting it. Audio steganography alters audio files to hide messages. Image steganographic technique is the most popular one to hide message in the images as no perceivable changes occur in images after hiding the data within them. There are several techniques of image steganography to hide the payload within the cover image and the most popular among them are spatial domain and transform domain steganographic techniques. Further spatial domain steganography includes: (i) Bit Plane Complexity Steganographic (BPCS) technique where the secret data is hidden by segmenting each image plane into small size blocks called informative and noise like blocks and noise blocks are replaced by secret information blocks. (ii) The Least Significant Bit (LSB) technique where LSBs of cover image are replaced by the MSBs of payload. In transform domain steganography, the cover image and/or payload are converted into frequency domain and the stego image is derived by embedding the payload into the coefficient of cover image. The major applications of steganography are in Defense and Intelligence, Copyright Protection Bank Transactions, Law Enforcements, Counter Intelligence Agencies and in medical field to hide information of a patient.

Contribution: In this paper SPT algorithm is proposed for secure communication. The cover image is segmented into 2∗2 cells and the threshold value is determined based on adjacent pixel intensity differences. The H_T obtained from identity matrix and payload bit pair, is multiplied by 2∗2 valid cover image matrix to generate stego image.

Organization: The 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 Conclusion is given in section 6.

2. LITERATURE SURVEY

Nan-I Wu and Min-Shiang Hwang [1] have done a survey of the existing steganographic techniques and discussed the requirements of stego systems, in various image formats like gray scale, JPEG, binary and Pallet images. They have summarised various spatial-domain hiding techniques like LSB, PVD and MBNS and made a comparison of the systems. Some suggestions regarding future research and development are made. Cachin [2] has proposed a model of steganography based on information theory by interpreting the adversary's task of differentiating between cover text and stego text as hypothesis testing problem. Relative entropy is used as a quantitative measure of a stego systems security. The universal stego system that needs no knowledge of cover text distribution, except that it is generated from independently repeated experiments is discussed. Neil F. Johnson and SushilJajodia [3] have discussed an overview of steganalysis technique. Some properties of information hiding techniques can help the steganalyst to infer the presence of hidden message and where to look for such hidden messages in the medium. İsmail Avcıbaş, et al., [4] have presented a steganalysis technique for images that have been subjected to embedding by steganographic algorithms. They have used the seventh and eighth bit planes of an image for the computation of several binary similarity measures. The correlation between the bit planes as well as the binary texture characteristics within the bit planes is used to construct a classifier that can distinguish between stego and cover images. The scheme is found to have complementary performance with other steganalysis schemes.

Young WANG et al., [5] discussed a steganographic method based on keyword shift by borrowing the ideas from cryptographic algorithm of low key authentic degree. Shifting of sensitive keywords in the text is the master key of the method. Hironori Takimoto et al.,[6] proposed an arrangement and detection method of an invisible calibration pattern based on human visual perception by adding high frequency component to blue intensity in a limited region, the calibration pattern is embedded in the original image. Yifeng Sun and Fenlin Liu [7] emphasised on selecting cover for image steganography by correlation coefficient to improve the security. The cover data are modelledas Gauss-Markov process and the cover with smaller correlation parameter is selected to improve security. VijayKumar and dinesh Kumar [8] experimentally augments that error block replacement with diagonal detail coefficients gives better PSNR through performance evaluation of DWT based image steganography. Che Lun Pan et al.,[9] proposed an improved shifting method compared to histogram shifting embedding using difference between sub-sampled image which results in the increase of image quality and decrease in unnecessary damage with high PSNR. Jayachandran and Manikandan [10] suggested Symthatic Aperture Radar (SAR) using steganography to conceal the confidential SAR image built during the surveillance flight by enabling satisfactory compression of both visible and concealed SAR images.

