ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
Available online at www.ijarbest.com

International Journal of Advanced Research in Biology Ecology Science and Technology (IJARBEST)
Vol. I, Special Issue I, August 2015 in association with VEL TECH HIGH TECH DR. RANGARAJAN DR. SAKUNTHALA ENGINEERING COLLEGE, CHENNAI
National Conference on Recent Technologies for Sustainable Development 2015 [RECHZIG'15] - 28th August 2015

Data Hiding using Efficient Steganography Techniques

[1]MRS.QUEENMARY VIDHYA [2]R.SWATHILAKSHMI1,[3]G.SHYLAJAY
[1] ASSISTANT PROFESSOR [2,3] UG SCHOLAR ,
VEL TECH HIGH TECH DR.RANGARAJAN DR.SAKUNTHALA ENGINEERING COLLEGE, CHENNAI
[1]swathi8675@gmail.com [2]gshylu05@gmail.com

Abstract

Steganography utilize the images as cover media to hide secret data. It is one of the secure ways of protecting data. It provides secrete communication between user and client. The common technique used in this field replaces the least significant bits (LSB) of image pixels with intended secret bits.The simplest methodology to hiding the data within an image is called LSB substitution method LSB substitution method take the binary representation of hidden data and overwrite the LSB of each byte with in a cover image. In existing method, there using cover image of 256*256 and they splited the image into four parts then they are using LSB substitution and pixel indicator in zigzag manner. They are achieved stegoimage with PSNR of greater than 50 DB and also the MSE value of existing method is low. In the proposed method, we are going to flip the image into 8 parts. By using pixel indicator and LSB substitution method we are trying to achieve the stego-image having greater than 60 DB PSNR value and lower MSE value. This type of embedding technique making it difficult for any attacker to extract the hidden data from the stego-image. Peak Signal-toNoise Ratio is used to measure the quality of the stego- image. The proposed method provides better PSNR value than the existing systems

.

Keywords: Pixel Indicators, Zigzag method, LSB.

I.Introduction

Steganography are the preferred techniques for protecting the transmitted data. Steganography is very closely related to cryptography, both are used to maintain the data in a confidential manner. . Steganography on the other hand, hides the existence of a secret message and in the best case nobody can see that both parties are communicating in secret. Today, with the explosion of internet users and its vast applications, Steganography on the *World Wide Web* (www), is used by governments for secure communication and to hide information from other governments. The techniques employed in Steganography are domain tools or easy system such as least significant bit (LSB) insertion. Data hiding is a technique of concealing secret messages into a cover-media such that an unintended observer will not be aware of the existence of the hidden messages. Cover-images with the secret messages embedded in them are called stego-images.

LSB technique uses the least significant bit of consecutive pixels for embedding the message which draws suspicion to transmission of a hidden message. The pixel indicator technique (PIT) proposed in this work is for Steganography utilizing RGB images as cover media. The technique uses least two significant bits of one of the channels Red, Green or Blue as an indicator of secret data existence in the other two channels. To improve security; the indicator channel is not fixed. The indicators are chosen based on a sequence. There are two types of pixel indicators used (**i**) Default, (**ii**) User Defined. if the first indicator selection is the Red channel in the pixel, the Green is channel 1 and the Blue is the channel 2 i.e. the sequence is RGB. In the second pixel if we select, Green as the indicator, then Red is channel 1 and Blue is channel 2 i.e. the sequence is GRB. If in third pixel Blue is the indicator, then Red is channel 1 and Green is channel 2 i.e. the sequence is BRG. Based on the indicators used the secret data can be embedded into the LSB of cover image. The embedding process is done in Zigzag manner and the resulting image is called stego-image. The aim of the proposed system is to achieve better PSNR than the existing systems.

