ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 5, Issue 1, January 2016

An Image Steganographic Scheme for Data Hiding Security by Considering Diagonally Three Pixel Pair Blocks

Vidya S Shirguppi

***Abstract*—In the proposed technique the aim is to store information by hiding that information's existence. Which carries out hidden exchanges and can enhance individual privacy? This Method uses four pixel pair from which are diagonally consider i.e. first pair and second pair are used and fourth pair is unused. Based on certain design criteria's such as Data Embedding, Data Extraction processes are used for security against unwanted users and hackers. For this different algorithms have been evaluated. This method reduces the weaknesses and explores the strengths for image steganographic techniques which will enable us to design a better steganographic algorithm.**

***Keywords*—**Steganography Techniques, Embedding Process, Extraction Process, Comparison PVD, TPVD.

I. INTRODUCTION

In our day to day life a security has become most important aspect for which certain measures has to be taken the security may be any form. Such like this We use internet for daily communication in which we transmit, receive various kind of Private data Where the goal is to secure communications from an eavesdropper, for this steganographic techniques is used to hide the very presence of the message itself from an observer. The most common way carried out to transform the data into a different form are Information hiding and cryptography are two main ways to secured communication.

In this paper I have proposed a new method which is uses a steganographic image of different sizes and text in which the text is hided into an image, without any changes in the original image or cover image and this is done by using the Triway-Pixel value differencing method. Here I have designed some algorithm through which private text data is hidden behind the original image that is cover image and send by using the TPVD Method. Then after embedding process the same image is generated which is called as stego image is which is approximately as same as original image. At the time of extraction by use of algorithm we can separate image and text data.

Department of Electronics & Telecommunication Engineering, D.Y. Patil College of Engineering & Technology, Kolhapur

Many different methods of hiding information in images exist. In a method of hiding information in images includes application of transform domain such as *Discrete Cosine Transform* (DCT) [7].The information hiding technique can be extensively used on applications of military, commercials, anti-criminal, and so on [1]. Many steganographic methods have been proposed to hide the secret data into the image. One of the common methods is called Least-Significant Difference value. Then find the optimal Reference point and Difference value of pixel pair. Now the embedded block is obtained from the above value and the combination of cover image & Secret data forms a stego-image.

The rest of the paper is organized as follows: We will review Wu and Tsai's method in Section 2. Next, our scheme will be presented in Section3. The experimental results in Section 4. Show that our scheme is feasible .Furthermore, we will depict analyses and discussions of the proposed method and Wu and Tsai's method in Section 5.Finally, conclusions are given in Section 6.

II. PREVIOUS WORK

In Wu-Tsai's steganographic method, a gray-valued cover image is partitioned into non-overlapping blocks of two consecutive pixels, states pi and pi+1.[14] A difference value is calculated from the values of the two pixels in each block. All possible difference values are classified into a number of ranges. The selection of the range intervals is based on the characteristics of human visions sensitivity to gray value variations from smoothness to contrast. The difference value then is replaced by a new value to embed the value of a sub-stream of the secret message. The number of bits which can be

embedded in a pixel pair is decided by the width of the range that the difference value belongs to.[1] The method is designed in such a way

III. SYSTEM MODEL

By the use of this techniques the system is able to enlarge the capacity of the hidden secret information and to Disposes an imperceptible stego-image for human vision. In this system the following block of system is given, each one carries a different function as follows.

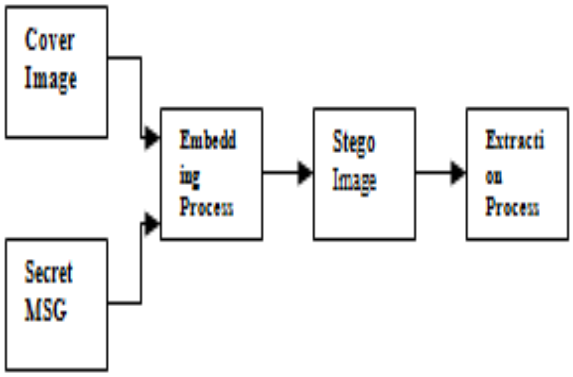

Figure 1. Proposed System.

A. Embedding Process

In embedding process the first step is to choose image inside in which you are going to hide an text data. That image is called as the cover image, the after the private data is hided inside an image called as secret message and both are compressed together and send to embedding process in which data is converted to binary code and image is converted to bitmap.

B. Stego-Image

When the compression is done the similar image is created which is the combination of the original cover image and the Secret hidden data that is called as Stego-Image.

C. Extraction Process

To retrieve the embedded secret data from the stego image, The extraction process is carried out. Here the value is converted back to its binary form and a new difference value is generated during embedding time this difference value is subtracted from the original value and a stego image is retrieve back so that the receiver can easily found the secret hidden data.