Manish Mahajan and Akashdeep Sharma [11] proposed a 2^k correction method to hide data in colour images using information reflector to assure the maximum security against the visual attacks. Mohamed Elsadig et al.,[12] gave an overview of the use data hiding methods in digital video and hoe least significant method is used in high rate video streaming steganography. The digital video file is considered as separate frames and changing the output image displayed on each video frame by hidden data that does not visually change the image. Xuping Hunh et al.,[13] designed and implemented a synchronised audio to audio steganography scheme for acoustic data by recording the secret data, embed it and sent to multiple receivers. Only the trusted receiver can extract the secret data using a shared secret key. Se-min kim et al., [14] described a steganographic scheme based on index-colour image which is applied in internet environment to hide 1 to 8 bits secret data per pixel with no distortion if number of colours are within 128. The secret data is divided into several parts based on number of colours in the cover image and then secret data is embedded in the cover image. Rasul Enayatifar et al.,[15] proposed a method for image steganography using the chaotic map in which two chaotic signals specify the location of different parts of the message in the picture. Shen Wang et al.,[16] proposed steganography method based on genetic algorithm. The secret image is embedded in LSB of the cover image and the pixel values of the stegimage are modified by the genetic algorithm to keep their statistic characters. Min-Wen Chao et al.,[17] presented a high capacity and low distortion 3D steganography technique based on multilayered embedding scheme to hide secret messages in the vertices of 3D polygon models.

3. MODEL

In this section evaluation parameters and proposed embedding and retrieval techniques are discussed.

3.1 Evaluation Parameters3.1.1 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 and is calculated using Equation 1.

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

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

3.1.2 Peak Signal to Noise Ratio (PSNR): It is the measure of quality of the image by comparing the cover image with the stego image, i.e., it measures the statistical difference between the cover and stego image, is calculated using Equation 2.

$$PSNR = 10\log_{10}\frac{255^2}{MSE}db \quad (2)$$

3.1.3 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 the Hiding Capacity (HC) in terms of percentage.

3.2 Proposed Embedding Technique
The cover image LSBs are replaced by all bits or only MSBs of payload directly in traditional steganography. The LSB steganalysis attacks such as chi-square [18] and pair of values [19] can be used to hack payload easily. The proposed algorithm use non LSB and non transform domain steganography. The stego image is obtained by multiplying cover image with transformation matrix H_T derived from identity matrix and payload bit pair to avoid easy hacking of payload and flow chart of the process is shown in Figure 1.

3.2.1: Cover Image: The carrier of secrete information is the cover image. The different size and formats of cover images are considered to test the algorithm.

3.2.2: Payload: The images of different size and formats are considered as secrete information to be embedded into the cover image to generate stego image which is communicated to destination. Payload pixels are arranged column-wise and the pixel values are converted into binary.

3.2.3: Segmentation

Cover image is divided into blocks of size 2∗2.

$$X = \begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{bmatrix}$$

The block is checked for unique rows. If the rows are same, then one of the elements is changed to get unique rows.

3.2.4: Threshold
Adjacent pixel intensity differences are considered i.e., $x_{11} - x_{12}$, $x_{11} - x_{21}$, $x_{21} - x_{22}$. The difference is pre-fixed according to the quality of the stego image and is denoted as *threshold* Δ. The adjacent pixel intensity differences shouldn't exceed Δ. If one of the differences exceeds the pre-fixed difference, then the sub matrix block is not considered for embedding payload. Threshold condition is used to choose blocks that do not fall in region where there is sharp change in pixel intensity. This reduces distortions in regions of sharp pixel intensity variation.

3.2.5: Transformation
Transformation Matrix H_T is derived from the identity matrix H = $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ based on the payload bit pair using the conditions

(i) If the payload bit pair is (0,0), then there is no shift in H to obtain,

$$H_T = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

(ii) If payload bit pair is (0,1), no change in first row but the second row is shifted one place right in H to get

$$H_T = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$$

(iii) If the payload bit pair is (1,0), then the first row is shifted one place right and no change in second row in H to obtain

$$H_T = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$$

(iv) If the payload bit pair is (1,1), then both rows of H are shifted to get

$$H_T = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

3.2.6: Multiplier
Multiply H_T with 2 ∗ 2cover image matrix say X=$\begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{bmatrix}$ to result in stego matrix, Y = H_TX.

