Volume 8 • Issue 6 • November 2014

Editor-in-Chief
Dr. Chen-Chi Shing

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND SECURITY (IJCSS)

ISSN : 1985-1553

Publication Frequency: 6 Issues / Year

CSC PUBLISHERS
http://www.cscjournals.org

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND SECURITY (IJCSS)

VOLUME 8, ISSUE 6, 2014

EDITED BY
DR. NABEEL TAHIR

ISSN (Online): 1985-1553

International Journal of Computer Science and Security is published both in traditional paper form and in Internet. This journal is published at the website http://www.cscjournals.org, maintained by Computer Science Journals (CSC Journals), Malaysia.

IJCSS Journal is a part of CSC Publishers
Computer Science Journals
http://www.cscjournals.org

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND SECURITY (IJCSS)

Book: Volume 8, Issue 6, November 2014
Publishing Date: 10-11-2014
ISSN (Online): 1985 -1553

IJCSS Journal is a part of CSC Publishers
http://www.cscjournals.org

Published in Malaysia

Typesetting: Camera-ready by author, data conversation by CSC Publishing Services – CSC Journals, Malaysia

CSC Publishers, 2014

EDITORIAL PREFACE

This is *Sixth* Issue of Volume *Eight* of the International Journal of Computer Science and Security (IJCSS). IJCSS is an International refereed journal for publication of current research in computer science and computer security technologies. IJCSS publishes research papers dealing primarily with the technological aspects of computer science in general and computer security in particular. Publications of IJCSS are beneficial for researchers, academics, scholars, advanced students, practitioners, and those seeking an update on current experience, state of the art research theories and future prospects in relation to computer science in general but specific to computer security studies. Some important topics cover by IJCSS are databases, electronic commerce, multimedia, bioinformatics, signal processing, image processing, access control, computer security, cryptography, communications and data security, etc.

The initial efforts helped to shape the editorial policy and to sharpen the focus of the journal. Started with Volume 8, 2014, IJCSS appears with more focused issues. Besides normal publications, IJCSS intend to organized special issues on more focused topics. Each special issue will have a designated editor (editors) – either member of the editorial board or another recognized specialist in the respective field.

This journal publishes new dissertations and state of the art research to target its readership that not only includes researchers, industrialists and scientist but also advanced students and practitioners. The aim of IJCSS is to publish research which is not only technically proficient, but contains innovation or information for our international readers. In order to position IJCSS as one of the top International journal in computer science and security, a group of highly valuable and senior International scholars are serving its Editorial Board who ensures that each issue must publish qualitative research articles from International research communities relevant to Computer science and security fields.

IJCSS editors understand that how much it is important for authors and researchers to have their work published with a minimum delay after submission of their papers. They also strongly believe that the direct communication between the editors and authors are important for the welfare, quality and wellbeing of the Journal and its readers. Therefore, all activities from paper submission to paper publication are controlled through electronic systems that include electronic submission, editorial panel and review system that ensures rapid decision with least delays in the publication processes.

To build its international reputation, we are disseminating the publication information through Google Books, Google Scholar, Directory of Open Access Journals (DOAJ), Open J Gate, ScientificCommons, Docstoc and many more. Our International Editors are working on establishing ISI listing and a good impact factor for IJCSS. We would like to remind you that the success of our journal depends directly on the number of quality articles submitted for review. Accordingly, we would like to request your participation by submitting quality manuscripts for review and encouraging your colleagues to submit quality manuscripts for review. One of the great benefits we can provide to our prospective authors is the mentoring nature of our review process. IJCSS provides authors with high quality, helpful reviews that are shaped to assist authors in improving their manuscripts.

Editorial Board Members
International Journal of Computer Science and Security (IJCSS)

EDITORIAL BOARD

EDITOR-in-CHIEF (EiC)

ASSOCIATE EDITORS (AEiCs)

EDITORIAL BOARD MEMBERS (EBMs)

Assistant Professor Vishal Bharti
Maharishi Dayanand University
India

Dr. Parvinder Singh
University of Sc. & Tech
India

Assistant Professor Vishal Bharti
Maharishi Dayanand University,
India

TABLE OF CONTENTS

Volume 8, Issue 6, November 2014

Pages

201 - 215 An Image Steganography Algorithm Using Huffman and Interpixel Difference Encoding
Nithyanandam Pandian

An Image Steganography Algorithm Using Huffman and Interpixel Difference Encoding

Nithyanandam Pandian *nithyanandam.p@vit.ac.in*
Professor, School of Computing Science and Engineering,
VIT University, Chennai Campus,
Kanchipuram Dt. 600127,India

Abstract

Steganography is an art of hiding secret information on a cover medium through imperceptible methodology. The three pillars on which a steganography algorithm should be erected are: Embedding capacity, Imperceptibility and Robustness. It is fortunate that all these goals are interdependent on one another. The state of art is finding an optimum solution that keep up all the steganography goals. It is believed that there is no productivity if the size of cover medium gets extended to meet in housing the secret data on it. This happens due to lack in refinement of embedding algorithm and failing in analyzing the data structure of secret data. In this paper, an attempt has made to improve embedding capacity and bring very less distortion to the cover medium by analyzing the data structure of the payload. A residual coding is carried on the pay load before it is submitted to Huffman encoding which is a lossless compression technique. As a result, the representation of payload had shrink. Further, the variable bit encoding (Huffman) do a lossless compression and finally the payload get housed on the cover medium. This ended with high embedding capacity and less imperceptibility. Peak signal to noise ratio confirms that the residual coding had given improvised results than few existing embedding algorithm.

Keywords: Steganography, Huffman Encoding, Peak Signal To Noise Ratio, Residual Coding, Distortion, Redundancy.

1. INTRODUCTION

Steganoraphy is a hidden communication technique, in which the event of communication taking place itself is concealed. The cover medium suitable for steganography can be any entity which can be digitally represented [2]. Steganography technique remains successful, until the artifacts of the cover medium remains intact. Ruining the cover image artifact while payload embedding is inevitable. But the artifact of the cover image can be retained to a possible extent, if the adulteration get introduced on the cover image is minimum during the payload get embedded on it. Improving embedding capacity and minimizing the distortion occurring to the cover image stands tradeoff. It is wiser to minimize the number (count) of distortion rather than controlling the occurrence of distortion. The net effect is that the overall distortion occurring to the cover image can be brought down. Despite of using lossless compression technique such as Huffman coding on the payload prior to embedding, sometime still our payload cannot be housed in the cover image. This conveys us not only to increase the size of cover image that is big enough to hold payload but also in the other direction of viewing the statistical structure of payload (secret data/image). In general most representation of any information has huge volume of redundancy [1][9]. This redundancy can exist in several forms such as spatially adjacent pixels in an image are too close in their intensities too. This is a breakthrough where one can exploit the property of Interpixel redundancy to make an attempt in implementing Interpixel differences as coding model for representing an image. This Interpixel difference coding will decrease the representation (file) size by the number of bits required to represent the image intensity. Since, we are going to code the Interpixel difference; the binary bit required will be lesser on an average. Exception exists in the boundary or edge region of an image where the Interpixel difference will be maximum. The Interpixel difference will be minimum for smooth region. Determining the Interpixel difference results in lesser magnitude of the pixel in contrast to the original intensity value. When these lesser magnitude symbols are fed as input to the variable bit encoding (Huffman) ,it ends up with better compression rate. In general, Huffman coding by itself compress the source symbols to an optimum extent ; but it is wise if the data structure characteristics of the payload is analysed prior to Huffman submission. This will help to carry out in calculating the Interpixel difference of the payload (secret image).

