ISBN 978-9937-0-4872-9
September 27, 2018

A SECURE AND EFFECTIVE PATTERN-BASED STEGANOGRAPHIC METHOD IN COLOURED JPEG IMAGES

Gaurav Subedi
Department of Computer and Electronics Engineering
Kantipur Engineering College
Dhapakhel, Lalitpur
subedi.gasu15@gmail.com

***Abstract*—The advent of the Internet and advances in communication have made information ubiquitous. This large availability of information poses risk on its own. Electronic communication is increasingly susceptible to eavesdropping and malicious interventions. Privacy and security are major concerns in this age. In this light, two methods have been brought into existence: Cryptography and Steganography. Cryptography scrambles the message to make it unreadable whereas Steganography masks the existence of the message.**

Steganographic methods may be spatial-domain (altering the pixel values to hide data) or frequency-domain techniques (altering the frequency coefficients of the image). Spatial domain techniques are more susceptible to steganalysis unlike the frequency-domain techniques. In this paper, I propose a unique pattern based approach for steganography and extended caesar cipher for cryptography. In this approach, the message is first encrypted using extended caesar cipher and four patterns are selected to hide the message in the image. The hidden message is secured with an AES-encrypted password, adding an extra layer of security. This method is imperceptible to visible attacks, histogram attacks and statistical attacks since the alterations produced by the method do not bring about a detectable change in the resulting image. Thus, this method provides a new insight into a more secure, efficient and flexible steganographic technique.

***Index Terms*—Discrete Cosine Transform, Payload, Peak Signal to Noise Ratio, Cover Image, Stego Image**

I. Introduction

Steganography is a means of storing information in a way that hides that information's existence. Paired with existing communication methods, steganography can be used to carry out hidden exchanges [1]. The main thrust of steganography is that open channels are not the only means for communication, confidential information can be exchanged through the parties using covert channels. One such medium can be still images which can act as innocent carriers of secret message.

Two methods are devised for secure exchange of information: Cryptography and Steganography. Cryptography is basically scrambling of the message to make it unreadable to the eavesdropper. Steganography is the use of innocent means (called as carrier files) to transfer information so that the eavesdropper doesn't even know about the presence of information. Steganography differs from cryptography in the sense that cryptography focuses on keeping the contents of message secret whereas steganography focuses on keeping the existence of message secret [4].

Steganography can be broadly classified into two categories:

i. Spatial Domain Steganography
   The message is embedded in the intensity of pixels directly. It is highly susceptible to steganalysis. LSB Substitution in pixel intensities is one of such techniques.
ii. Frequency Domain Steanography
   The coefficients in the frequency domain are manipulated for data embeding. These techniques are robust against steganalysis and introduce less noise.

The primary goal of steganography is to design embedding function that is statistically undetectable and capable of communicating practical payloads [2]. Steganographic techniques are perfect supplements for encryption that allow a user to hide large amount of information within an image. Thus, it is often used in conjunction with cryptography so that the information is doubly protected [3].

Suppose, K_s denotes a stego key drawn from a set, K of all secret stego keys, M the set of all embeddable messages, and C the set of all cover works. A steganographic scheme is formed by two mappings, the embeding mapping, *Emb* and the extraction mapping, *Ext* as:

$$Emb : C \times K \times M \to C$$
$$Ext : C \to M$$

such that,
Ext(*Emb*(c,K_s,m)) = m for all $c \in C$, $K_s \in K$, and $m \in M$
The work S = *Emb*(c, K_s, m) is called Stego Work [2].

A coloured JPEG image consists of three planes Y, Cb and Cr. This research delves into the steganographic method of LSB substitution in the DCT coefficients of the Cb plane of a JPEG image. A colored JPEG image is selected as carrier and YCbCr color space values are extracted from it. Since human eye is less sensitive to changes in the blue spectrum of color, blue difference component, Cb is selected as the stego-plane. This plane is divided into 8×8 blocks starting from the top left of the plane, traversing all the way to the bottom right of the plane. This research paper uses baseline JPEG images with no chroma subsampling so that a MCU is the same as 8×8 data unit. Each MCU is subjected to DCT, quantization and then the encrypted message is hidden in the mid-frequency coefficients of the DCT matrix using LSB substitution. The embedding of message is done using one of the four patterns proposed in the paper. The message

is encrypted using Extended Caesar Cipher and secured with AES-encrypted password. Thus, a stego image is formed. This is sent to the receiver. The receiver can decode the message only if the password is correct, making the process secure. The extraction process is just the inverse of the embedding process.