Let 2∗2 cover image block be X = $\begin{bmatrix} 128 & 127 \\ 125 & 128 \end{bmatrix}$

Case (i): If the payload bit pair is (0, 0), then the resulting stego matrix is

$$Y = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 128 & 127 \\ 125 & 128 \end{bmatrix} = \begin{bmatrix} 128 & 127 \\ 125 & 128 \end{bmatrix}$$

The stego image matrix is same as cover image matrix and rows are not identical.

$$Y = \begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{bmatrix}$$

Case(ii): If the payload bit pair is (0, 1), then the resulting stego matrix is

$$Y = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 128 & 127 \\ 125 & 128 \end{bmatrix} = \begin{bmatrix} 128 & 127 \\ 128 & 127 \end{bmatrix}$$

The rows are identical in Stego matrix and same as the first row of cover image X,

$$Y = \begin{bmatrix} x_{11} & x_{12} \\ x_{11} & x_{12} \end{bmatrix}$$

Case (iii)If the payload bit pair is (1,0), then the resulting stego matrix

$$Y = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 128 & 127 \\ 125 & 128 \end{bmatrix} = \begin{bmatrix} 125 & 128 \\ 125 & 128 \end{bmatrix}$$

The rows are identical in Stego matrix and same as the second row of cover image X,

$$Y = \begin{bmatrix} x_{21} & x_{22} \\ x_{21} & x_{22} \end{bmatrix}$$

Case (iv): If the payload bit pair is (1, 1), then resulting stego matrix is

$$Y = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 128 & 127 \\ 125 & 128 \end{bmatrix} = \begin{bmatrix} 125 & 128 \\ 128 & 127 \end{bmatrix}$$

The rows of cover image are interchanged in the stego matrix and rows are not identical.

$$Y = \begin{bmatrix} x_{21} & x_{22} \\ x_{11} & x_{12} \end{bmatrix}$$

3.2.6: Key: First bit of the bit pair is taken as key which is used for payload extraction at the destination without having Cover Image reference.

3.3: Payload Extraction

The retrieval of payload from stego image is given in the Figure 2.

3.3.1: Stego Image (SI): The image received at the destination from which the secret information is retrieved using reverse process of embedding technique.

3.3.2: Segmentation**:** Stego image is divided into blocks of 2∗2 sizes.

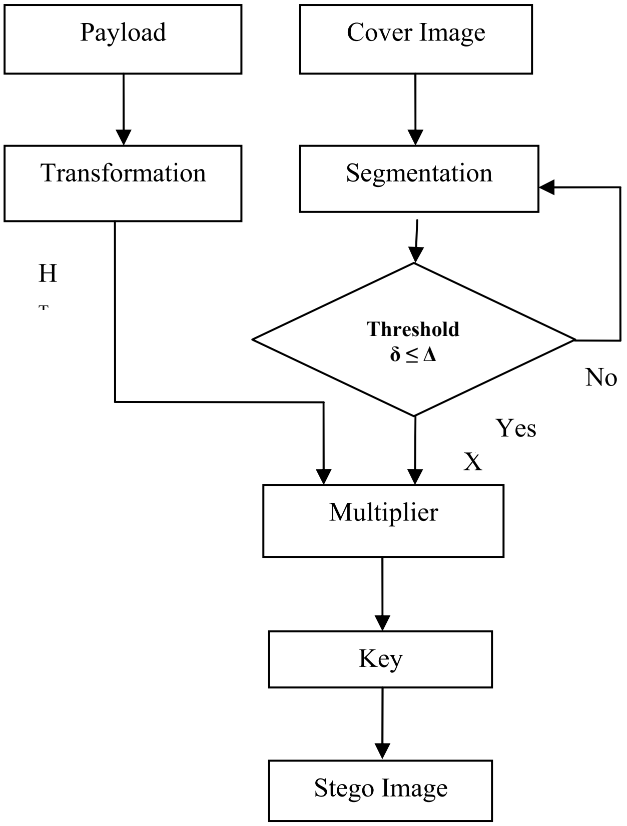

Figure1: Flow Chart of SPT Embedding Process

3.3.3: Threshold: Adjacent pixel differences do not exceed the threshold condition; hence we can use the same conditions as were used in embedding part to identify the cells that were used for embedding.