D . Flow Chart for Embedding & Extraction Process

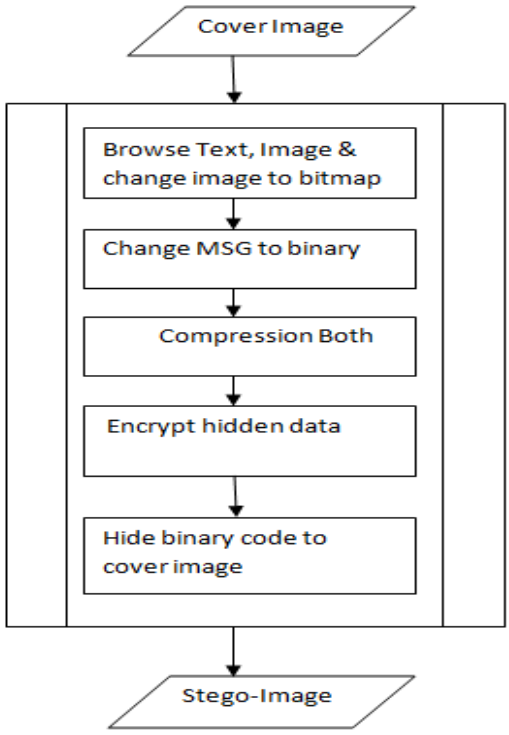

Figure 2. Flowchart of Embedding Process

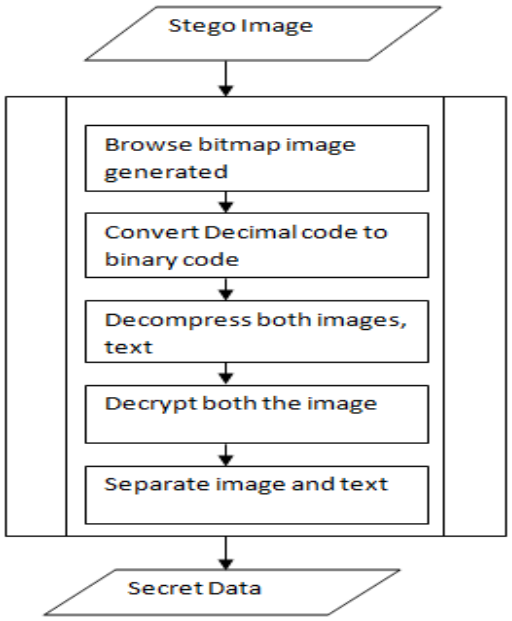

Figure .3. Flowchart of Extraction Process

The Embedding Algorithm

BEGIN

Input: Calculate four difference value designed using range table

Transfer secret MSG to text file

Convert text file to Binary_ code

Encode message to Binary_ code

Calculate new generated difference value

Output: Stego_Image

END

The Extraction Algorithm

BEGIN

Input: Partition the Block into two by two pixel pair

Convert Decimal_Code to Binary_ code

Decode message to Binary_ code

Subtract new generated difference value from original value

Output: Secret Code

END

IV. EXPERIMENTAL RESULTS

In order provide feasibility for our method which will raise the capacity of hiding with an acceptable quality of the Stego-image, we used the MATLAB program language tool to implement the proposed idea and Wu and Tsai's scheme.

A .Capacity

Capacity is calculated as in byteswhich depends upon the design criteria. The hiding capacity is more in this technique.

B. PSNR

The PSNR is peak signal noise ratio which is measure in db. The lowest PSNR value the distortion is negligible.

C.COMPARISON IMAGE RESULT FOR PROPOSED METHOD

Figure 5.a) Appearance of the selected Image; b) Appearance of the Stego Image

V CONCLUSION

I tested few images with various sizes of data to be hidden. With the proposed algorithm, I found that the stego image does not have a noticeable distortion on it (as seen by the naked eyes). I also tested our stego images using PSNR value. Based on the PSNR& Capacity value of each images for PVD & TPVD Methods the stego image has a higher Capacity & PSNR value. Hence this new steganography algorithm is very efficient to hide the data inside the image. TPVD can be used by various users who want to hide the data inside the image without revealing the data to other parties. TPVD

maintains privacy, confidentiality and accuracy of the data.

The Proposed technique gives the image quality of high standards and with the necked eyes it is impossible to find the variations in the Stego image. The result comparisons also support the statement strongly. the participation of original cover images. This has shown multiple merits of the proposed technique for data hiding.

REFERENCES:

[1] D.-C. Wu and W.-H. Tsai, "A steganographic method for images by pixel-value differences," *Pattern Recognition Letters, Vol. 24, pp. 1613–1626, 2003.*
[2] H.-C. Wu, N.-I. Wu, C.-S. Tsai and M.-S. Hwang, "Image steganographic scheme based on pixel-value differencing and LSB replacement methods," *IEEE Proceedings on Vision, Image and Signal Processing, Vol. 152, No. 5, pp. 611-615, 2005.*
[3] W. Bender, D. Gruhl, N. Morimoto, A. Lu, "Techniques for data hiding," *IBM* Systems *Journal Vol. 35 (3–4), pp. 313–336, 1996.*
[4] W.-N. Lie and L.-C. Chang, "Data hiding in images with adaptive numbers of least significant bits based on the human visual system," *IEEE International Conference on Image Processing, Vol. 1, pp. 286–290, 1999.*
[5] Ali Shariq Imran, M. Younus Javed, "A Robust Method for Encrypted Data Hiding Technique Based on Neighborhood Pixels Information," *World Academy of Science, World Academy of Science, Engineering and Technology 7 2007*
[6] Ali Shariq Imran, M. Younus Javed, and Naveed Sarfraz Khattak, "*A Robust Method for Encrypted Data Hiding Technique Based on Neighborhood Pixels Information*" World Academy of Science, Engineering and Technology 7 2007.
[7] Norishige Morimoto, "*Digital Water Marking Technology with Practical Application"*
Information Science Special Issues on Multimedia Information Technologies-Part 1 Vol 2 No 4
1999.