This paper first gives an overview of the past works, techniques used and then dives into the algorithms for extraction and embedding. Analysis of the method as well as comparison with previous works is presented in the later sections.

A. Abbreviations and Acronyms

AES	Advanced Encryption Standard
JPEG	Joint Photographic Experts Group
DCT	Discrete Cosine Transform
LSB	Least Significant Bit
MCU	Minimum Coded Unit
MSE	Mean Squared Error
PSNR	Peak Signal to Noise Ratio
2D	Two Dimensional
FDCT	Forward DCT
CCDA	Counter Clockwise Direction Algorithm

II. Literature Review

A great amount of research has been done in the field of Frequency-Domain Steganography.

One of the earliest methods proposed in 1999 by Seki et. al [5] is hiding a bit of message in the highest frequency coefficient of the DCT matrix. Their method hides data only in the 64th quantized DCT coefficient of a block in zigzag order. This produces minimal distortion but has very limited payload capacity.

The proposed method is inspired by Mathkour et al. [6] method of Spiral LSB Substitution. They devise a CCDA algorithm working from center of four blocks to embed information using LSB Substitution in the frequency domain. The image is divided into four segments and CCDA is applied starting from the top left block. However, their method changes the high frequency components of the image resulting in higher distortion. My method uses patterns which affect the middle frequency components only, introducing less distortion.

Jsteg is one of the first steganographic algorithms for JPEG images. Jsteg embeds messages by decompressing the JPEG bit stream to individual quantized DCT coefficients and replacing the LSBs of coefficients having values other than 0 and 1 with message bits. This operation is often referred to as LSB replacement [7]. However, this poses limitations in payload capacity as well as is prone to steganalysis.

Authors in [8] recently proposed an image steganographic technique using pseudo-random LSB encoding algorithm with AES encryption. Their method was based in spatial-domain.

Jessica Fridrich et al. [16] have devised a heuristic algorithm known as nsF5 (no shrinkage F5), an improvement over the F5 algorithm. This algorithm simulates the embedding changes as carried out in the F5 algorithm coupled with wet paper codes. However, a significant image distortion is introduced.

The major drawback of these methods is that there is a large trade-off between image quality, embedding capacity and security of the information. My paper proposes a balanced algorithm with improved security, high quality and a significant embedding capacity.

III. Performance Parameters

Various parameters are used to evaluate the efficiency of the algorithm comparing the cover image and stego image. MSE and PSNR are most widely used.

A. MSE

MSE measures the average of the squares of errors i.e. average squared difference between the estimated values and the estimate. MSE is always non-negative and the closer the values are to zero, the better the technique. MSE is calculated between the pixel intensities of cover image and stego image [14]. It is computed using equation 1 [13].

$$MSE = \frac{1}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} (p_{ij} - q_{ij})^2 \tag{1}$$

where, $m \times n$ denotes image dimension
p_{ij} denotes cover image pixel intensity
q_{ij} denotes stego image pixel intensity

B. PSNR

The PSNR is a measure of distortion in the stego-image. It is computed using MSE as in equation 2.

$$PSNR = 10 \times \log_{10} \frac{255 \times 255}{MSE} \tag{2}$$

Higher PSNR value means lesser distortion. A PSNR value more than 40 decibels (dB) is considered good. If it is in between 30 dB and 40 dB, can be acceptable, but a PSNR less than 30 dB is not acceptable because the distortion produced is very high [13].

IV. Algorithms Used

A. LSB Substitution

LSB is a substitution method of steganography where the rightmost bit in binary notation is replaced with a bit from the message [9]. Consider binary notation of a DCT coefficient as 00101101 and the message bit to be embedded is 0. Then, after LSB substitution, the coefficient becomes 00101100. For this method, the image should have a lot of varying colors; it must be "noisy", so that the added noise is covered by the already present ones [9].

