HISTOGRAM TECHNIQUE WITH PIXEL INDICATOR FOR HIGH FIDELITY STEGANOGRAPHY

V.Meiamai[#1], A.Minu[#1], R.Anushia Devi[*2]
[#1]Department School of Computing, SASTRA University, Thanjavur,TamilNadu, India.
[*2] Asst Prof II, School of Computing, SASTRA University, Thanjavur,TamilNadu India.
[1] meiamai.v@gmail.com
[1] minu2391@gmail.com
[2] anushiadevi@it.sastra.edu

***ABSTRACT*- In this current world of increasing technology trends and the "internet age", the security of our personal information has become more important than it has ever been there are media reports of identity theft and fraud and the numbers of innocent victims are increasing exponentially. Steganography plays an important role in preventing such information destruction by implementing a principle of imperceptible secret sharing. By this security can be established by clearly embedding data in such a way that the quality of the image is not affected. The existing methodology prevailing now is based on pixel indicator and number of data to be embedded is by pixel value differencing technique. A limitation in this methodology is that the pixel indicator channel is manually selected. The proposed methodology uses pixel indicator channel which is decided using histogram technique and the secret message file has to be embedded in the plane which has the highest color intensity.**

Keywords: Information hiding, LSB Steganography.

I.INTRODUCTION

Information hiding is a technique for providing security to the communication channel thereby preventing attackers from hacking our personal data. A third person who is watching the communication should not be able to decipher whether the sender is sending any additional information along with the cover. It is a "multilevel secure" system used by military organizations. To prevent information sabotage various technologies are adopted like cryptography, water marking, finger printing and steganography. Most of the precedent algorithms have been cracked easily by hackers thus increasing the necessity for an impregnable algorithm. In this context, steganography extends its helping hand to protect secrets by hiding information in video, audio, digital image, etc which in turn is very hard to be hacked or cracked. If the presence of some secret message file is suspected then the purpose of steganography will be defeated, however its strength can be maximized by using it with cryptography. The cover of steganography can be an image, audio or video. In steganography the original image is called as the cover image and the image after embedding the secret message file is called the stego image which will be passed to the receiver through a communication medium. This way, the secret data will travel from sender to the receiver safely.

II.EXISTING METHOD

In this approach the color image is used as the cover object. Color image is divided into red plane, green plane, blue planes. It uses pixel indicator methodology to select a pixel and the number of bits that needs to be embedded in the selected pixel is decided using Pixel value differencing (PVD) methodology. The secret message file is embedded in the channel which is designed to be selected manually.

III.PROPOSED METHOD

The entire cover image will be divided into red, green and blue plane. In this paper we are choosing the pixel indicator channel by comparing the color planes which is having the highest intensity decided using histogram technique. The data is embedded in the chosen pixel indicator channel plane using Least Significant Bit (LSB) substitution technique. In order to increase the security, a 8-bit key is passed and encrypted with the stego-image using TripleDES Cryptographic algorithm. Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) are used to measure distortion in the stego image. Lower the value of MSE and higher the value of PSNR makes the image quality better. These methodologies incorporate reduction of detectability and increase of entropy at the same time.

IV. METHODOLOGY

4.1. COMPUTING HISTOGRAM:

The cover image is divided into three planes namely, Red (R), Green (G) and Blue (B).Histogram of Color

image is obtained in order to find the color intensity for these RGB planes. Then the plane having maximum color intensity is decided as a Pixel Indicator Channel (PI).

4.2. TEXT EMBEDDING TECHNIQUE:

A mean is computed for the pixels in the Pixel Indicator Channel. The Secret data will be embedded in the computed mean value of Pixels. Embedding technique used in this methodology is Least Significant Bit (LSB) Substitution.

According to LSB Substitution, the secret message file and the cover image is converted into Binary format. XOR operation is performed for the Binary data and the resultant binary will be converted to decimal and will be stored in the cover image which is called as Stego image with secret data embedded in it.

4.3. SECURITY ENHANCEMENT:

The security for this methodology can be improved by generating and authenticating the key. Hence, only authorized user can recover the secret message file. This can be achieved in this methodology by using a 8-bit key and can be implemented by Data Encryption (DES) Cryptographic Algorithm.

According to DES Cryptographic Algorithm, for a 64-bit block of plaintext, initial permutation is carried out and the block are divided into a left half and right half of 32 bits long. Following that 16 rounds of identical operations along with the key is performed. After the completion of sixteenth round, the left and right halves will be combined and the final permutation will end the algorithm.

4.4. TEXT RETRIEVAL TECHNIQUE:

After the Authentication of key, Authorized user can retrieve the secret message file by uploading the Stego image and following the reverse process of Text embedding Technique.

4.5. ERROR METRICS:

The distortion in the Stego image can be calculated by Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR).The lower the value of MSE and Higher the value of PSNR will make the quality of the image better. For this proposed methodology MSE and PSNR value is analyzed and reported in TABLE-1 and a Histogram of the image is reported in FIG-3.