II. PROPOSED METHODOLOGY:

In the proposed system, Secret data is embedded into the LSB of the cover imageIt is depending upon the pixel indicators used in a Zigzag manner. The aim of the proposed system is to provide a high security by achieving maximum PSNR value. ***A. Methodology:***

The methodologies used for data hiding includes LSB substitution, Pixel Indicators and Zigzag embedding methods. The cover image is used to hide the secret data. The cover image is a RGB image, it is 24 bit depth colour image using RGB colour model. 24 bit in RGB colour model refers to 8 bit for each RGB colour channel, i.e. 8 bits for red, 8 bits for green and 8 bits for blue. This implies that we can store three bits of information per pixel at the LSB of RGB image. It is having high embedding capacity. The cover image considered here is having the size of (256*256).First the cover image is divided into eight sub images. After dividing it into eight parts of sub images the size of each sub images is (32*32).These sub images are further subdivided into three planes (R, G, B).Then different Pixel indicators are applied in each sub image in a zigzag manner. Based on the pixel indicators applied in each sub image the secret data is embedded into LSB of the cover image by using LSB substitution method.

1) LSB Substitution method:

LSB substitution method for information embedding and modified forms of Arnold transform are applied twice in two different phases to ensure security.It uses the least significant bit of consecutive pixels for embedding the message which draws suspicion to transmission of a hidden message. LSB technique is the most widely used as it is simple.

LSB method comes under substitution techniques of Steganography. For hiding maximum data more than one LSB can be modified. The LSB substitution method is a versatile technique for Steganography and can be used for various file formats. The basic idea here is to embed the secret message in the least significant bits of images. In this technique, the message is stored in the LSB of the pixels. Therefore altering them does not significantly affect the quality of the cover image. The procedure for such technique is to convert the desired hidden message into binary form and then encrypt each digit into a least significant bit of the data image.

2) Pixel indicators method:

Pixel indicator method 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. If the bit is 0 means no data hidden inside the channels. If the bit is 1,it indicates the channel contains hidden data.

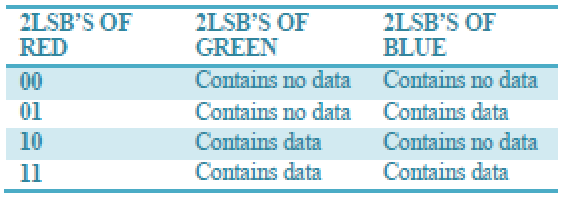
There are two types of pixel indicators. They are,

(i) Default

(ii) User defined.

Table I

Relation between the pixel indicators



2LSB'S OF RED	2LSB'S OF GREEN	2LSB'S OF BLUE
00	Contains no data	Contains no data
01	Contains no data	Contains data
10	Contains data	Contains no data
11	Contains data	Contains data

In the *Default pixel indicator*, Red is assigned as a default indicator. It is denoted as channel one. The two least significant bits of the red channel will be used as a indication to the existence of hidden information in green channel and blue channel. Green is denoted as channel two and blue is denoted as channel three.

In *User defined Pixel indicator*, among the three channels (R, G, B) any one is used as a indicator channel. Based on the chosen indicator's last two least significant bits the secret data is embedded in to the other two channels .Here 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 is Channel 1 and Green is Channel 2.

B.Algorithm implementation for proposed method

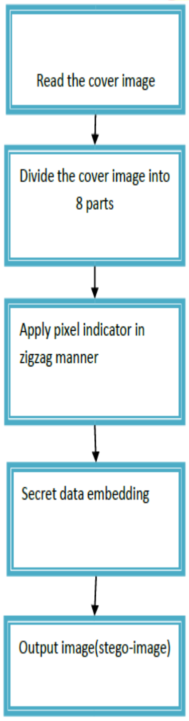

Read the cover image
Divide the cover image into 8 parts
Apply pixel indicator in zigzag manner
Secret data embedding
Output image(stego-image)

Fig 1.algorithm implementation for proposed method

III.TESTING PROCEDURE

The testing procedure is involved using two techniques: i.PSNR(Peak Signal to Noise Ratio) ii.MSE(Mean Square Error)

A.PSNR(Peak Signal to Noise Ratio) PSNR is most commonly used to measure the quality of reconstruction of lossy compression codecs (e.g., for image compression). The signal in this case is the original data, and the noise is the error introduced by compression. When comparing compression codecs, PSNR is an *approximation* to human perception of reconstruction quality. Although a higher PSNR generally indicates that the reconstruction is of higher quality, in some cases it may not. One has to be extremely careful with the range of validity of this metric; it is only conclusively valid when it is used to compare results from the same codec (or codec type) and same content.