3.3.4: Key: Each 2∗2 stego-matrix block is associated with a key which is used for extracting bits. First element of the key corresponds to the first 2∗2 stego-matrix block; ith element of key corresponds to the ith2∗2 stego-matrix block. Using the key and by observing the patterns of rows, the bits embedded are extracted.

3.3.5: Matrix Check

- When (0,0) or (1,1) is hidden, the first row of the cell(r_s^1) is different from second row(r_s^2). When receiver observes it, he will have an ambiguity as to (0,0) or (1,1) was embedded. This ambiguity is resolved by taking into account the key corresponding to that block. If the key is 0, then (0,0) was embedded and hence the bits extracted are (0,0). If the key is 1, then the bits embedded were (1,1) and hence the extracted bits are (1,1).

- When (0,1) or (1,0) is embedded, rows of 2×2 stego-image block are identical. Again, the ambiguity is resolved by taking into account the key-element corresponding to that cell. If it is 0, then the bits embedded were (0,1) and hence the extracted bits will be (0,1). If key-element is 1, then the bits embedded were (1,0) and hence the extracted bits are (1,0).

- The extracted bits are arranged in proper order and converted into unsigned integer form to extract payload.

4. ALGORITHM

The embedding and retrieval of payload using SPT algorithm is discussed in this section.

Problem definition: Given cover image and the payload, the objectives are:

1. To embed the payload into the cover image to derive stego image.
2. High robustness with reasonable PSNR.
3. Reasonable capacity with different cover and payload image formats

Assumptions:

1. Noisy channel
2. The stego image is distressed by LSB attack.

4.1 Embedding Algorithm

The payload is embedded into the cover image using non-LSB technique. Cover Image is segmented and modulated in accordance with the payload and the algorithm is given in Table 1

4.2 Extraction Algorithm

The payload is extracted from the stego image by adapting reverse process of embedding using the key received at the destination and the algorithm is given in Table 2.

Table 1: Embedding Algorithm of SPT

Input: Cover image, Payload,
Output: Stego Image

1. Divide the cover image into blocks of size 2×2.
2. Consider a 2×2 block at a time for embedding.
3. If the rows of the block are identical, then change one of the elements; else go to step 4.
4. If the adjacent pixel differences are more than threshold value, drop that block and go next block
5. Consider a bit pair (b_1, b2) of payload and identity matrix H.
6. If the first bit of payload bit pair is zero, then the first row of H is not changed in H_T else the elements of the first row are interchanged in H_T.
7. If the second bit of payload bit pair is zero, then the second row of H is not changed in H_T else the elements of the second row are interchanged in the H_T.
8. The matrix H_T is multiplied with the 2×2 valid cover image block to get stego image block.
9. First bit of bit-pair is considered as key for payload extraction at the destination.

Table 2: Extraction Algorithm for SPT

Input: Stego image
Output: Payload

1. Divide the stego image into blocks of size 2×2 blocks.
2. Access one block at a time.
3. Check the adjacent pixel differences. If it is more than threshold, drop that block and go to next block.
4. Access the key corresponding to that block.
5. If the rows are not identical and the key is 0, then the bits extracted are (0, 0).
6. If the rows are not identical and the key is 1, then the bits extracted are (1, 1).
7. If the rows are identical and key is 0, the bits extracted are (0,1).
8. If the rows are identical and key is 1, the bits extracted are (1,0).
9. Construct the payload with bits extracted

5. PERFORMANCE ANALYSIS

Cover images of different sizes and formats viz., JPEG, BMP, TIF and PNG are considered for performance analysis are as shown in the Figure 3. Both cover image and payload considered are grey scale images.