The objective of the proposed work is to embed a grayscale secret image on a 24 bit RGB cover image using various coding technique. The Interpixel difference computed secret image is submitted to Huffman encoding technique results in supporting higher embedding capacity and peak signal to noise ratio. The rest of the paper is organized as follows: Section 2 discusses the background study, Section 3 covers the related works. The proposed work is exhibited in Section 4, experimental results and discussions were given in Section 5. Finally, the concluding remark and future direction are given.

2. BACKGROUND STUDY

2.1 Interpixel Differencing

Interpixel differerencing technique is used in conjunction with Huffman coding to achieve higher data compression. Increasing the cover medium size to house the secret data on it should be the secondary option. If there is scope to determine the redundancy and eliminate the same with alternative representation technique, then the need of searching a big cover image to house the secret data can be avoided. One such attempt has been taken in the proposed work. For example consider intensity value of very small portion of an image as shown in figure1.

187	170	170	153	170	170	187	153	153	170
170	170	170	153	170	170	170	153	153	170
187	136	170	187	153	170	170	153	153	153
170	136	170	170	170	170	170	187	187	170
170	136	153	170	153	153	170	187	170	170
170	153	170	170	187	136	136	170	170	187
170	170	170	204	187	170	153	170	187	187
170	170	170	187	204	170	187	204	170	187
170	170	153	170	170	170	187	204	170	153
153	153	153	153	153	153	187	170	187	187

FIGURE 1: A snapshot of an image intensity values.

To represent the above 10 ×10 image matrix we require 100 × 8 = 800 bits. If the matrix is directly Huffman coded, it ends up with a binary representation requirement of 850 bits. But in reality this image matrix will be in larger size, so we get better compression. But look in other dimension of the same matrix with respect to structural characteristics of it. Figure 2 shows the structural difference of the same matrix using Interpixel difference. In every row the first element remains the same, whereas i^{th} element is the difference between i^{th} pixel and $i\text{-}1^{th}$ pixel and i >0.

187	-17	0	-17	17	0	17	-34	0	17
170	0	0	-17	17	0	0	-17	0	17
187	-51	34	17	-34	17	0	-17	0	0
170	-34	34	0	0	0	0	17	0	-17
170	-34	17	17	-17	0	17	17	-17	0
170	-17	17	0	17	-51	0	34	0	17
170	0	0	34	-17	-17	-17	17	17	0
170	0	0	17	17	-34	17	17	-34	-17
170	0	-17	17	0	0	17	17	-34	-17
153	0	0	0	0	0	34	-17	17	0

FIGURE 2: Interpixel Difference Value of image intensity.

When the Interpixel difference matrix that is Fig.2 is fed as input matrix to Huffman encoding, it ends up with a binary representation requirement of 566 bits. When we apply the same to a larger scale there is scope to achieve better compression and this attempt has been carried out in the proposed work. The Interpixel difference matrix is reversible. Every rows first element of the Interpixel difference matrix is used as initial value and successively the rest of the elements is computed by referring the preceding value. Here ith element of every row is the Interpixel summation of ith pixel and i-1th pixel and i >0. The number of unique symbols (counts) in the Interpixel difference image (refer Fig.2) is more than original image (refer Fig.1). For some cases even it may be lesser i.e. Interpixel difference image has lesser symbol than original image. But the net effect is that, when Interpixel differencing technique is applied on an image for compression, it results in doing the compression with lesser number of bits. The bit rate is 5.66/pixel in the case of Interpixel difference technique. This include both the Huffman table and Huffman Encoding.

2.2 Huffman Encoding

Huffman encoding [1][10][11] is a variable length lossless compression technique that can exactly reproduce the source data. Entropy of source symbol is given in equation 1.

$$\boldsymbol{H(s) = -\sum_{i=1}^{m} p(a_i)\, log_2 p(a_i)} \qquad \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots(\mathbf{1})$$

where i=1-m, a$_i$ are various symbols in the source. Average length of any variable coding technique is given in equation 2.

$$\boldsymbol{l = \sum_{i=1}^{m} p(a_i)\, n(a_i)} \qquad \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots..(\mathbf{2})$$

where n(a$_i$) is the number of bits in the codeword for symbol a$_i$ and the average length is given in in bits/symbol. In an image, unique pixel intensities were considered as different symbols. The symbols vary from 0- 255. 0 denotes minimum and 255 denotes maximum intensity. The intensity of the pixels across the image is spatially correlated [1][9]. Information is pointlessly repeated in the representation of the correlated pixels. These repetitive pixels should also be represented by fixed number of bits in unencoded Huffman format. Actually these values are the best source for exploiting compression. Frequently occurred intensity value can be represented by variable numbers of bits (i.e. shorter bits) in contrast to the fixed number of bits for representing the pixel intensity used in unencoded Huffman technique. This is the core concept of Huffman encoding technique.

Huffman encoding give compressed coding for the symbols provided as input. Huffman table has prefix free codes and corresponding symbols. Huffman table is used during Huffman decoding. Both the Huffman encoded prefix free binary code and Huffman table should be treated as payload and embedded in cover medium. The compression ratio depends on the count of the unique symbols and their frequencies. Lesser the symbol and higher the frequency results in higher compression, in contrast higher the symbols with less frequency results in lower compression. This is common in both text and image compression. Generally if the symbol count increases, this in turn influences the size of Huffman table. As a result the Huffman table entries get increased, which has impact on the compression ratio. Huffman table is an additional overhead in Huffman encoding technique.

3. RELATED WORKS

A stenographic technique proposed in [12] which is based on LSB replacement technique. Varying lengths of secret bits get embedded in every pixel. In method1 green and blue are embedding channels keeping red channel as indicator channel. In method2 an option is provided for choosing the indicator channel among the three channels. Once chosen, the remaining two channel act as embedding channel. In method3 the indicator channel is chosen by rotation scheme across all the pixels. In the first pixel red channel is indicator; green channel is the indicator in second pixel and in third channel blue act as indicator. Once indicator is finalized the remaining two channels will be used for embedding. This scheme is repeated for the consecutive pixels. The Mean Square Error (MSE) and PSNR is calculated for all channel and the average number of bits get embedded in every pixel is shown in their results.

A stenographic technique proposed in [7] is based on edge adaptive scheme. The absolute difference between two adjacent pixels are the primary criteria in identifying the region for embedding secret message. They use LSBMR (Least Significant Bit Matching Revisited) as their data hiding algorithm. Only 2 secret bits can be embedded in each embedding unit and threshold T is used in identifying the embedding region. Region selection and cover image hiding capacity is determined through trial and error process. The sharper edge regions of cover image alone are used for embedding. Even though the embedding capacity is lesser it withstand against statistical attack and they had proved that RS steganalysis is ineffective in detecting stego work.

In the steganography scheme adopted in [13], the embedding efficiency is improved by adopting matrix embedding method. ME-RA (matrix embedding repeat accumulate) is the data hiding algorithm used to hide the secret data. The reason to choose matrix embedding is to less adulterate the cover image, at the same time the secret data bits should get embedded. Here, a hamming code matrix is employed in attaining the goal. In the proposed work, instead of hamming code (for matrix embedding) a simple XOR operation is performed on the host image bits to check its coincidence against the secret bits. The host image bit is adjusted accordingly to suit the secret bits.