B. Discrete Cosine Transform

DCT separates image into spectral sub-bands of differing importance with respect to image's visual quality. JPEG compression uses DCT in a 8×8 block. The general equation for a 2D (8×8 data items) DCT is defined by equations 3 and 4 [10].

I. Forward DCT

$$S_{vu} = \frac{1}{4} C_u C_v \sum_{x=0}^{7} \sum_{y=0}^{7} s_{yx} \cos\frac{(2x+1)u\pi}{16} \cos\frac{(2y+1)v\pi}{16} \quad (3)$$

II. Inverse DCT

$$s_{yx} = \frac{1}{4} \sum_{x=0}^{7} \sum_{y=0}^{7} C_u C_v S_{vu} \cos\frac{(2x+1)u\pi}{16} \cos\frac{(2y+1)v\pi}{16} \quad (4)$$

$$Where,$$
$$C_u, C_v = \frac{1}{\sqrt{2}} for\ u, v = 0$$
$$C_u, C_v = 1\ otherwise$$

An 8×8 block of source image sample is effectively a 64-point discrete signal which is a function of two spatial dimensions x and y. FDCT takes such signal as input and decomposes it into 64 orthogonal basis signals [10]. The output of FDCT consists of three frequency components: low, medium and high. The lowest frequency component (with zero frequency)is known as DC coefficient and the other 63 as AC coefficients. A visualization of the data block after DCT is depicted in Figure 1.

DC	1	5	6	14	15	27	28
2	4	7	13	16	26	29	42
3	8	12	17	25	30	41	43
9	11	18	24	31	40	44	53
10	19	23	32	39	45	52	54
20	22	33	38	46	51	55	60
21	34	37	47	50	56	59	61
35	36	48	49	57	58	62	63

Fig. 1: Frequency Distribution of a 8*8 DCT block.

The components in white are the low frequency components, the gray ones are middle frequency components and the ones in black are high-frequency components.

C. AES

AES is a symmetric key, symmetric block cipher based on Rijndael algorithm for encrypting text. It supports data block of 128-bit and variable key sizes of 128, 192 and 256 bits [8].

In AES, input data is arranged in 4x4 arrays of bytes called a State, with four rows and four columns consisting of 16 bytes in total. AES uses a round function that is composed of four different byte-oriented transformations [12]. A more abstract level description of the algorithm is as follows:

a. `Key Expansion` - Round keys are derived from the cipher key using Rijndaels key schedule.
b. Initial round key addition:
   `AddRoundKey` - Each byte of the state is combined with a block of the round key using bitwise XOR.
c. The following steps are repeated according to key size. For 128-bit key, the repetition is done for 9 rounds.
   i. `SubBytes` - It is a non-linear substitution step in which each byte is replaced with another according to the entries in a lookup table called an S-box. A S-box is a one to one mapping for all byte values from 0 to 255.
   ii. `ShiftRows` - It is a transposition step in which each row of the state is shifted cyclically at a certain number of steps. The rows are shifted x number of bytes to the left where x is the row number.
   iii. `MixColumns` - A mixing operation is operated on the columns of the state, combining the four bytes in each column.
   iv. `AddRoundKey`
d. Final round consists of the following steps:
   i. `SubBytes`
   ii. `ShiftRows`
   iii. `AddRoundKey`

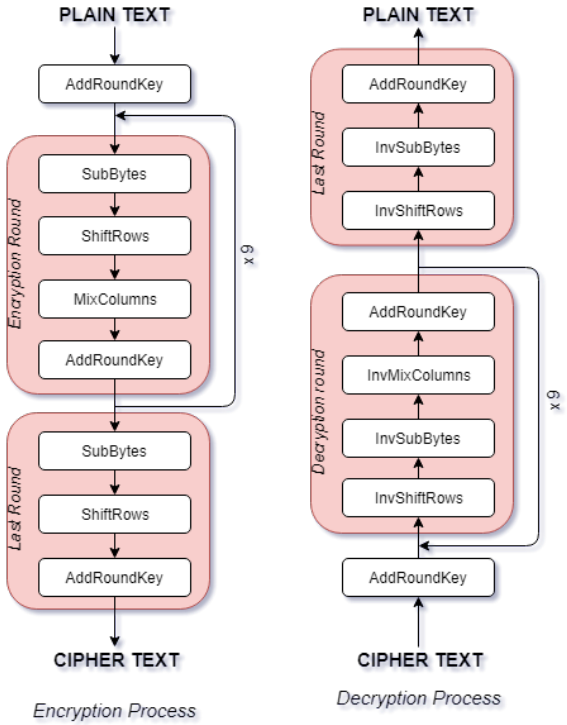


Fig. 2: AES Schemes for 128-bit Key

V. Proposed Methods

A. Extended Caesar Cipher

Caesar cipher is a type of substitution type cipher. In this cipher, each letter in the plain text is replaced by a letter some