Performance is analysed using PSNR, capacity and robustness

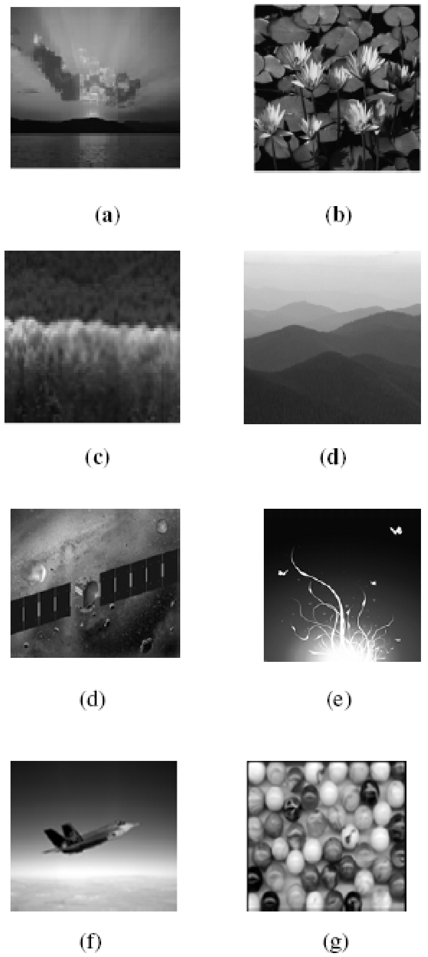

Fig. 3: (a) Sunset (b) Water Lilies (c) Winter (d) Blue Hill (e) Satellite (f) Art (g) jet (h) Marbles

The payload of around 4 kilo bytes of data can be hidden in a cover image of size 350×350 to generate stegoimage of good quality with PSNR of around 40dB.The first three LSBs of stego image are manipulated to introduce noise for the verification of robustness.

The increase in the value of threshold marks more number of sub matrices of Cover Image (CI) to be used for embedding the payload (PL) which increases distortion in the region where sharp intensity variations in the pixels results in (i) high MSE results in low PSNR for CI and SI and (ii)low MSE results in high PSNR for PL and Extracted Payload (EPL)is shown in the Figure 4.

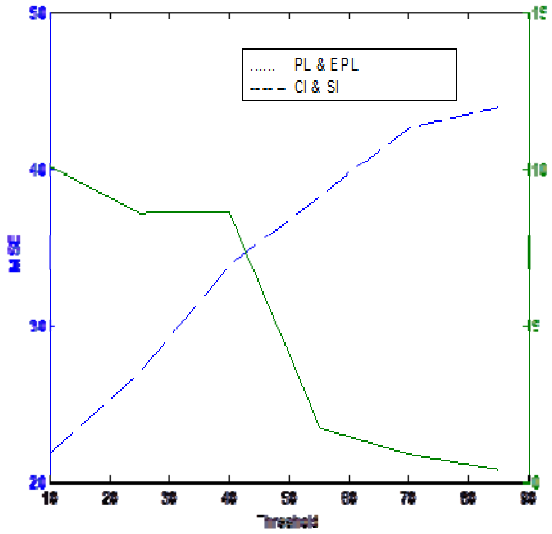

Fig.4: The variation of MSE with Threshold

Table 3: PSNR between Pl and EPL with and without noise

Images	HC (bpp)	PSNR (Without Noise)	PSNR (With Noise)
CI-Sunset PL-water lilies (JPEG)	**0.27**	**38.89**	**37.91**
CI-Lena PL-Jet (BMP)	**0.27**	**39.23**	**38.12**
CI-Marbles PL-Satellite (TIFF)	**0.27**	**38.82**	**37.90**
CI-Art PL-Logo (PNG)	**0.27**	**38.55**	**37.57**

The PSNR of EPL from stego image corrupted by noise and possible intruder attack is almost same as EPL from stego image without noise and has reasonable PSNR which proves the algorithm is robust for an attack is given in the Table 3 for different image formats. The algorithm is secure because (i) the key is used to extract payload from a particular stego image and is payload dependent, hence it is less susceptible to hacking and (ii) the threshold is known only between sender and receiver. The existing Chaos based Spatial Domain Steganography using MSB (CSDS) algorithm [20] is compared with the proposed SPT algorithm in terms of PSNR for 0.27 bpp capacity is given in the Table 4. The value of PSNR is better in the case of proposed algorithm compared to the existing algorithm.