A novel image steganography technique [14] was discussed in which the cover image's spatial value is transformed in to Discrete Cosine Transformation (DCT); its LSB is modified to match the secret message. The secret message is Huffman encoded prior to the embedding scheme which achieves a significant compression rate. A higher embedding capacity and PSNR is obtained using this technique. This technique is superior to the method proposed in [16].

A stenographic technique [15] based on wavelet transformation on the images is proposed. Discrete Wavelet Transformation (DWT) converts the spatial domain of cover image into frequency domain. Huffman compression is applied for the stream of secret bits before overlaying them on the cover image. A high PSNR and very high embedding capacity is achieved. A higher level of security is obtained because the Huffman table and encoding rules are black box to the intruder.

A Least Significant Bit [17] steganographic scheme technique in which the secret image is bit plane coded, runlength encoded and finally Huffman compressed yielded a high embedding capacity. The payload (secret image) get embedded is just 4 bits out of every 8 bit pixels. Remaining 4 bits of every pixel is artificially constructed in the destination during the process of making the secret image from the stego image. The secret image retrieved in the destination is a lossy one, but sill PSNR above 30dB is acceptable.

4. PROPOSED METHOD

Interpixel redundancy is a very basic fact exists in any image. If the Interpixel differences are recorded for representing the intensities of every pixel, it could result in exhibiting a smaller magnitude. Huffman encoding take the full advantage of the Interpixel redundancy value and perform encoding for the same. The net effect is that, the obtained payload compression ratio is high. This is experimentally proved through simulation result. This is the central theme behind the proposed work. Least significant bit embedding and matrix embedding are the two spatial domain steganography embedding algorithm used in the proposed method.

4.1 Least Significant Embedding

Least Bit (LSB) embedding [4][5][6][19][20][21][22] is one of the renowned spatial domain steganography techniques. The process of LSB embedding carried on a cover medium is explained below.Suppose we want to encode the letter A (**ASCII 65 or binary 01000001**) in the following 8 bytes (pixel intensities) of an image cover medium, it can be done as follows:

93	**208**	**28**	**172**	**231**	**135**	**107**	**227**
01011101	11010000	00011100	10101100	11100111	10000111	01101011	11100011
becomes							
92	**209**	**28**	**172**	**230**	**134**	**106**	**227**
0101110**0**	1101000**1**	0001110**0**	1010110**0**	1110011**0**	1000011**0**	0110101**0**	1110001**1**

4.2 Matrix Embedding

In matrix embedding[3][8][13] technique, the LSB's of all the channels of every pixels are taken to embed two bits of secret image.

4.2.1 Embedding

To encode bit b1 and b2 in the LSB of three channels of a pixel: say X1, X2 and X3. Equation3 must be satisfied.

$$\begin{aligned} b_1 &= \mathrm{LSB}(x_1) \oplus \mathrm{LSB}(x_2) \\ b_2 &= \mathrm{LSB}(x_2) \oplus \mathrm{LSB}(x_3) \end{aligned} \qquad \dots\dots\dots\dots.\dots.(3)$$

If equation3 is not satisfied, a minor modification will be done on $X_{1,}$ or X_2 or X_3 to satisfy the same. If the first one is satisfied but not the second one, simply flip the LSB of x3. If the second one is satisfied but not the first one, flip the LSB of x1. If neither is satisfied, flip LSB of x2.

4.2.2 Extraction

Every consecutive 3 bytes of stego image are extracted to construct 2 bits of secret image. This process is repeated until the required secret image bits are constructed. To extract bit b_1 and b_2 from LSB of three channels of a pixel: say X_1, X_2 and X_3 equation4 is applied on the stego image pixels.

$$\begin{aligned} \mathrm{LSB}(x_1) \oplus \mathrm{LSB}(x_2) &= b_1 \\ \mathrm{LSB}(x_2) \oplus \mathrm{LSB}(x_3) &= b_2 \end{aligned} \qquad \dots\dots\dots\dots.\dots..(4)$$

These collected bit streams are grouped and submitted for further operation of constructing the secret image.

4.3 Embedding Process

Figure 3 shows the embedding process carried on the sender side. After embedding the sender will send the cover image which has secret data (Image) embedded in it. The steps carried on the sender side are given below.

While computing Interpixel difference, preserve the 0th column of secret image as it is. For the rest of the element do the following process. Assume A is a secret image matrix and B is the resultant matrix, where the Interpixel difference are computed and stored. Refer Fig1 and Fig2 for understanding.

Step1: Compute Interpixel difference by subtraction: B(i,j) =A(i,j+1) – A(i,j) where i = 0-m-1 and j = 0- n-1. m and r are rows and column respectively. For every row B start at first column,since 0th column already preserved from A matrix. This means that index value of j for B matrix vary from 1-m, and i vary from 0-n.

Step2: Apply Huffman encoding for the output obtained from Step1 which results in Huffman table and Huffman encoded secret image bit streams.

Step3: Embed dimensions of secret image and the resultant component (Huffman table and Huffman encoded secret image bit streams) obtained from Step2 into the cover image using matrix/LSB embedding technique.

Step4: Send the stego image obtained from Step3 to the receiver.

4.4 Extraction Process

Figure 4 shows the extraction process carried on the receiver side. Upon receiving the stego image, the receiver should extract the Huffman table, Huffman encoded bit streams and secret image dimension from the stego image. The steps carried on the receiver side are given below.

Step 1: For retrieving the secret image's binary bits from the stego image, extract the LSB's from every pixel, apply matrix/LSB extraction technique and construct Huffman table and Huffman encodings using the LSB's bit streams.

Step 2: The Huffman table and Huffman encodings obtained in Step1 is used in Huffman decoding process.

Step 3: Finally to construct the secret image, reverse Interpixel difference process should be carried out on the Huffman decoded data. Assume Huffman decoded result as matrix B. Refer Fig.1 and Fig.2 for understanding. Reverse Interpixel calculation are carried out as follows:

a. To construct the secret_image matrix, 0th column can be directly taken from Huffman decoded result ,say matix B 0th column.
b. To construct other pixel, secret_image(i,j)= secret_image(I,j-1)+B(i,j). where i varies from 0-m-1 and j varies from 1 – n-1.

Step 4: At last,the image is constructed using all the pixels which will reveal the secret image.

The rate of adulteration between the cover matrix and stego matrix should be measured. To assess the distortion introduced by the proposed algorithm, objective measure phenomenon i.e. Peak Signal to Noise Ratio SNR (PSNR) and Mean Square Error (MSE) were used. Equation 5 and Equation 6 depict MSE and PSNR respectively.

$$MSE = \frac{1}{m * n}\sum_{i=1}^{m}\sum_{j=1}^{n}\left(A_{ij} - B_{ij}\right)^2 \qquad \dots\dots\dots(5)$$

where A_{ij} represents pixel in the cover image and B_{ij} represents pixel in the stego image; m, n represents the height and width of the image respectively.

$$PSNR = 10 * log_{10}\left(\frac{Max^2}{MSE}\right) \qquad \dots\dots\dots\dots(6)$$

here max denote maximum color intensity of grayscale(255). PSNR is measured in decibels (dB).