fixed number of positions down the alphabet using modular arithmetic [11]. The classical Caesar Cipher is a shift Cipher operating on the letters of the English alphabet. Since symbols such as '?', '.', ',' and others are commonly used in day-to-day communication, the cipher is extended to include these symbols as well. The character sets for the ciphers are:
Clasical Caesar Cipher: abcdefghijklmnopqrstuvwxyz
Extended Caesar Cipher: abcdefghijklmnopqrstuvwxyz.?," "
The classical cipher supports 26 characters whereas the extended cipher supports 32 characters. Consider, x is a character in the set and k is the shift. Then, the encryption function is defined by equation 5.

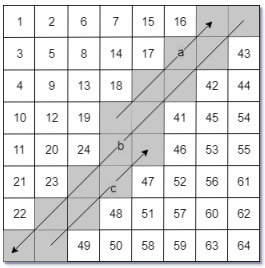
$$e(x) = (x - k) \, mod \, 32 \tag{5}$$

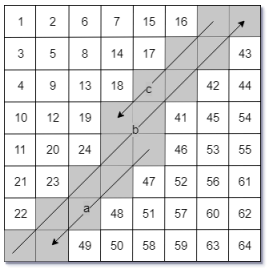
The decryption function is defined by equation 6.

$$d(x) = (x - k) \, mod \, 32 \tag{6}$$

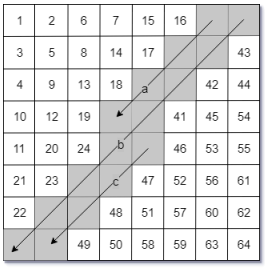
B. Pattern Based Embedding

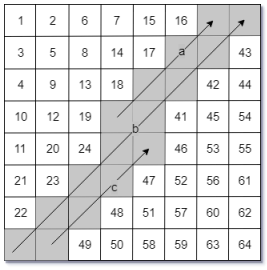
A different approach is used in hiding message in the quantized DCT blocks. For this, a 8×8 window is traversed from the top-left to the bottom-right of quantized DCT plane of Cb component of image. Window traversing is done left to right in a row and top to bottom along rows. The embedding is done in the middle most frequency components i.e. from 25^{th} to 40^{th} in the zigzag sequence of encoding. The selection of blue difference component (Cb) exploits the human vision as human eye is less sensitive to changes in Cb component than the luma (Y) or red chroma (Cr) component. Here, only Cb plane is used to hide the message because if Cr plane is also used, the statistical similarities in the mid-band coefficients between these planes may be exploited by steganalysis. Also, the use of patterns removes any monotony in the amplitudes of the components. The method makes use of the following four patterns:





(c) Pattern 3





(d) Pattern 4

Here, the numbering represents the order of the dct coefficients in zigzag pattern and the alphabets denote the sequence of the coefficients to be taken, from base of the arrow to the tip of the arrow.
Sequence of coefficients:
Pattern 1: 25 26 27 28 29 30 31 32 33 34 35 36 37, 38 39 40
Pattern 2: 40 39 38 37 36 35 34 33 32 31 30 29 28 27 26 25
Pattern 3: 28 27 26 25 29 30 31 32 33 34 35 36 40 39 38 37
Pattern 4: 25 26 27 28 36 35 34 33 32 31 30 29 37 38 39 40
Since, 16 bits(2 bytes) are embedded in a MCU,

$$Payload \; Capacity = \left(\frac{width \times height}{64} \right) \times 2 \; bytes$$

Algorithm:
Each MCU is given an id, mcuid. mcuid=0 for the first (top-left) MCU and incremented by one as the window traverses.
Steps for embedding:

