Image Steganography by Enhanced Pixel Indicator Method Using Most Significant Bit (MSB) Compare

Vijaya Raghava Kukapalli, Dr.B. Tarakeswara Rao, Mr.B.Satyanarayana Reddy

MTech,CSE,KHIT,Prakasam

Professor,CSE,KHIT,Guntur

Associate Professor,CSE,KHIT,Guntur

***Abstract*---Steganography is one of the secure ways of protecting data. It provides secrete communication between user and client. The current paper presents an enhanced Pixel Indicator Method (PIM) by comparing three MSB bits at each pixel to embed the data. And we also use Blowfish algorithm to convert message into cipher text. By using the combination of these two techniques we can achieve greater complexity. Due to this mechanism proposed method makes the message difficult to be discovered with less distortion and embedding rates.**

Keywords: Steganography, Pixel Indicator, Blowfish, Distortions, Embedding Rates.

I. INTRODUCTION

Since the rise of the www (World Wide Web) one of the most important facts of Internet. Cryptography is one of the method through which we can achieve security. Two main methods of cryptography are encryption and decryption. By using these two techniques we can provide security for our secrete data. But there are some drawbacks in cryptography such as Brute-force attacks by which the intruders can identify the data. To avoid brute-force attacks it is necessary to have a larger key space [1]. And using Cryptanalysis the can extract the original data.

Steganography is a technique to hide the secrete information. It I related to Cryptography is just about old technique. It was used by the Ancient Greeks to hide information from other troops. The word steganography I derived from the Greek word "stegos" meaning "cover" and "grapy" meaning "writing" defining as covered writing. Essentially information hiding is the main task of steganography.

The embedding process creates a stego image which contains information. The basic method used to hide data in image is LSB technique. By using this technique we store the information in least significant bit of each pixel. One of the common encoding performed over the secret image before embedding is Huffman Encoding [2].

Steganography has two primary goals: 1) Security-It is the hidden data stored by either person or a computer.2) Capacity-It shows how much data can be hidden in a given cover image. These two goals are often in competition.

As a result, steganography started to attract the attention of computer researchers and users. In fact, the goal of steganography is to hide the important information of communication by embedding the secrete data to transmit into a digital media file such as image or text files.

II. OVERVIEW OF STEGANOGRAPHY

A. Least Significant Bit (LSB) Method

This is one of the most important and popular techniques of steganography. By this method, least significant bits of the pixel (in black & white images) or colors are used to embed secret message bits. It is a good steganography mechanism since changes in a least significant bit yield few changes in the original image.

The stego-image quality is improved by using LSB technique. In this technique, certain least significant bits of cover image are replaced with secrete data [3].

Suppose, for example, the by the American Standard Code for Information Interchange (ASCII) with the numerical value as "01000111", is replaced with the following pixel values (the underlined bits represent the embedded bits):

Pixel 1= (R=00011101, G=00111010, B=11001010) =>(R=0001110**0**, G=0011101**1**, B=1100101**0**)

Pixel 2= (R=01011001, G=10011011, B=11001110) =>(R=0101100**0**, G=1001101**0**, B=1100111**1**)

Pixel 3= (R=10010100, G=10101001, B=00110000) =>(R=1001010**1**, G=1010100**1**, B=0011000**0**)

The LSB approaches are divided into two fixed- and variable-length categories [4]. By the fixed-length methods, a given number of least significant bits of a byte are selected for embedding the data. In the variable-length method an assortment numbers of least significant bits of the proposed byte are chosen [5]. Cleanness and the pace of little changes in the portrait are the advantages of these techniques, while the disadvantage includes the chance of fast revealing.