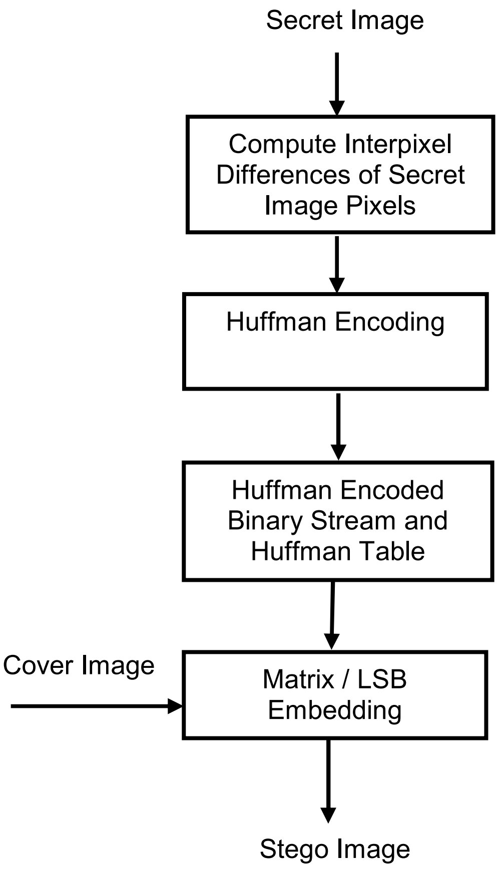
Secret Image
Compute Interpixel Differences of Secret Image Pixels
Huffman Encoding
Huffman Encoded Binary Stream and Huffman Table
Cover Image
Matrix / LSB Embedding
Stego Image

FIGURE 3: Embedding Process.

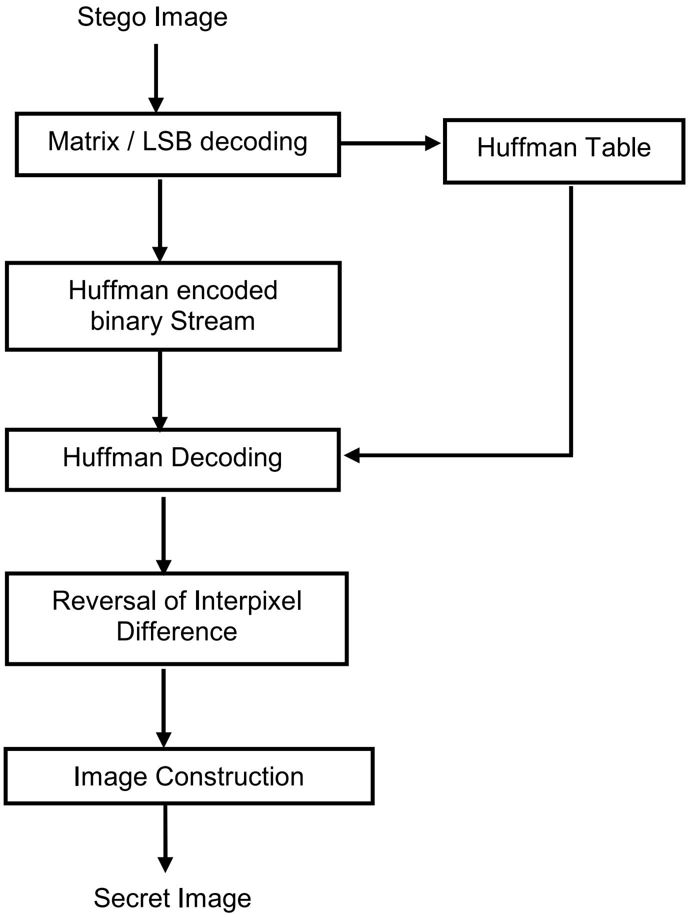

FIGURE 4: Extraction Process.

5. EXPERIMENTAL RESULTS

Java 2.0 and MATLAB R2009a are the programming tools used to implement the proposed method. Standard 24 bit cover images of size 256 x 256 such as Lena, Baboon, Gandhi and Temple were used. Fig. 5 shows the secret image and Fig 6a-6d shows the cover image Lena and its histogram of RGB channels before distortion. Fig 6e-6h shows the stego image Lena and its histogram of RGB channels after distortion using Least Significant Bit embedding technique. Fig 6i-6l shows the stego image Lena and its histogram of RGB channels after distortion using Matrix embedding technique. Similarly, Fig.7,Fig.8 and Fig.9 shows the results for the cover image Baboon, Gandhi and Temple respectively. PSNR and embedding Capacity are the metrics taken here to consolidate the strength of proposed method. Histogram of the stego image shows that the distortion between cover and stego image is minimum. Interpixel difference coding is used in the proposed to improve the performance of Huffman coding. The performance of Huffman encoding depends upon unique symbol present in the secret image. Here symbol refers to various unique pixel intensity or grayscale value. Table1 shows the experimental results of Method 3 of [12] (R.Amirtharajan et al., 2010). There is a significant improvement in PSNR and embedding capacity through the proposed method. The improvement obtained for LSB and matrix embedding is exhibited in both Table2. The maximum embedding capacity of [12] and the proposed method are shown in Table3 and Table4. The secret image constructed in the destination is lossless since no quantization process is carried out. PSNR above 30dB is acceptable [23] but high quality recovering (secret) image should strive for 40dB and above.

The last 64 pixel in cover image is reserved for storing the technical details, which will be used in the receiver side to extract the secret data from the stego image. This 64 pixel (64x3=192 bytes) should be excluded while computing the maximum hiding capacity of cover image. Secret data of more unique symbol with any size can be hidden through our proposed method, provided it meets the above said condition.

TABLE 1: PSNR and MSE RESULTS for the Method3 of (R.Amirtharajan et al., 2010).

Cover Image [256 × 256]	**Method 3 of (R.Amirtharajan et al., 2010)**						
	Red Channel		**Green Channel**		**Blue Channel**		**Bits per Pixel**
	MSE	PSNR	MSE	PSNR	MSE	PSNR	RGB
Lena	0.51	51.09	0.64	50.04	0.78	49.23	4.49
Baboon	0.50	51.15	0.63	50.13	0.78	49.21	4.48
Gandhi	0.53	50.92	0.64	50.06	0.78	49.24	4.49
Temple	0.49	51.16	0.64	50.10	0.78	49.21	4.48

TABLE 2: PSNR and MSE Results of Proposed Method.

Secret Data (Image) Of Capacity 295704 Bits / 111 × 111		**Cover Image of size 256 X 256**						
		Red Channel		**Green Channel**		**Blue Channel**		**Bits per Pixel**
		MSE	PSNR	MSE	PSNR	MSE	PSNR	
Lena	Lsb	0.24	54.30	0.24	54.26	0.24	54.26	5.31
	Matrix	0.18	55.37	0.18	55.50	0.18	55.47	5.31
Baboon	Lsb	0.24	54.29	0.24	54.28	0.24	54.26	5.31
	Matrix	0.18	55.43	0.18	55.45	0.18	55.45	5.31
Gandhi	lsb	0.24	54.31	0.24	54.29	0.24	54.26	5.31
	Matrix	0.18	55.37	0.18	55.46	0.18	55.42	5.31
Temple	lsb	0.24	54.24	0.24	54.29	0.24	54.27	5.31
	Matrix	0.18	55.51	0.18	55.39	0.18	55.39	5.31

TABLE 3: Maximum Embedding Capacity of (R.Amirtharajan et al., 2010).