1) mcuid = 0
2) If mcuid mod 4 = 0
   select pattern 1
   Else if mcuid mod 4 = 1
   select pattern 2
   Else if mcuid mod 4 = 2
   select pattern 3
   Else if mcuid mod 4 = 3
   select pattern 4
3) Embed the message bits as per the selected pattern. The encryption method used is the LSB substitution. Bits of message is substituted in the LSB of the selected frequency components in an order determined by the pattern.
4) Increment mcuid by one
5) Repeat steps 2 to 4 until all the message bits are embedded

Steps for extraction:
The extraction method is similar to the embedding method except in that the message bits are extracted from the LSBs of the selected coefficients based on pattern and appended to form the message.

VI. System Design

The system consists of two modules: Embedding module and Extraction module.

A. Embedding Module

1) Algorithm:

a. Decode the JPEG image and convert it into YCbCr color planes.

b. Select the Cb (Blue Chrominance) plane and divide it into 8×8 blocks. Since no subsampling is used, the block becomes the MCU for encoding.

c. For each MCU, perform 2D FDCT and then quantization. The quantization is done with the JPEG specified quantization matrix as in [15]. The quantization matrix is

altered using a quality factor, which plays an important role in controlling image quality as well as stego file size.
d. Step c generates a new Cb plane with quantized DCT coefficients. Then, perform encoding using the proposed algorithm.
e. Perform DCT and quantization in Y and Cr planes.
f. Combine the encoded Cb plane with the original Y and Cb plane and compress the data using Huffman encoding.
g. Finally, combine the compressed data with the appropriate headers and footers to form the stego JPEG image.

2) Hiding of Message:

a. Scramble the message using the extended Caesar cipher.
b. Feed the cipher message to step d of the embedding algorithm.

3) Hiding of Password: The password is limited to 8 characters in order to minimize the storage size for the encrypted bits. Password hiding steps are:

a. AES encrypt the plain password using a 128-bit key and a 16-byte initialization vector.
b. Inject the encrypted password into the stego image. To keep the payload size consistent, the encrypted password is inserted as comment in the image file.

B. Extraction Module

1) Algorithm:

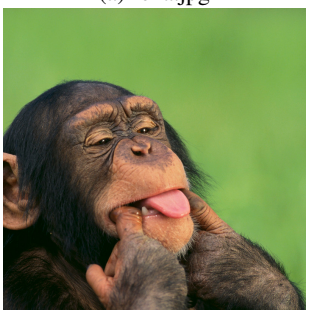
a. The message in stego-image is password protected. First, decrypt the the password (shared as a comment) using AES decryption and ask the receiver for password.
b. Upon successful verification, decompress the stego-image using Huffman decoding into YCbCr color planes.
c. Extract the encrypted message from the Cb plane using the proposed method.
d. Decrypt the encrypted message using the decryption function of the Extended Caesar Cipher to obtain the original message.

VII. Experimental Results

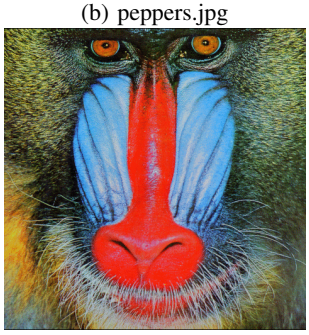
For the purpose of the research, a Java-based program was formulated for embedding and extraction scenario. JPEG encoder and decoder were hardcoded using the JPEG specifications by ITU [15]. For the calculations of the PSNR of the images, MATLAB was used. For the analysis, the quality factor was kept 100 so as to keep the artifacts of the image intact as well as to produce minimal distortion. For the purpose of this research, images with different histogram characteristics are required. Owing to this, following four images are used in this research:

(a) lena.jpg

(b) peppers.jpg



(c) monkey.jpg



(d) baboon.jpg

For comparison of the proposed algorithm with Jsteg, first a 1KB message was embedded in the images and the results were tabulated. Then, maximum payload size obained from the Jsteg algorithm was used for comparison. Table I shows the results obtained after comparing the proposed algorithm with the Jsteg algorithm.