V. ALGORITHM

1. Read the Cover image.
2. Find the Histogram of the Cover image.
3. Compare Color planes and choose the highest Color intensity as Pixel Indicator Channel.
4. Read the message file to be hidden.
5. Convert the message file from decimal to binary.
6. Convert the Cover image from decimal to binary.
7. Divide the byte to be hidden into bits.
8. Take first 8-byte of the pixel from the cover image and replace the least significant bit by one bit of the data to be hidden.
9. Data is embedded in chosen pixel indicator channel plane of cover image and resulting image is Stego image.
10. In Stego image, key is encrypted using DES CRYPTOGRAPHIC technique.
11. Authenticate the Key.
12. Reverse process is followed for the decryption of secret message.

VI.RESULTS AND DISCUSSION

To prove the effectiveness of the stego process PSNR and MSE values are calculated. The value of PSNR and MSE is calculated using the following equations

$$MSE = \frac{1}{m\,n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

$$PSNR = 10\log_{10}\left(\frac{R^2}{MSE}\right)$$

COVER IMAGE	CHANNEL-1 (RED)		CHANNEL-2 (GREEN)		CHANNEL-3 (BLUE)	
	MSE	PSNR	MSE	PSNR	MSE	PSNR
BIG TEMPLE	0.0418	61.9180	0.0396	62.1558	0.0239	64.3477
LENA	0.0285	63.5820	0.0314	63.1558	0.0528	60.9071
BABOON	0.0388	62.2384	0.0388	62.2448	0.0260	63.9852
GANDHI	0.8704	48.7334	0.9898	48.1755	0.9446	48.3785

TABLE-1

FIG-1.Original image(Big Temple,Lena,Baboon,Gandhi)

FIG-2.Stego image(Big Temple,Lena,Baboon,Gandhi)

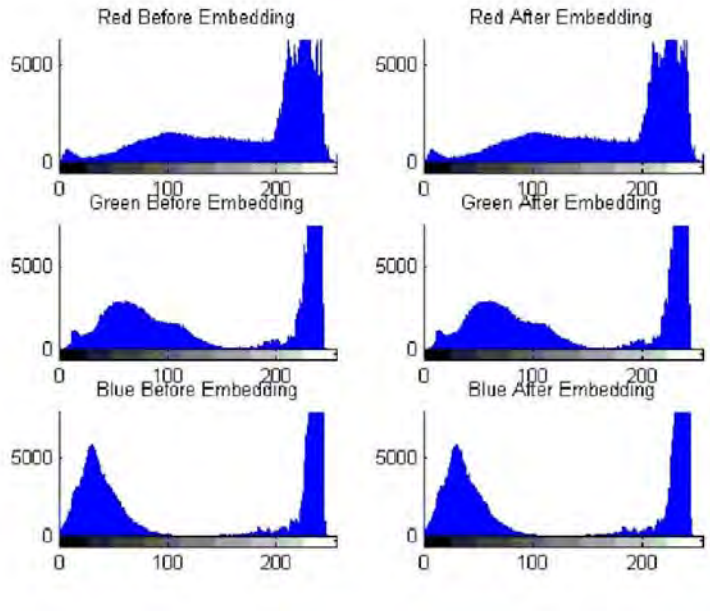

FIG-3.Histogram Analysis of Big Temple

VII. CONCLUSION

The process of embedding data using histogram technique has eliminated manual selection of pixel indicator channel thus making it flexible and more efficient. The Mean Square error has decreased thus making it difficult to distinguish with the cover image. By this method maximum number of bits can be embedded in the cover medium. The efficiency of this method can be enhanced by authenticating the user with a key. This provides

increased security to the communication channel.

REFERENCES

[1] Amirtharajan.R, Adarsh.D, Vignesh.V and John Bosco Balaguru.R,"PVD blend with Pixel Indicator -OPAP composite for high fidelity Steganography".

[2] C.K.Chan,L.M.Chen,Hiding data in images by simple LSB substitution, Pattern Recognition 37(3)(2004)469-474

[3] Abbas Cheddad, Joan Condell, Kevin Curran, Paul Mc Kevitt, "Digital image steganography: Survey and analysis of current methods Signal Processing" 90, 2010,pp. 727752.

[4] W. [4] Bender, D. Gruhl, N. Morimoto, A. Lu, "Techniques for data hiding " IBM Syst. 1. 35 (3&4) ,1996, 313-336.

[5] S.Katzenbeisser,F.A.P.Petitcolas,Information HidingTechniquesforSteganographyandDigital Watermarking,Artech House,Norwood,MA,2000.

[6] Xinpeng Zhang,Shuozhong Wang.,Vulnerability of pixel value differencing steganography to histogram analysis and modification for enhanced security(2003)331-339.

[7] Cheng-Hsing Yang, "Inverted pattern approach to improve image quality of information hiding by LSB substitution", Pattern Recognition 41(2008)2674-2683.

[8] Amirtharajan R.; Mahalakshmi, V.; Sridharan, N.; Chandrasekar, M.; Rayappan, J.B."Modulation of hiding intensity by channel intensity - Stego by pixel commando", International Conference on Computing, Electronics and Electrical Technologies [ICCEET] 2012 .

[9] Lisa.M.Marvel and Charles T.Retter,"A Methodology for Data Hiding using Images,"IEEE conference on Military communication,vol.3,Issue.18-21,pp.1044-1047,1998.

[10] Wang,R.Z.,Lin,C.F.,Lin,J.C.,2001.Image hiding by optimal LSB substitution and genetic algorithm. Pattern Recognition 34(March),671-683.