Table 4: PSNR between CI and SI for existing CSDS and proposed algorithms

Images	HC (bpp)	CSDS PSNR (db)	SPT PSNR (db)
CI-Sunset PL-water lilies (JPEG)	**0.27**	**41.13**	**42.02**
CI-Lena PL-Jet (BMP)	**0.27**	**40.91**	**42.23**
CI-Marbles PL-Satellite (TIFF)	**0.27**	**41.53**	**42.12**
CI-Art PL-Logo (PNG)	**0.27**	**40.37**	**41.76**

6. CONCLUSIONS

The covert communication over public channel by hiding a secret message from unauthorized persons is the aim of steganography. In this paper SPT algorithm is proposed. The payload pixels are converted into binary and while embedding, two bits are considered at a time. Based on payload bit pair and identity matrix, the transformation matrix $H_{T.}$ is obtained. The cover image is converted into 2*2 cells and adjacent pixel intensity values are computed to fix threshold value in order to decide valid 2*2 cells. By multiplying H_T with valid cover image matrix, the stego image matrix is obtained. At the destination, the payload is extracted by adopting reverse process of embedding technique. It is observed that with acceptable PSNR and capacity, security has improved. Compared to existing algorithms.

REFERENCES

[1] Nan-I Wu and Min-Shiang Hwang, “Data Hiding: Current Status and Key Issues,” *International Journal of Network Security*, vol.4, no.1, pp. 1-9, January 2007

[2] C Cachin, “An Information-Theoretic Model for Steganography,” Journal Information and Computation, vol.192, no.1, pp.41-56, 2004

[3] Neil F Johnson and SushilJajodia, “Steganalysis: The Investigation of Hidden Information,” *Proceedings of IEEE International Conference on Information Technology*, pp. 113-116, September 1998.

[4] İsmail Avcıbaş, Mehdi Kharrazi, NasirMemon and BülentSankur, “Image Steganalysis with Binary Similarity Measures,” EURASIP Journal on Applied Signal Processing, pp. 2794-2757, 2005

[5] Yong WANG, Qichang HE, Huadeng WANG, Bo YIN and Shaoling DING, “Steganographic Method Based on Keyword Shift,” Information Management and Engineering (ICIME), pp. 454-456, 2010

[6] Hironori Takimoto, Seiki Yoshimori and Yasue Mitsukura “Invisible Calibration Pattern based on Human Visual Perception,” 20th International Conference on Pattern Recognition (ICPR), pp. 4210-4213, 2010

[7] Yifeng Sun and Fenlin Liu, “Selecting Cover for Image Steganography by Correlation Coefficient,” International Workshop on Education Technology and Computer Science, pp. 159-162, 2010

[8] Vijay Kumar and Dinesh Kumar, “Performance Evaluation of DWT Based Image Steganography,” International Advance Computing Conference (IACC), pp. 223-228, 2010

[9] Che Lun Pan, Jeanne Chen, Tung Shou Chen, Rong-Chang Chen and Wan Yi Ji , “Lossless Embedding Using Difference Between Sub-Sampled Images,” International Conference on Education Technology and Computer(ICETC) , pp. 124-127, 2010

[10] M Jayachandran and J Manikandan, “SAR Image Compression using Steganogrphy,” International Conference on Advances in Computer Engineering, pp. 203-206, 2010

[11] Manish Mahajan and Akashdeep Sharma, “Steganography in Colored Images Using Information Reflector with 2^k Correction,” International journal of Computer Applications, pp. 53-59, 2010

[12] Mohamed Elsadig, Miss Laiha Mat Kiah, Bilal Bahaa Zaidan and Aos Alaa Zaidan, “High Rate Video Streaming Steganography,” International Conference on Management and Engineering, pp. 550-553, 2009

[13] Xuping Huang, Ryota Kawashima, Norihisa Segawa and Yoshihiko Abe, “Design and Implementation of Synchronized Audio-To-Audio Steganography Scheme,” International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 331-334, 2008

[14] Se-Min Kim,Ziqiang Cheng and Kee-Young Yoo, “A New Steganography Scheme based on an Indexe-colour Image,” International Conference on Information Technology: New GEnerations, pp. 376-381, 2009

[15] Rasul Enayatifar, Saed Faridnia and Hossein Sadeghi “Using the Chaotic Map in Image Steganography,” International Conference on Signal processing Systems, pp. 754-756, 2009

[16] Shen Wang, Bian Yang and Xiamu Niu “A Secure Steganography Method based on Genetic Algorithm,”

Journal of Information Hiding and Multimedia Signal Processing, Vol 1 , pp. 28-35, 2009

[17] Min-Wen Chao, Chao-hung Lin, Cheng-Wei and Tong-Yee Lee, “A High Capacity 3D Steganography Algorithm,” *IEEE Transactions on Visualization and Computer Graphics*, vol 15, No 2, pp. 274-283, 2009.