TABLE I: Comparison Results With Jsteg

Image	Jsteg			Proposed Method		
	Max. Capacity (bytes)	Payload (bytes)	PSNR (dB)	Max. Capacity (bytes)	Payload (bytes)	PSNR (dB)
lena.jpg (400x400)	1893	1024	41.06	5000	1024	45.79
		1893	40.09		1893	45.70
peppers.jpg (304x304)	1320	1024	39.1213	2888	1024	46.30
		1320	38.94		1320	46.20

Table II shows the PSNR values obtained after embedding maximum capacity payload in the images. Table III presents the comparison results obtained after comparing the proposed method with the nsF5 algorithm.

TABLE II: PSNR Values of Images With Maximum Payload

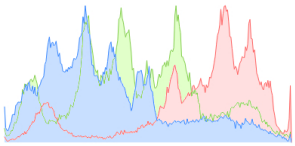
Image	Dimensions	Maximum Payload Capacity (bytes)	PSNR (dB)
lena.jpg	400x400	5000	45.41
pepper.jpg	304x304	2888	46.00
monkey.jpg	800x800	20000	45.27
baboon.jpg	480x480	7200	45.43

TABLE III: Comparison with nsF5 Algorithm

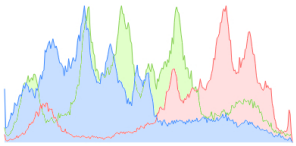
Image	nsF5 PSNR (dB)	Proposed PSNR(dB)
lena.jpg	34.74	45.41
pepper.jpg	31.67	46.00
monkey.jpg	36.09	45.27
baboon.jpg	24.81	45.43

The histograms of cover image and stego images for the different images after the embedding of maximum-capacity payload are shown below.

1) lena.jpg

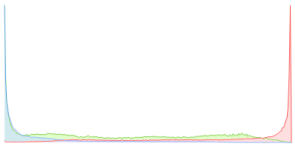


(a) Cover Image Histogram

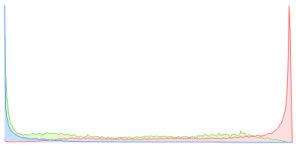


(b) Stego Image Histogram

2) peppers.jpg

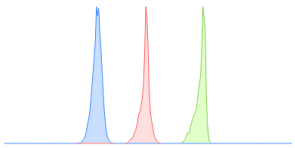


(a) Cover Image Histogram

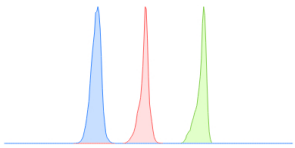


(b) Stego Image Histogram

3) monkey.jpg

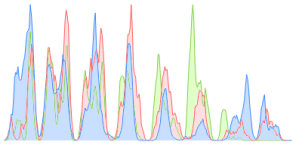


(a) Cover Image Histogram

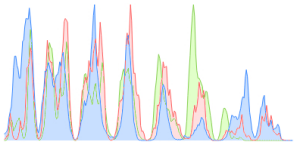


(b) Stego Image Histogram

4) baboon.jpg



(a) Cover Image Histogram



(b) Stego Image Histogram

The statistical properties of the cover and stego images under full-capacity embedding is shown in Table IV. The calculation of the statistical parameters is done on the basis of pixel intensities of the cover and stego image.

TABLE IV: Statistical Properties of Cover and Stego Images

S.N.	Image	Mean	Variance	Standard Deviation
1	lena.jpg	118.99	4700.95	68.56
	lenaStego.jpg	118.17	4697.47	68.54
2	peppers.jpg	107.43	8919.15	94.4412
	peppersStego.jpg	106.74	8897.99	94.33
3	monkey.jpg	99.98	2916.59	54.00
	monkeyStego.jpg	99.18	2934.94	54.17
4	baboon.jpg	101.19	3819.36	61.80
	baboonStego.jpg	100.40	3822.49	61.83

VIII. Enhancements

The current method embeds message bits in the LSB of the quantized DCT coefficients of Cb plane. For increasing message capacity, a 2-bit substitution scheme may be used. Further, increase in payload capacity can be achieved by using the Cr plane in conjunction with other statistically undetectable methods. The proposed algorithm provides flexibility in incorporating other embedding techniques, too.