B. Pixel Indicator Process

Adnan Gutub(2010)[6] in reference developed a method where a single color among three color components of a pixel was served as the pixel indicator; meaning that it indicates which colors in the pixel contains hiding bits of a secret message. Random values are selected for the indicator of each pixel, based on which message bits are placed in other colors of that pixel. The indicator uses two bits inserted inside two least significant bits of a specific color considered as the indicator. To increase the security of this technique, the color chosen as the pixel indicator is varied, so in the first pixel, Red is the indicator, Green is Channel 1, and Blue is Channel 2. For second pixel, Green is the indicator for pixel, Red and Blue act as Channel 1 and Channel 2, respectively. Finally, in third pixel, Blue is the indicator, while Red and Green act as Channel 1,Channel 2. The embedding of message is flowcharted in Figure 1.Pixel Indicator Embedding Process Because of the application of indicator; this method needs a wide space and, obviously, registration of color

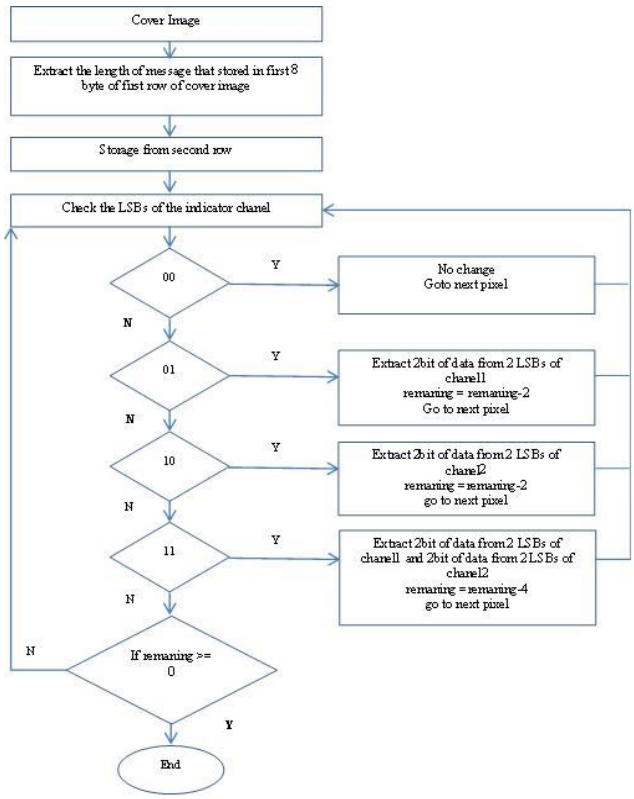

Figure 1: Pixel indicator embedding process

The study uses the basic model of LSB swap along with Pixel Indicator and follows the same but with different think [7].Two such methods are described here: one with evade indicator and other with recurring indicator. LSB swap offers enhanced quality and capacity. On the words, confidential data is entrenched in data channels by modifying the cover image bits.

In his propose method we first estimate the mean and standard deviation of every pixel if the entire image. The accidental traversing path is used for embedding to increase messiness .The representation for this study is given by the author.

Before embedding process starts up, each cover image submits itself to control by means of translation of matrix and modulo [8].Hence the cover image undergoes successive alterations even before embedding. The plan of calculating mean and also standard deviation increases the difficulty of embedding rates.

III. PROPOSED SOLUTION

The study uses the primary concept of LSB swap along with Pixel Indicator and follows the same but with different methodology .The technique uses the MSB bit of RGB channels of a pixel. The channels can be choose in random (or) in sequence i.e. RGB, RBG etc soon [9] .However the indicated MSB bits are available at random based on image size, quality and its properties. The relationship between the hidden data in 3 channels is shown in Table 1. Indicator values based action.

TABLE 1: INDICATOR VALUES BASED ACTION

Indicator Channels RGB(MSB) bits	Channel 1(R)	Channel 2(G)	Channel 3(B)
000	1-bits of secret data	1-bits of secret data	1-bits of secret data
001	No secret data	No secret data	1-bits of secret data
010	No secret data	1-bits of secret data	No secret data
011	No secret data	1-bits of hidden data	1-bits of secret data
100	1-bits of secret data	No secret data	No secret data
101	1-bits of secret data	No secret data	1-bits of secret data
110	1-bits of secret data	1-bits of secret data	No secret data
111	1-bits of secret data	1-bits of secret data	1-bits of secret data

We have selected the indicator channels in sequence that is Red, Green and Blue. And then we find the MSB bit of each channel to know the bits. Once we got the bits we needed then we can perform the following process. The process of encryption and decryption takes place before hiding and after retrieving original information. During the encryption and decryption both sender and receiver uses same key/password.

The encryption technique we used here is Blowfish which is having key length from 32 bits to 448 bits and it uses symmetric block cipher. Blowfish is developed in 1993 by Bruce Schneier as an alternative to existing algorithms.