Cover Image [256 × 256]	**Method 3 of (R.Amirtharajan et al., 2010)**	
	Bits per Pixel (RGB)	Maximum Embedding Capacity
Lena	4.49	256 X 256 X 4.49 =294256 bits
Baboon	4.48	256 X 256 X 4.48 =293601 bits
Gandhi	4.49	256 X 256 X 4.49 =294256 bits
Temple	4.48	256 X 256 X 4.48 =293601 bits

5.1 Discussion

In the proposed method, Interpixel difference coding is done prior to Huffman coding technique which has enhanced the embedding capacity when comparing [12]. The reason is that structure of data[1][13] in an image (pixel value) can be characterized by an equation which is discussed in Section 4.3 and 4.4. This residual coding resulted in getting higher embedding capacity.

TABLE 4: Maximum Embedding Capacity of Proposed Method.

Secret data (Image) of size 950424 bits for LSB and 532824 bits for Matrix embedding		**Cover Image of size 256 X 256**						
		Red Channel		**Green Channel**		**Blue Channel**		**Bits per Pixel**
		MSE	PSNR	MSE	PSNR	MSE	PSNR	
Lena	Lsb	0.48	51.23	0.49	51.20	0.49	51.17	1.65
	Matrix	0.22	54.55	0.23	54.42	0.23	54.38	2.95
Baboon	Lsb	0.49	51.16	0.49	51.15	0.49	51.18	1.65
	Matrix	0.23	54.45	0.23	54.45	0.23	54.45	2.95
Gandhi	Lsb	0.49	51.18	0.49	51.16	0.49	51.19	1.65
	Matrix	0.24	54.29	0.23	54.53	0.23	54.52	2.95
Temple	Lsb	0.49	51.19	0.49	51.17	0.49	51.15	1.65
	Matrix	0.23	54.40	0.23	54.42	0.23	54.49	2.95

It is quite often found that a secret image which is richer and whose dimension is lesser than Cameraman 111 X 111 shown in Fig.4 (image used as secret image in the proposed method) cannot be embedded in this 256 x 256 cover image Lena. In contrast, a secret image which is not richer whose dimension is higher than cameraman 111 X 111 can be embedded in the cover image. This makes us to finalize that the embedding capacity of our proposed technique depends on Huffman encoding. Any image, whose Huffman compression is less, fits in the cover image irrespective of its size and richness. To discuss on security side, the proposed technique is robust enough; because extracting a data without knowing the architecture of the proposed technique is difficult, moreover data is Huffman encoded. Based on how the symbols are treated, the implementation of Huffman may vary. But however the basic rule that should be adhered is that Huffman codes are uniquely decodable[1]. Even if the intruder collects the LSBs from the cover image, the intruder should separate the Huffman table and actual Huffman encodings.

6. CONCLUSION

An Interpixel difference image steganography algorithm which brings a better PSNR than [12] is proposed. Histogram of stego image and cover image are almost equal which emphasize on the result that distortion between cover and stego image is minimum. Capacity improvement and distortion reduction has been addressed in this proposed technique. In the proposed work, the embedding capacity of the cover image is increased, at the same time the PSNR are also controlled.

7. FUTURE WORK

A comparative study with predictive coding should be experimented and their result should be compared with Interpixel difference encoding algorithm. The proposed work should be refined in such a way that more embedding algorithm should be tested on a pixel before the embedding took place. A separate channel should be reserved for storing the embedding technique attempted. The proposed algorithm should be customized to support embedding in the frequency domain. It should be enhanced to support color images and withstand few geometrical distortion induced on the image.

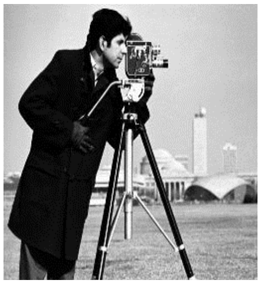

FIGURE 5: Secret Image Cameraman.

