International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 3, Issue 11, November 2014

SECURITY ENHANCEMENT OF DATA BEFORE TRANSMISSION

Fiji Joseph[1] ,Asst.Prof.S.Sivakumar[2]
Department of Electronics and Communication
Sri Shakthi Institute Of Engineering And Technology , Coimbatore

***Abstract*-Steganography is a process that enables communication of secret data in an appropriate carrier like image, audio, video etc. It is mainly employed for providing security. Here we are discussing Adaptive Pixel Value Differencing technique as image steganographic scheme. In APVD the image is divided into blocks and then data will be hidden. If we use simple pixel value differencing as embedding algorithm then there is a possibility that the resultant stego image may exceed the grey scale range of 0 to 255.This can affect the quality of stego image which in turn causes the observer to identify that a hidden communication is happening. The main objective of this proposed work is to enhance the quality of stego image and to increase the embedding capacity.**

***Keywords*: Adaptive pixel value differencing, Data hiding, Steganography, Stego Image**

1. INTRODUCTION The electronic communication is a widely accepted means of communication. So Information security and privacy became a growing concern. Humans have continually sought new efficient secret ways to protect confidential information. In the initial stage of communication numerous methods were used to protect the confidentiality of data. First techniques included usage of invisible ink or chemicals. Other methods like templates laid over text messages, microdots, changing letter or word or line or paragraph spacing, changing fonts etc. were also used initially. Within the computer networks, confidential information are generally found in two states: stored or transmitted through the network. During data exchange, it is a basic request that only the intended recipient should be able to decipher the contents of the transmitted data. The security is mainly provided by two methods. One is cryptography and the other one is information hiding.

Under the information hiding we have watermarking and steganography. Watermarking is the process of hiding digital information in a carrier signal. Steganography is the process of hiding a message, image, or file within another image, or file.

2. STEGANOGRAPHY

The word Steganography is derived from the ancient Greek words '*steganos'* and '*graphia'*[3]. The word Steganos means covered, whereas graphia means writing. Steganography is the field that gives a meaningful way of secure data being transmitted through an open channel without the attention of eavesdroppers.

The data hiding using steganography mainly involve two process. They are Embedding process and Extracting process. The embedding process uses a cover image to embed the secret text data. The result thus obtained after embedding is known as stego image. The extracting process is used to recover the secret text data from the stego image. Here we require an extraction algorithm. The mathematical formulas are given below:

For embedding Process:

Cover Image +Secret text data=Stego Image

For Extracting Process:

Stego Image+ Extraction Algorithm=Secret Text Data

Steganography can be used for wide range of applications such as, in defense organizations for safe circulation of secret data, in military and

intelligence agencies and in smart identity cards where personal details are embedded in the photograph itself for copyright control of materials [2]. In medical imaging, patient's details are embedded within image providing protection of information and reducing transmission time and cost. It can also be used in online voting system so as to make the online election secure and robust against a variety of fraudulent behaviors. It is used for data hiding in countries where cryptography is prohibited, in improving mobile banking security, in tamper proofing so as to prevent or detect unauthorized modifications

2.2 FEATURES

Steganographic techniques have various features which characterizes their strengths and weaknesses [2]. The main features include the following:

2.2.1Embedding Capacity:

It is the amount of data that can be inserted into the cover media without deteriorating its integrity.

2.2.2Perceptual Transparency:

It is necessary that the embedding should occur without significant loss of quality of the cover image.

2.2.3Robustness:

It is the ability of embedded data to remain intact when the stego-image undergoes various transformations like scaling, rotation, cropping ,compression etc.

2.2.4Tamper Resistance:

It indicates the difficulty to change the message when it is embedded in a cover-media.

2.2.5Computational Complexity:

Computational complexity of steganography technique employed for encoding and decoding is another consideration and should be given importance. The complexity should be minimum as possible and also it should be less time consuming. So this factor plays an important role.

3. EXISTING METHOD

The existing method is Pixel Value Differencing. In PVD method, gray scale image is used as a cover image with a long bit-stream as the secret data. At first we have to partition the cover image into non-overlapping blocks of two consecutive pixels, pi and pi+1. From each block the difference value di is calculated by subtracting pi from pi+1. The set of all difference values may range from -255 to 255. Therefore, |di| ranges from 0 to 255. The blocks with small difference value locates in smooth area where as block with large difference values are the sharp edged area. According to the properties of human vision, eyes can tolerate more changes in sharp-edge area than smooth area. So, more data can be embedded into edge area than smooth areas. Therefore, in PVD method a range table has been designed with n contiguous ranges Rk (where k=1,2, …,n) where the range is 0 to 255. The lower and the upper bound are denoted as lk and uk respectively,then Rk∈[lk,uk]. The width of Rkis denoted as wk. It determines the number of bits that can be hidden in a pixel block. This width is calculated as:

$$wk = uk - lk + 1 \quad (1)$$

For security purpose Rk is kept as a variable. As a result, original range table is required to extract the embedded data.