Blowfish algorithm [10] is a Feistel Network in which there are 16 rounds. In each round different sub keys are used. The block size is of 64 bits and key can be any length up to 448 bits.

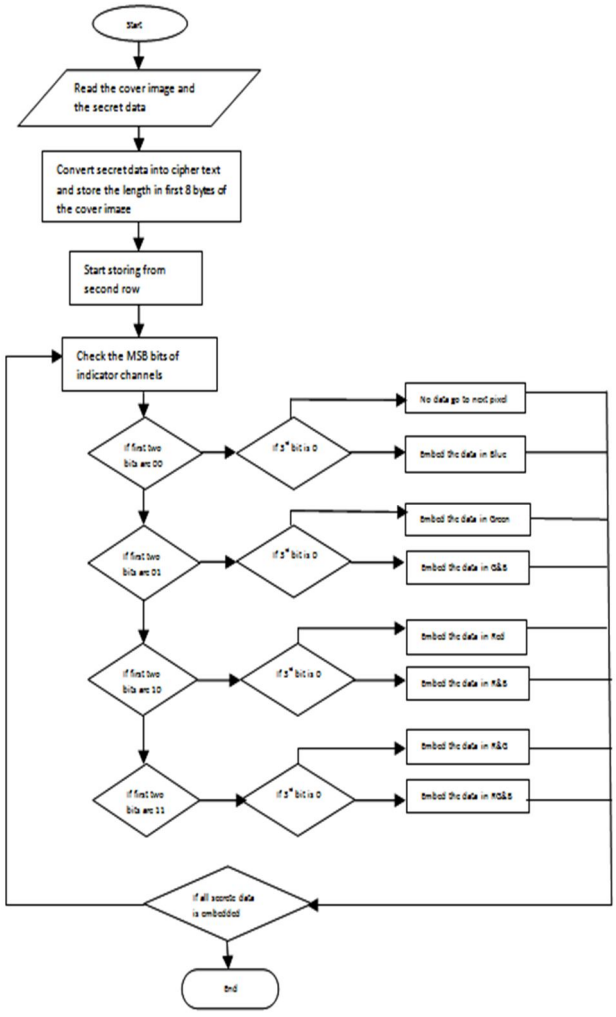

Figure-2: Flow chart for embedding data

I. *Algorithm for embedding*

- Read the cover image(C) and secrete data to be embedded (D).
- Converting the secrete data into cipher text using BLOWFISH algorithm.
- Extract the length of the secrete data and store it in first 8 bytes.
- Divide each pixel into R, G, and B planes.
- And find the MSB bits of the 3 planes.

- By using the Tabel-1 select the channels where you want to store data.
- Repeat the process till all the secrete data is stored.
- Store the resultant stego image.

B. *Algorithm for Extraction*

- Read the stego image.
- Split the pixel into RGB channels and find the MSB bit of each channel.
- Compare the retrieved bits with the Table 1 to find the channels that contain data.
- Now get the encrypted data and perform the decryption process to get original data.
- Repeat the process until the all data is retrieved.

IV. RESULTS AND DISCUSSION

The technique was implemented and tested in java. The technique accepts all mainly JPEG, PNG; BMP images of size 260×349.We can select a bmp image for testing the proposed Enhanced PIT algorithm. The PIT method is compared with the Stegoimage-1bit, Stegoimage-2bit, Stegoimage-3bit, Stegoimage-4bit. The approximate BMP image size used is 512 X 384 used to veil a text message of 11,733 characters length. The algorithm is used to hide 1-bit, 2-bits, to find the effect of transparency, security and capacity. Tests results showed different levels of diagrammatic inspections and histograms based study. For influence obligation the numbers of pixels used are recorded in each trial run.

Figure 3: Original image

Figure 4: Stego image

Higher PSNR (Peak Signal-to-Noise Ratio) [11] indicates that the steganography images are of high feature and does not hunt for the interest of the intruder because if zilch image artifacts. MSE (Mean Squared Error) and PSNR (Peak Signal-to-Noise Ratio) are given by:

$$MSE=\frac{1}{MN}\sum_{i=1}^{M}\sum_{i=1}^{N}(C_{i,j}-S_{i,j})2$$

Where

M, N=Dimensions of the image.