IX. Conclusion

JPEG is one of the most popular image formats for digital communication through web and other mediums. JPEG follows a lossy compression algorithm that converts the spatial domain components to frequency domain. This technique can be exploited for transferring secret information. Since grayscale images do not contain Cb plane, they are not used in this paper.

This research paper proposed a secure and undetectable method of hiding message in JPEG image. AES and Extended Caesar Cipher added an extra layer of security. Analysis of the method showed that it is more superior to existing techniques, and is more efficient and robust. Comparison showed that the proposed method is superior to the existing methods in terms of visual ans statistical imperceptibility as well as payload capacity. The changes in PSNR values of the images with increasing payload was very minimum. The histograms and statistical properties of the cover image and their corresponding stego images showed no conspicuous difference. This proves that the method is resistant against histogram attacks as well as statistical attacks.

Studying the unexplored horizons in Steganography in the past, this paper proposes an efficient Steganographic technique. Future researchers can further improve this technique by incorporating pattern based approach with other algorithms.

Acknowledgment

A lot of helping hands were involved in this research. I would like to express my heartfelt gratitude to my father, Asst. Prof. Shankar Subedi, at the Central Department of English, TU for proofreading the paper. My sincere thanks goes to Er. Rajeev Prajapati, Er. Surendra Tamrakar, Er. Rabindra Khati (HOD), Er. Dipesh Shrestha at the Department of Computer and Electronics for their support, encouragement and continuous feedback. I thank my friends and others who

were instrumental in the completion of this project. I would like to acknowledge all the intellectuals and professionals whose work were contributory in this research.

REFERENCES

[1] Artz, Donovan. "Digital steganography: hiding data within data." IEEE Internet computing 5.3 (2001): 75-80.
[2] Cox, Ingemar, et al. "Digital watermarking and steganography." Morgan kaufmann, 2007.
[3] Younes, Mohammed Ali Bani, and Aman Jantan. "A new steganography approach for images encryption exchange by using the least significant bit insertion." International Journal of Computer Science and Network Security 8.6 (2008): 247-257.
[4] Wang, Huaiqing, and Shuozhong Wang. "Cyber warfare: steganography vs. steganalysis." Communications of the ACM 47.10 (2004): 76-82.
[5] Seki, Yusuke, et al. "Quantization-based image steganography without data hiding position memorization." Circuits and Systems, 2005. ISCAS 2005. IEEE International Symposium on. IEEE, 2005.
[6] Mathkour, Hassan, et al. "A novel approach for hiding messages in images." Signal Acquisition and Processing, 2009. ICSAP 2009. International Conference on. IEEE, 2009.
[7] Kodovsky, Jan, and Jessica Fridrich. "Quantitative structural steganalysis of Jsteg." IEEE Transactions on Information Forensics and Security 5.4 (2010): 681-693.
[8] Chikouche, Sofyane Ladgham, and Noureddine Chikouche. "An improved approach for lsb-based image steganography using AES algorithm." Electrical Engineering-Boumerdes (ICEE-B), 2017 5th International Conference on. IEEE, 2017.
[9] Kipper, Gregory. "Investigator's guide to steganography". crc press, 2003.
[10] Wallace, Gregory K. "The JPEG still picture compression standard." IEEE transactions on consumer electronics 38.1 (1992): xviii-xxxiv.
[11] Srikantaswamy, S. G., and Dr HD Phaneendra. "Improved Caesar cipher with random number generation technique and multistage encryption." International Journal on Cryptography and Information Security (IJCIS) 2.4 (2012): 39-49.
[12] Daemen, Joan, and Vincent Rijmen. "AES proposal: Rijndael." (1999).
[13] Pradhan, Anita, et al. "Performance evaluation parameters of image steganography techniques." Research Advances in Integrated Navigation Systems (RAINS), International Conference on. IEEE, 2016.
[14] Lehmann, E. L.; Casella, George (1998). Theory of Point Estimation (2nd ed.). New York: Springer. ISBN 0-387-98502-6. MR 1639875.
[15] Joint Photographic Experts Group. "Standard IS 10918-1 (ITU-T T. 81)." (2001).
[16] Fridrich, Jessica, Tom Pevn, and Jan Kodovsk. "Statistically undetectable jpeg steganography: dead ends challenges, and opportunities." Proceedings of the 9th workshop on Multimedia & security. ACM, 2007.