The PSNR (in dB) is defined as:

PSNR= 10log10 (Imax2/ MSE)DB

Where, I max = maximum intensity value of each pixel.

MSE = Mean square error.

B.Mean square error:

The MSE (Mean Square Error) is the cumulative squared error between the compressed and the original image. A lower value for MSE means lesser error, and as seen from the inverse relation between the MSE and PSNR, this results to a high value of

PSNR. It is defined by,MSE= Where, X i, j is the original image,

Y i, j is the stego-image,

M, N is the dimensions of the images

IV. SIMULATION AND EXPERIMENTAL RESULTS FOR EXISTING METHOD

A. Simulation

The simulation is done by using Mat lab (7.9 or higher) version. The secret data of size 16.9kb & 18.4kb is embedded in the cover image of dimension (256*256).The cover images taken here is Lena.jpg of size 15.6kb.

The input image taken here is Lena and and it shows

Fig 2.lena image simulation result for existing Stego-lena image:

method

1) Lena Image

Lena image taken here is having dimension (256*256).First it is divided into 4 sub images. After dividing into three planes(R,G,B) the secret data is embedded into the LSB of the Lena image based on the Pixel indicator applied in a Zigzag manner.

TABLEII

PSNR AND MSE VALUES FOR EXISTIG METHOD

COVER IMAGE	K=2	K=3
LENA IMAGE FOR PSNR	56.6434	53.7184
LENA IMAGE FOR MSE	0.1805	0.1809

Table shows the PSNR (Peak to Signal Noise Ratio) and MSE(Mean Square Error) values obtained in the proposedapproach Zigzag Pixel indicator based data hiding method. PSNR value obtained in the existing method is greater than 50 dB. There are 3 cases (k=2,k=3) and this yield higher PSNR value.50 DB and lower MSE value.

V.CONCLUSION

In existing method, they divided the cover image into 4 parts and achieved PSNR value greater than 50 DB. But in our proposed method we are going to divide the cover image into 8 parts to achieve PSNR value greater than 60 DB. There are two data hiding methods are proposed. They are pixel indicator and LSB substitution method. The contributions of the proposed method are summarized as follows: in the first step the cover image is divided into eight sub images. Then Pixel Indicator method is applied in a Zigzag manner .in the second step based on the applied Pixel Indicators the secret data is embedded into the LSB of the cover image using LSB substitution method. Finally the proposed method Secret data hiding based on Zigzag Pixel Indicator Method provide a high quality stego-image with PSNR of greater than 60 dB and also provide better security than the existing methods.

REFERENCES

[1] Islam, M.R; Siddiqa, A. ; Uddin, M.P. ; Mandal, A.K ; Hossain, M.D" An efficient filtering based approach improving LSB image steganography using status bit along with AES cryptography" Hajee Mohammad Danesh Sci. & Technol. Univ. (HSTU), **ISBN:**978-1-4799-5179-6,2014.

[2] **Geetha.C.R ; Basavaraju, S.; Puttamadappa, C. "Variable load image steganography using multiple edge detection and minimum error replacement**

method", Information & Communication Technologies (ICT),ISBN: 978-1-4673-5759-3, 2013 IEEE Conference.

[3] Amitava Nag, Saswati Ghosh,"An Image

Steganography Technique using X-Box Mapping," IEEEInternational Conference On Advances In Engineering, Science And Management (ICAESM -2012) March 30, 31, 2012 ,ISBN: 978-81-909042-2-3.

[4] Kulkarni, S.A ; Patil, S.B,"A robust encryption method for speech data hiding in digital images for optimized security", Instrum. & Control, Cummins Coll. of Eng. for Women, **INSPEC Accession Number:**15058353,2015.

[5] Gupta, P.K; Roy, R. ; Changder, S.;" A secure image steganography technique with moderately higher significant bit embedding" Computer Communication and Informatics (ICCCI), 2014 International Conference on 3-5 Jan. 2014, **ISBN:**978-1-4799-2353-3.

[6] Mahimah. P; Kurinji, R."Zigzag pixel indicator based secret data hiding method" Computational Intelligence and Computing Research (ICCIC), IEEE International Conference on 26-28 Dec. **ISBN:**978-1-4799-1594-1.