4. PROBLEM DEFINITION

Steganography is used to hide messages in the cover of something else. During the embedding phase an algorithm is required to determine how the message is embedded. This algorithm can be more or less advanced, ranging from simple least-significant bit (LSB) embedding in the spatial domain to bit scattering in the frequency domain. The actual hiding process starts with embedding bits of the message into the cover image.Most methods in use today are invisible to an observer's senses. The mathematical analysis reveals statistical anomalies in the stego medium. These discrepancies expose the fact that hidden communication is happening. This will also make the image fidelity degrades.So, there are two important issues must be considered during the embedding process. They are:

(i) the decision of the number of bits that each pixel uses to embed message, and

(ii) analysis of the generated image

Many techniques are there to embed data bits into a cover image. In simple pixel value differencing there is a possibility that the pixel values in the stego image can exceed the grey scale range which is 0 to 255. Also there is a possibility for the quality of stego image to get affected. If the quality of stego image degrades too much then there is a possibility for the observer to easily identify that a hidden communication is occurring. So we have to avoid such situations.

5. PROPOSED METHOD

We are using APVD for overcoming the limitations of pixel value differencing. If the stego image exceeds the grey scale range improper visualization occurs. This can be avoided if we are able to limit the range of stego image within the grayscale value. This is accomplished by using an adaptive PVD steganographic scheme.In APVD method a gray scale digital image has been used as a cover image where pixel values ranged between 0 and 255 and the pixel values of stego-image will not exceed the gray scale range.

The implementation involves mainly embedding and extracting process. To evaluate the quality of stego image we calculate the PSNR (peak signal to noise ratio) and MSE (mean square error).The algorithm is given below.

5.1 Algorithm for Embedding Process:

Step 1:Start
Step 2:Select an image file of any format
Step 3:Read the image file
Step 4:Resize the image into 256 × 256
Step 5: Check whether the image is a color image. If yes go to step 6 else go to step 7
Step 6:Convert the image into grey scale
Step 7: Split the image into blocks and performs block processing
Step 8:Read the input message to be hidden
Step 9: Find out the length of the message and convert it into ascii codes. Also find out the number of bits in the message
Step 10:Convert the ascii into binary and arrange them as a column matrix
Step 11:Generate the hamming code to reduce the error
Step 12:Perform the embedding process
Step 13:Save the reshaped image
Step 14:Display the results
Step 15:Stop

5.2 Algorithm for Extracting Process:

Step 1: Start
Step 2:Load the saved image in which data is hidden
Step 3: Store it in an alternate variable
Step 4:Read the image and convert it into binary and store it as a column matrix
Step 5:Calculate the number of bits embedded
Step 6:For i=9:8:bits
(i) Convert the binary values into decimal which corresponds to the ascii value of hidden data
(ii) Convert the ascii value into Unicode
Step 7:Store the Unicode and arrange the in a row matrix and then display
Step 8:Stop

5.3 Algorithm for PSNR and MSE Calculation

Step 1: Start
Step 2:Read the image in which bits are embedded
Step 3:Read another image as reference image
Step 4:If the reference image is color image goto step 5 else goto step 6
Step 5: Convert color image into grey scale
Step 6:Resize the image
Step 7:Split the reference image into blocks of same length as that of the original image
Step 8:Calculate MSE using the formula:

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left|x_{ij} - y_{ij}\right|^2 \qquad (2)$$

Step 9:Calculate the PSNR using the formula:

$$PSNR = 10 * \log_{10}\left[\frac{L^2}{MSE}\right], where\ L = 256 \qquad (3)$$

Step 10:Display the results
Step 11:Stop

6. BLOCK DIAGRAM

The block diagram of the proposed method is as shown below.

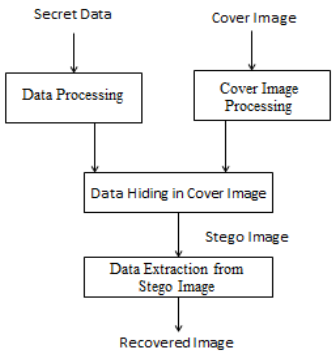

Fig 2:Block Diagram

The important operations involve secret data processing, cover image processing, data hiding and data extraction. The information that the center want to keep confidential is known as secret data. The sender may wish to limit the access to the data. In such case to keep it confidential some security should be provided. The data can be in the form of a letter, word or character etc. The data processing involves processing of this secret data. It involves calculating the number of bits in the input data and converting it into binary. This binary data is used for embedding purpose.

The cover image is one in which the secret data is hidden. The cover image should be a grey scale image. Also the pixel size should be 256×256.If the pixel size is high we have to first bring it to this range. If cover image is a color image we have to first convert it into grey scale range.

The data hiding is the process of hiding the data into the cover image and is done by an algorithm. The data extraction is the process of recovering the data bits that are hidden in the cover image. This is also done with the help of an algorithm.