Ci,j=The pixels in the original image.

Si,j=The pixels of the stego image.

$$PSNR=10\log_{10}(I_{max}^2/M_{SE})\ DB$$

Where, for color image I_{max}=255.

V. CONCLUSION

The current paper provided a technique by exploiting differences made between colors to embed message bits in two least significant bits. Since color selection is based on color differences and values of variable N, the message will be hard to detect. Furthermore, as there is no need to insert additional information, changes in image will be small and image quality will be higher. Another important point to be mentioned is that embedding which is first applied on first least significant bits and, then, second least significant bits yields few changes in the original image for messages with small sizes. Because changes in second least significant bits will make more changes in color values. Therefore, it is likely to be avoided, unless this approach needs to be worked.

ACKNOWLEDGEMENT

First and foremost, I would like to be grateful Dr. B. Tarakeshwar Rao for his most support and encouragement. He benevolently read my paper and offered valuable meticulous advices on grammar, association, and the idea of the paper.

Finally, I honestly thank to my parents and friends.

REFERENCES

[1] Enhanced chaotic key-based algorithm for low-entropy image encryptionYavuz, E.Yazici, R. Kasapbasi,M.C.Yamac, E.Signal Processing and Communications Applications Conference(SIU), s201422nd DOI: 10.1109/SIU.2014.6830246Publication Year: 2014, Page(s): 385 - 388

[2] A novel steganography method for image based on Huffman EncodingDas, R. ; Tuithung, T.Emerging Trends and Applications in Computer Science (NCETACS), 2012, 3rdNationalConference n DOI: 10.1109/NCETACS.2012.6203290 Publication Year: 2012, Page(s): 14 - 18.

[3] Enhancing the Security and Quality of LSB Based ImageSteganographyAkhtar, N. Johri,P. Khan,S.Computational Intelligence and Communication Networks (CICN), 20135th International Conferenceon DOI: 10.1109/CICN.2013.85 Publication Year: 2013 , Page(s): 385 - 390

[4] Potdar, Vidyasagar M., Song Han, and Elizabeth Chang,"Finger printed secret sharing steganography for toughness against image crop attacks", INDIN'05. 2005 3rd IEEE International Conference, 2005, pp. 717-724.

[5] Lou, Der-Chyuan, and Jiang-Lung Liu, "Steganographic method for secure communications", Computers & Security 21, no. 5, 2002, pp. 449-460.

[6] Gutub, Adnan, Mahmoud Ankeer, Muhammad Abu-Ghalioun, AbdulrahmanShaheen, and AleemAlvi, "Pixel indicator soaring capacity performance for RGB image based Steganography", WoSPA 2008-5th IEEE International.

[7] Evaluating image steganography techniques: Future research challenges Roy,Ratnakirti Changder,Suvamoy ; Sarkar,Anirban ; Debnath,NarayanComputi ng, Management and Telecommunications (ComManTel), 2013 International Conference,on DOI: 10.1109/ComManTel.2013.6482411
Publication Year: 2013 , Page(s): 309 – 314.

[8]Free vibration analysis of circular cylindrical shells using transfer matrix methodGuanmoXie Electric Information and Control Engineering (ICEICE), 2011 International Conferenceon DOI: 10.1109/ICEICE.2011.5778195 Publication Year: 2011 , Page(s): 423 – 426.

[9] RGB based dual key image steganography Dagar, S.Confluence 2013: The Next Generation Information Technology Summit (4th International Conference) DOI: 10.1049/cp.2013.2334 Publication Year: 2013, Page(s): 316 - 320

[10] Security analysis of blowfish algorithmAlabaichi, A. ; Ahmad, F. ; Mahmod, R.
Informatics and Applications (ICIA), 2013 Second International Conference on DOI: 10.1109/ICoIA.2013.6650222 Publication Year: 2013 , Page(s): 12 – 18.

[11] Stego image quality and the reliability of PSNRAlmohammad, A. ; Ghinea, G.
Image Processing Theory Tools and Applications (IPTA), 2010 2nd International Conference on DOI: 10.1109/IPTA.2010.5586786 Publication Year: 2010 , Page(s): 215 – 220.