Fig.6a Lena Cover Image

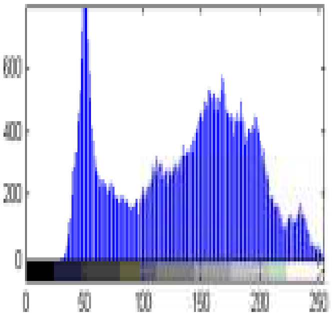

Fig.6b Red Channel Histogram

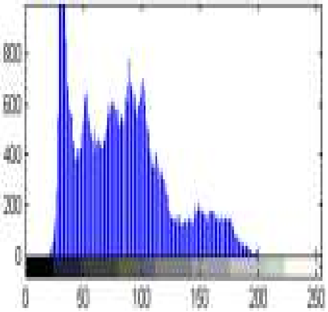

Fig.6c Blue Channel Histogram

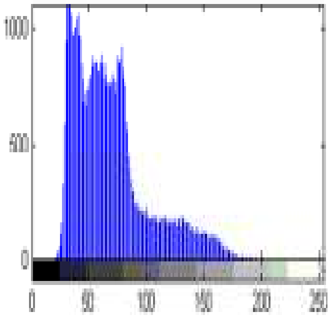

Fig.6d Green Channel Histogram

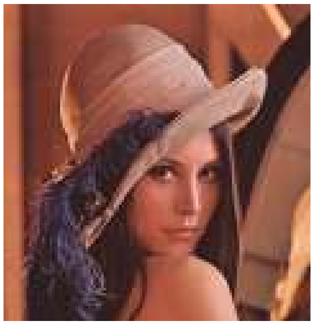

Fig.6e Lena LSB Stego Image

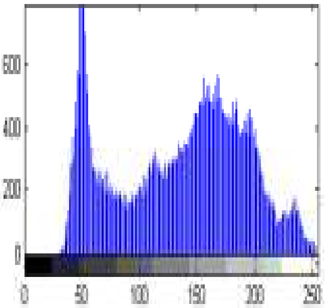

Fig.6f Red Channel Histogram

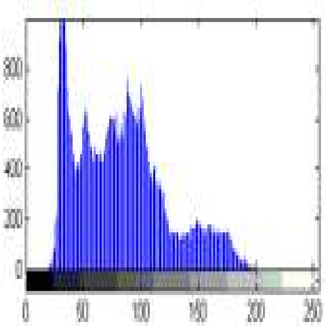

Fig.6g Blue Channel Histogram

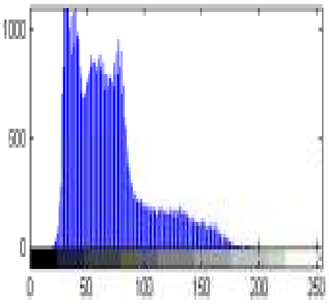

Fig.6h Green Channel Histogram

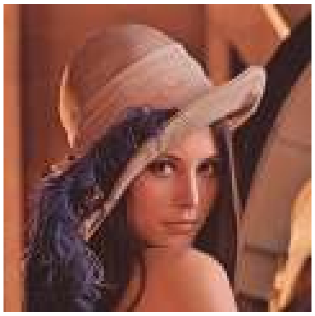

Fig.6i Lena Matrix Stego Image

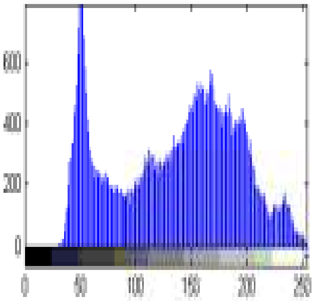

Fig 6j Red Channel Histogram

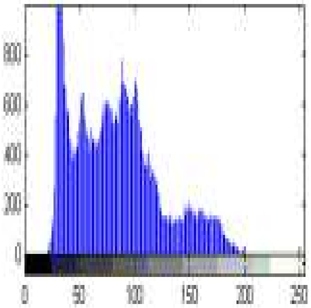

Fig 6k Blue Channel Histogram

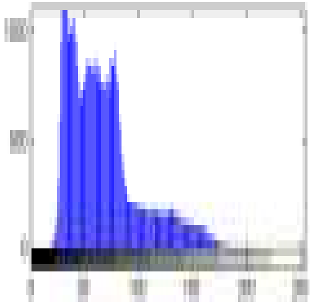

Fig 6l Green Channel Histogram

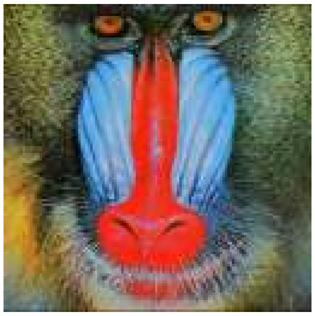

Fig.7a Baboon Cover Image

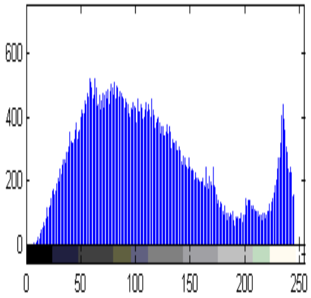

Fig.7b Red Channel Histogram

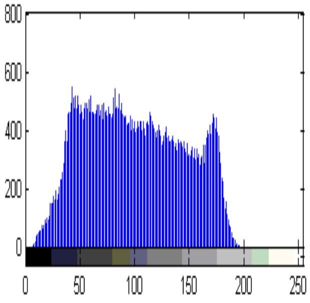

Fig.7c Blue Channel Histogram

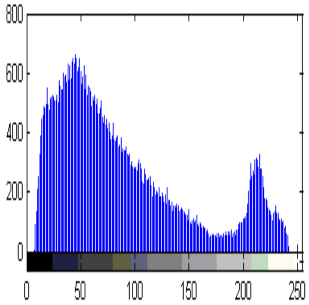

Fig.7d Green Channel Histogram

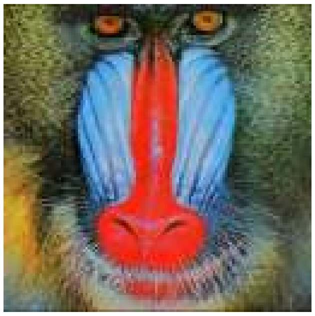

Fig.7i Baboon Matrix Stego Image

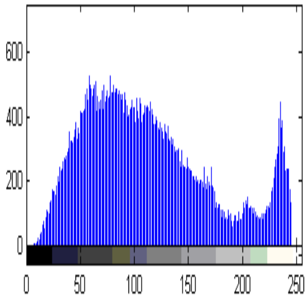

Fig.7j Red Channel Histogram

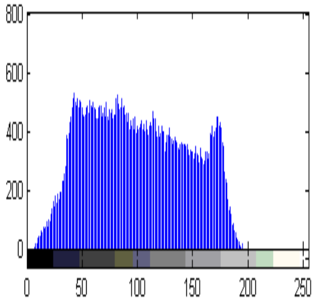

Fig.7k Blue Channel Histogram

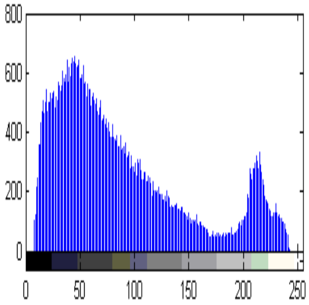

Fig.7l Green Channel Histogram

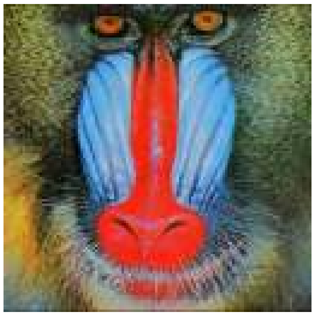

Fig.7e Baboon LSB Stego Image

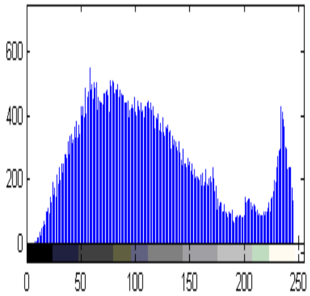

Fig.7f Red Channel Histogram

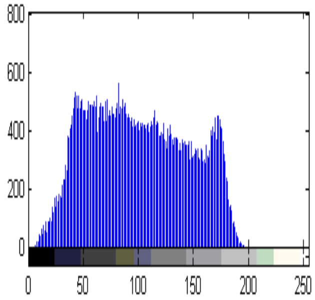

Fig.7g Blue Channel Histogram

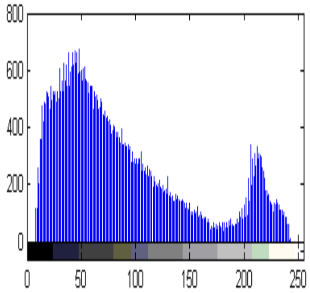

Fig.7h Green Channel Histogram

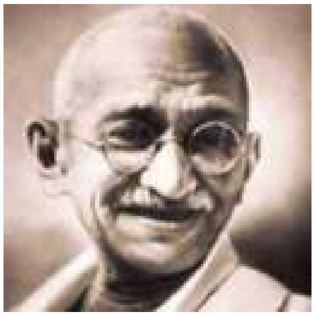

Fig.8a Gandhi Cover Image

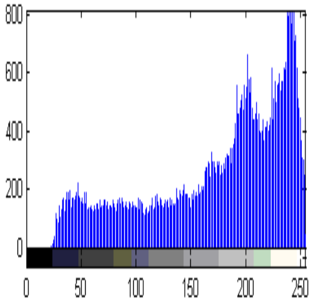

Fig.8b Red Channel Histogram

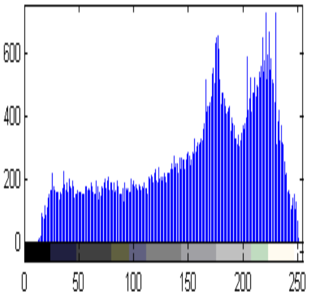

Fig.8c Blue Channel Histogram

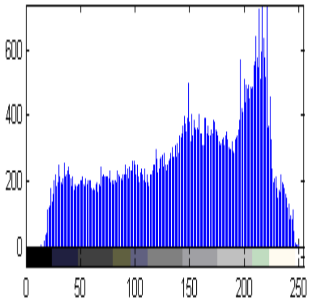