7. RESULTS & ANALYSIS

Grey Scale image of size 256 × 256 pixels is taken to implement the above process. If the image that we are taking is color then we have to convert it into grey scale. Also if the size of the image exceeds the limit we have to first resize the image into 256 × 256 pixels. The performance is analyzed with the help of PSNR and MSE. The higher the value of PSNR, then greater will be its image quality. The PSNR is inversely proportional to MSE and so as PSNR increases the MSE decreases.

Figure below shows the original image. It is the image of Great Wall of China. The actual size of this image is 183 × 275.We first convert it into 256 × 256 size. For performing this operation we have an image resize function in MATLAB.

Fig 3:Original Image

Also we can notice the fact that the image is a color image. We convert this into grey scale range. The command used is rgb2grey. After the execution of this command our image will be converted into grey scale range. Before embedding we have to split the images into blocks. The resulting image is the one in which we are embedding the data. So this image is termed as the cover image. It is shown in figure 5.So before embedding the data we have to ensure the size of the cover image. If we take a grey scale image as cover image the processing operations will be rather simple.

Fig 4:rgb2grey converted image

Fig 5:Grey image splitted into blocks

The image that is used for embedding purpose is known as cover image or cover object. Here we are collecting the secret data from the user. After receiving the data which is to be kept secret we have to first find out the number of bits in it. This data is converted into ascii codes and then to their corresponding binary values. Hamming codes are also generated. Data which is in binary format is embedded into the cover image along with the hamming codes. The hamming codes enable us to reduce the error that occurs during the embedding process. The resultant image obtained after embedding is known as stego image.

Fig 6:Stego Image

After embedding we have to do extraction process inorder to get the data embedded in it.

The results obtained after the calculation of MSE and PSNR are shown in the table 1 & 2.

Table 1:PSNR & MSE Values for 24 Bit input

PARAMETER USED	OBTAINED VALUE
Peak Signal to Noise Ratio (PSNR)	60.8342
Mean Squared Error (MSE)	0.054083

Table 2: PSNR & MSE Values for 32 Bit Input

PARAMETER USED	OBTAINED VALUE
Peak Signal to Noise Ratio (PSNR)	60.7058
Mean Squared Error (MSE)	0.055706

The MSE value is very much small. This indicates that the error that occurs while embedding is also reduced. As the number of bits increases error also increases. But this increase is very much small and is negligible.This means that the quality of stego image is good. This enables us to transmit our data without the attention of eavesdroppers.

8. CONCLUSION

A Steganographic scheme using Adaptive Pixel Value Differencing is implemented using MATLAB and evaluated its performance using two parameters. The parameters are Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE).The main disadvantage of pixel value differencing is that if the image exceeds grey scale range then it will result in the improper visualization of the stego image. This problem is avoided here. The quality of stego image is also ensured. This approach yield high PSNR value and this results in reduction in the mean square error as they are inversely proportional to each other. In other steganographic schemes, as the number of bits that are to be embedded increases, the error also increases abruptly. In this approach the error does not increase that much as the number of bit increasesand is one of the great success of this work. The method presented here is applicable to the entire image format.

9. ACKNOWLEDGEMENT

First of all we sincerely thank the almighty who is most beneficent and merciful for giving us knowledge and courage to complete the project work successfully. We also express our gratitude to all the teaching and non-teaching staff of the college especially to our department for their encouragement and help done during our work. Finally, we appreciate the patience and solid support of our parents and enthusiastic friends for their encouragement and moral support for this effort.

REFERENCES

[1] J. K. Mandal and Debashis Das, "*Steganography Using Adaptive Pixel Value Differencing(APVD) of Gray Images Through Exclusion of Overflow/Underflow*", The second International

Conference onComputer Science, engineering and applications (CCSEA-2012) ,May 2012.

[2] Babloo Saha and Shuchi Sharma, "*Steganographic Techniques of Data Hiding using Digital Images*", Defence Science Journal, Vol. 62, No. 1, January 2012, pp. 11-18, DOI: 10.14429/dsj.62.1436,2012, DESIDOC.

[3] H.B.Kekre, Archana Athawale, Swarnalata Rao and Uttara Athawale, "*Information Hiding in Audio Signals*",International Journal of Computer Applications (0975 – 8887)Volume 7– No.9, October 2010.

[4] Sumedha Sirsikar and Jagruti Salunkhe,"*Steganog raphic Techniques of Data Hiding using Digital Images*", International Conference on Electronic Systems, Signal Processing and Computing Technologies,2014.

[5] Ankita Sancheti, "*Pixel Value Differencing Image Steganography Using Secret Key"* **,**International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-2, Issue-1, December 2012.

[6] Jagruti Salunkhe and Sumedha Sirsikar, "*Pixel Value Differencing a Steganographic method:A Survey*", International Journal of Computer Applications (0975 – 8887) and International Conference on Recent Trends in engineering & Technology - 2013(ICRTET'2013).