[18] Hong-Juan Zhang and Hong-Jun Tang, “A Novel Image Steganography Algorithm against Statistical Analysis,” *IEEE International Conference on Machine Learning and Cybernetics*, pp. 3884-3888, 2007.

[19] K B Raja, Lavu Rohita, Rekha S, Swetha P V, Venugopal K R, L M Patnaik, “LSB Steganalysis to Detect the Embedded Message Length Using Pixel Pair Threshold,” *Fifteenth International Conference on Advanced computing and Communications*, pp. 765-770, 2007.

[20] N Sathisha, Madhusudan G N, Bharathesh S, K Suresh Babu, K B Raja, Venugopal K R, “Chaos based Spatial Domain Steganography using MSB,” *Fifth IEEE International Conference on Industrial and Information Systems*, NITK, Surathkal, 2010.

ShivaKumar K B received the BE degree in Electronics & Communication Engineering, ME degree in Electronics, MBA from Bangalore University, Bangalore and MPhil from Dravidian University Kuppam. He is pursuing his Ph.D. in Information and Communication Technology of Fakir Mohan University, Balasore, Orissa under the guidance of Dr. K. B. Raja, Assistant Professor, Department of Electronics and Communication Engineering, University Visvesvaraya College of Engineering, Dr.Sabyasachi Pattanaik Reader & HOD, Department of Information and Communication Technology F M University, Balasore, Orissa R K Chhotaray, Principal, Seemantha Engineering College, Orissa. He has got 27 years of teaching experience and has over 25 research publications in National and International conferences and journals. Currently he is working as Professor, Dept. of Telecommunication Engineering, Sri Siddhartha Institute of Technology, Tumkur. His research interests include Signal processing, Multi rate systems and filter bags, and Steganography.

Dr. K B Raja is an Assistant 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 has been awarded Ph.D. in Computer Science and Engineering from Bangalore University. He has got 25 years of teaching experience and he has over 60 research publications in refereed International Journals and Conference Proceedings. Currently he is guiding 10 Ph D scholars in the field of image processing. He has received Best Paper Award for the contributed paper in Fourteenth IEEE-ADCOM 2006. His research interests include Image Processing, Biometrics, VLSI Signal Processing and computer networks.

Dr. Sabyasachi Pattnaik has done his B.E in Computer Science, M Tech., from IIT Delhi. He has received his Ph D degree in Computer Science in the year 2003 & now working as Reader in the Department of Information and Communication Technology, in Fakir Mohan University, Vyasavihar, Balasore, and Orissa, India. He has got 20 years of teaching and research experience in the field of neural networks, soft computing techniques. He has got 50 publications in national & international journals and conferences. He has published three books in office automation, object oriented programming using C++ and artificial intelligence. At present he is involved in guiding 8 Ph D scholars in the field of neural networks, cluster analysis, bio-informatics, computer vision & stock market applications. He has received the best paper award & gold medal from Orissa Engineering congress in 1992 and institution of Engineers in 2009.

Dr. R K Chhotaray received B.Sc Engineering in Electrical Engineering and M.Sc Engineering in Electrical Engineering with specialization in Control Systems from Banaras Hindu University, and Ph D in Control Systems from Sambalpur University. He was Professor and Head of Department of Computer Science and Engineering, Regional Engineering College, Rourkela, from which he retired in 2003. Currently he is working as Principal of Seemanta Engineering College, Orissa. He has been associated with many Universities of India in the capacity of Chairman and member of various Boards of Studies, syllabus committee, and Regulation committee. He has about hundred publications in International and National journals of repute, and has received Best Technical Paper award in many occasions. His special fields of interest include Control of Infinite dimensional Hereditary Systems, Modeling and Simulation, Theoretical Computer science, signal and Image processing, and optimization.