Fig.8d Green Channel Histogram

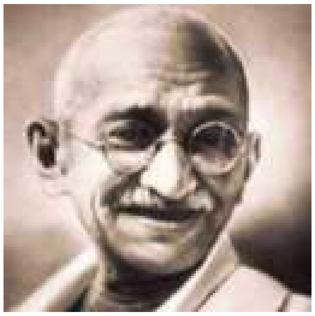

Fig.8e Gandhi LSB Stego Image

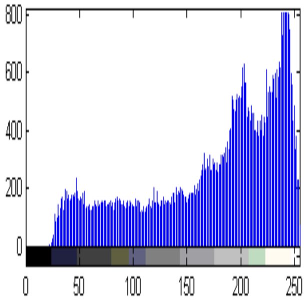

Fig.8f Red Channel Histogram

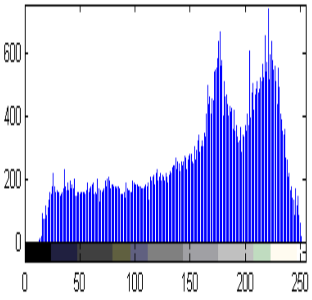

Fig.8g Blue Channel Histogram

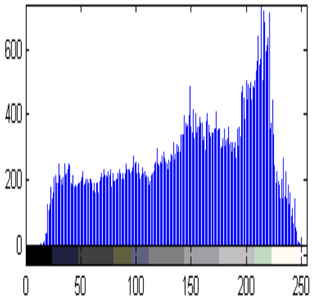

Fig.8h Green Channel Histogram

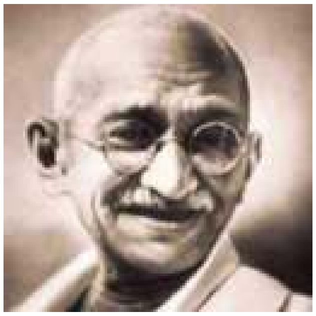

Fig.8i Gandhi Matrix Stego Image

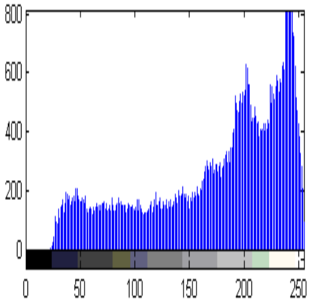

Fig.8j Red Channel Histogram

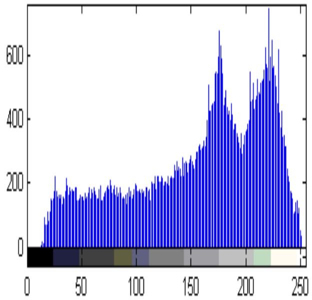

Fig.8k Blue Channel Histogram

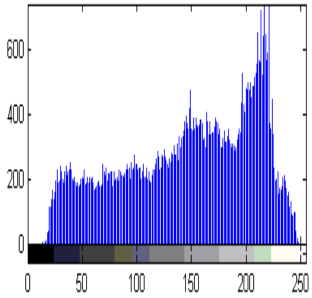

Fig.8l Green Channel Histogram

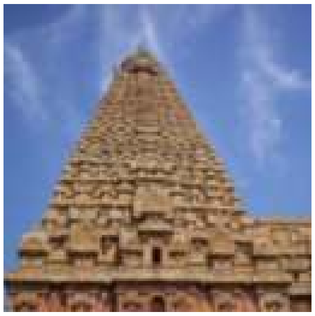

Fig.9a Temple Cover Image

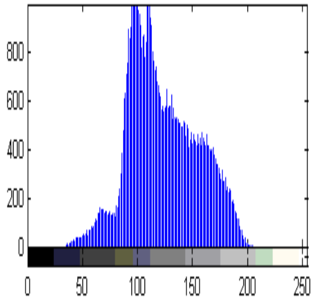

Fig.9b Red Channel Histogram

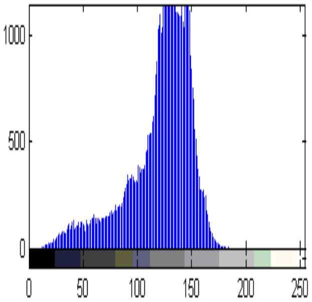

Fig.9c Blue Channel Histogram

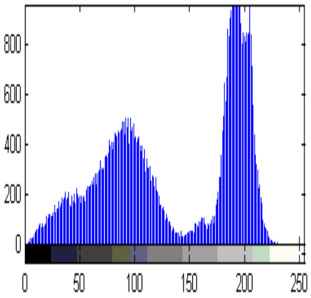

Fig.9d Green Channel Histogram

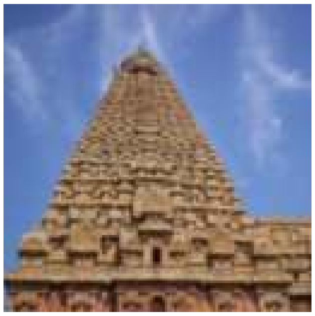

Fig.9e Temple LSB Stego Image

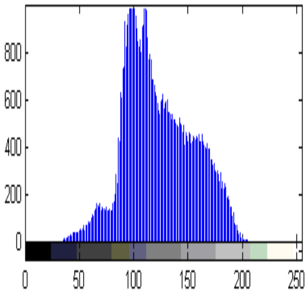

Fig.9f Red Channel Histogram

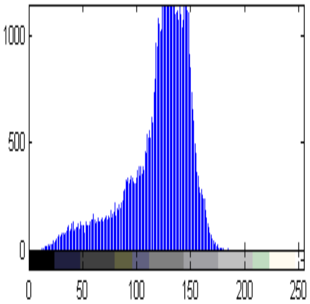

Fig.9g Blue Channel Histogram

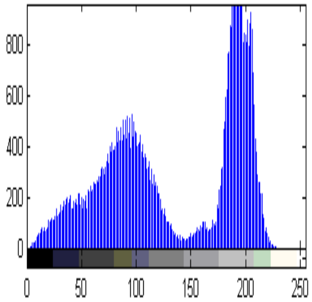

Fig.9h Green Channel Histogram

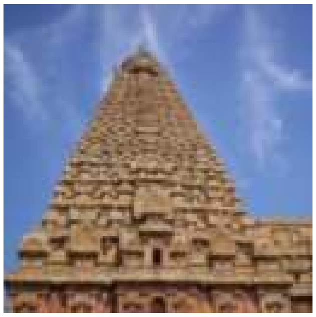

Fig.9i Temple Matrix Stego Image

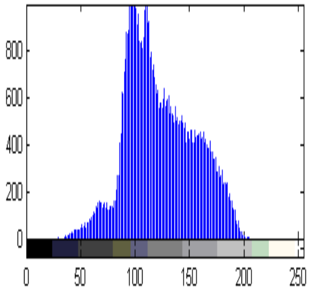

Fig.9j Red Channel Histogram

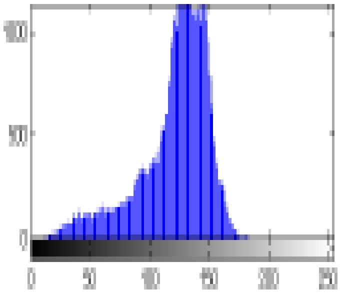

Fig.9k Blue Channel Histogram

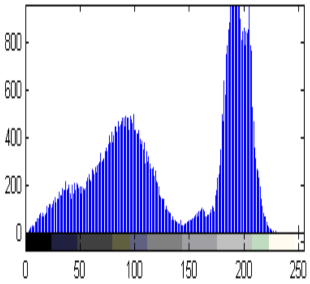

Fig.9l Green Channel Histogram

8. REFERENCES

[1] Khalid Sayood, Introduction To Data Compression: 3rd edition, Morgan Kaufmann Publications, 2005.

[2] Tayana Morkel, Jan H P Eloff and Martin S Olivier "An Overview of Image teganography", Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sandton, South Africa, Jul. 2005.

[3] Injemar J. Cox,Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich and Ton Kalker. “Digital Watermarking and Steganography”, Burlington, MA 01803, USA: Morgan Kaufmann, Second Edition,2008.

[4] Sutaone, M. S., and Khandare, M.V. “Image Based Steganography Using LSB Insertion Technique” in IET International Conference on Wireless, Mobile and Multimedia Networks(Beijing,China) IET,2008, pp.146-151.

[5] Chan,C-K., and Cheng, L.M. 2004. “Hiding data in images by simple LSB substitution”,Pattern Recogn. 37(3),pp.469 – 474.DOI:10.1016/j.patcog.2003.08.007.

[6] Luo,W.,Huang,F.,and Huang,J. ”Edge Adaptive Image Steganography Based on LSB Matching Revisited” IEEE T INF FOREN SEC, 5(2), pp.201-214,2010, DOI:10.1109/TIFS.2010.2041812.

[7] Wu,D-C.,and Tsai,W-H. “A steganographic method for images by pixel-value differencing”.Pattern Recogn.Lett. 24(9),pp.1613–1626,2003. DOI:10.1016/S0167-8655(02)00402-6.

[8] Fridrich,J.,and Soukal, D. “Matrix Embedding for Large Payloads”, IEEE T INF FOREN SEC,1(3),pp.390-395,2006. DOI: 10.1109/TIFS.2006.879281.

[9] Gonzalez, R.C. and Woods, R.E. “Digital Image Processing”,3rd Edition , New Delhi, India:PHI, 2008.

[10] David A. Huffman "A method for the construction of minimum-redundancy codes. Proceedings of the Institute of Radio Engineers" 40(9):1098–1101, Sep. 1952.

[11] Data Compression Project. [Online] Available at http://www.binaryessence.com [Feb. 20, 2013]

[12] Amirtharajan R, Sandeep Kumar Beher, Motamarri Abhilash Swarup, Mohamed Ashfaaq K and John Bosco Balaguru Rayappan. “Colour Guided Colour Image Steganography”, Universal Journal of Computer Science and Engineering Technology, Volume 1, pp.16 – 23, Oct . 2010.

[13] Sarkar,A.,Madhow,U.,and Manjunath B.S. “Matrix Embedding With Pseudorandom Coefficient Selection and Error Correction for Robust and Secure Steganography”,IEEE T INF FOREN SEC,5(2),pp.225-239,2010,DOI:10.1109/TIFS.2010.2046218.

[14] Amitava Nag, S. Biswas, D. Sarkar, P.P. Sarkar. “A Novel Technique for Image Steganography Based on Block-DCT and Huffman Encoding” , International Journal of Computer Science and Information Technology, Volume 2, Number 3, pp. 103-112,June 2010.

[15] Amitava Nag, S. Biswas, D. Sarkar, P.P. Sarkar. “A Novel Technique for Image Steganography Based on DWT and Huffman Encoding” , International Journal of Computer Science and Security, Volume 4, Issue 6, pp. 561-570, Feb. 2011.

[16] Chang, C.C and Tseng, H.W. “A Steganographic method for digital images using side match”,Pattern Recognition Letters, 25: pp.1431 – 1437, Jun. 2004.

[17] Nithyanandam, P., Ravichandran, T., Santron, N.M. and Priyadarshini.(2011) “A Image Steganography Technique On Spatial Domain Using Matrix and LSB Embedding based on Huffman Encoding’ ,Journal of Future Engineering and Technology, Volume 6, Issue 3,pp.25-34, Feb.2011.

[18] Nithyanandam, P., Ravichandran, T., Santron, N.M. and Priyadarshini, E. “A Spatial Domain Image Steganography Technique Based on Matrix Embedding and Huffman Encoding”, International Journal of Computer Science and Security, Vol. 5, No. 5, pp. 456-468, 2011.

[19] Nithyanandam, P., Ravichandran, T., Santron, N.M. and Priyadarshini, E. “A Image Steganography for Color Images using Lossless Compression Technique”, International Journal of Computational Science and Engineering, Vol. 7, No. 3, pp. 194-205, 2012.

[20] Nithyanandam, P., Ravichandran, T. “Geometrical Rotation Addressed Steganography Technique using Matrix Embedding and Huffman Encoding”, European Journal of Scientific Research, Vol. 87, No. 1, pp. 31-45, 2012.

[21] Nithyanandam, P., Ravichandran, T. “Gray Coded Grayscale Image Steganography using Hufman Encoding”, International Journal of Image Processing, Vol. 6, No. 5, pp. 334-348, 2012.

[22] Nithyanandam,P., Ravichandran, T. “A Hybrid Embedded Steganography Technique: Optimum Pixel Method and Matrix Embedding”, presented in International Conference on Advances in Computing, August 3-5, 2012.

[23] Abbas Cheddad. "Steganoflage: A New Image Steganography Algorithm",Ph.D. Thesis, School of Computing & Intelligent Systems Faculty of Computing & Engineering University of Ulster, United Kingdom,2009.

INSTRUCTIONS TO CONTRIBUTORS

The *International Journal of Computer Science and Security (IJCSS)* is a refereed online journal which is a forum for publication of current research in computer science and computer security technologies. It considers any material dealing primarily with the technological aspects of computer science and computer security. The journal is targeted to be read by academics, scholars, advanced students, practitioners, and those seeking an update on current experience and future prospects in relation to all aspects computer science in general but specific to computer security themes. Subjects covered include: access control, computer security, cryptography, communications and data security, databases, electronic commerce, multimedia, bioinformatics, signal processing and image processing etc.

To build its International reputation, we are disseminating the publication information through Google Books, Google Scholar, Directory of Open Access Journals (DOAJ), Open J Gate, ScientificCommons, Docstoc and many more. Our International Editors are working on establishing ISI listing and a good impact factor for IJCSS.

The initial efforts helped to shape the editorial policy and to sharpen the focus of the journal. Started with Volume 8, 2014, IJCSS is appearing with more focused issues. Besides normal publications, IJCSS intend to organized special issues on more focused topics. Each special issue will have a designated editor (editors) – either member of the editorial board or another recognized specialist in the respective field.

We are open to contributions, proposals for any topic as well as for editors and reviewers. We understand that it is through the effort of volunteers that CSC Journals continues to grow and flourish.

IJCSS LIST OF TOPICS

The realm of International Journal of Computer Science and Security (IJCSS) extends, but not limited, to the following:

- Authentication and authorization models
- Computer Engineering
- Computer Networks
- Cryptography
- Databases
- Image processing
- Operating systems
- Programming languages
- Signal processing
- Theory
- Communications and data security
- Bioinformatics
- Computer graphics
- Computer security
- Data mining
- Electronic commerce
- Object Orientation
- Parallel and distributed processing
- Robotics
- Software engineering

CALL FOR PAPERS

Volume: 9 - **Issue: 1**

i. Submission Deadline : December 31, 2014 **ii. Author Notification:** January 31, 2015

iii. Issue Publication: February 2015

CONTACT INFORMATION

Computer Science Journals Sdn BhD

B-5-8 Plaza Mont Kiara, Mont Kiara

50480, Kuala Lumpur, MALAYSIA

Phone: 006 03 6204 5627
Fax: 006 03 6204 5628
Email: cscpress@cscjournals.org

CSC PUBLISHERS © 2014
COMPUTER SCIENCE JOURNALS SDN BHD
B-5-8 PLAZA MONT KIARA
MONT KIARA
50480, KUALA LUMPUR
MALAYSIA

PHONE: 006 03 6204 5627
FAX: 006 03 6204 5628
EMAIL: cscpress@cscjournals.org