International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 02 | Feb -2017 www.irjet.net p-ISSN: 2395-0072

Steganography System for Hiding Text and Images Using Improved LSB Method

Deepika, Er. Jasdeep Singh Mann

Deepika, Student

Er. Jasdeep Singh Mann, Assistant Professor

BMSCE, Shri Muktsar Sahib, Punjab

Abstract: *During data transfer, stealing of data by unauthorized parties is common now days. Various techniques are available to provide security to data; from which proposed system uses LSB and pseudo random encoding technique. Steganography means covered writing. The main goal of this technique is to hide existence of message from unauthorized parties by hiding it into image. The quality of proposed system is compared using various parameters like MSE, RMSE, PSNR and Capacity based on different sets of images. Our proposed system attains a PSNR of 49.32 and 94% Accuracy.*

Keywords: *Steganography, LSB, Random-key, Stegano-Key*.

1. INTRODUCTION

Digital steganography is the art and science of hiding communication. A steganography system embeds a secret data in cover media to hide its existence from unauthorized parties. A steganography system has two main aspects: steganographic capacity and imperceptibility. These two characteristics are odd to each other. It is difficult to increase the steganographic capacity simultaneous with imperceptibility. There are few methods of steganography to be used with communication protocols. Digital image steganography is method of secret communication that aims at hiding large number of secret data based on size of cover image. The main goal of stegano system is to embed secret message in cover image by choosing a random stegano key. The stegano file is created that represent the cover file with embedded message that is indistinguishable neither by human nor by computer system. An encoded message is send to receiver side along with stegano key where it is decoded to get the credential information.

2. Methods of Classification

The steganographic system is classified based on the type of cover image it use or on the method of hiding or on the basis of layout of modification used in embedding process.

2.1 Cover-Type Based Classification

There are various kind of digital media used as cover file of steganography. The properties of cover file vary from one cover file to another. The properties of these files control how the secret message can be hidden in these files. The type of cover file give us an idea that where secret message might be hidden. The different

kind of media cover files are image, audio, video and text. The system that uses video as cover image is video-based steganographic system. Our proposed system is image-based steganographic system.

2.2 Hiding Method-Based Classification

The other method on which steganographic system is classified is method used to hide secret data. There are three ways in which secret data is hided in cover files: insertion-based, substitution-based and generation-based methods.

Insertion-Based Method: This method focused on finding the areas that are usually ignored by applications that read any type of cover image and then embed secret data at that area. The main condition that is size of stegano file would be larger than the size of cover file. The main advantage of this method is that contents of cover file are unchanged after embedding process.

Substitution-Based Method: As insertion-based method, this method doesn't base on adding secret data to cover file. As its name suggests, substitution-based method finds some insignificant area in cover file and replace that information with secret data. The size of both stegano and cover file is similar because some of data is either modified or replaced without any additional data. The quality of cover file is degraded by embedding data using this method.

Generation-Based Method: This method doesn't need any cover file to embed secret data. It uses secret data to generate a stegano file. The main advantage of this method is stegano files, which are difficult to detect. While the main disadvantage of this system is that the generated stegano files might be unrealistic for end user.

3. PROPOSED ALGORITHM: The proposed system is based on cover-based method that uses digital image as cover image and hides the secret message in form of text file. The main objective of proposed system is to encode and decode the cover image using LSB (Least Significant Bit) and Random Improved LSB techniques. The proposed system comprises of two components: Embedding module and Extracting module.

Embedding Module: Embedding is the process of hiding the embedded message and generates a stegano image. Hiding of data may require a stegano key which is additional information that protects it from unauthorized parties, example-password. When secret message is hidden within cover image the resulting product is called as stegano image or stegano object.

The algorithm for above method is summarized as follows:

Step1: Input the secret text files that to be hidden in cover image.

Step2: Select the cover image from list of stored image files and text files.

Step3: Binary the text message.

Step4: Calculate the size of secret text.

Step5: Generate the Fibonacci series

a) Calculate mod.

b) If mod=0, embed in Red

c) If mod=1, embed in Green

d) If mod=2, embed in Blue

Step6: If I<=N, Then I=I+1, Else display the stegano image.

Extracting Module: Extracting is process of getting embedded message from stegano image.

The algorithm for above method is summarized as follows:

Step1: Select the stegano image.

Step2: Count the number of pixel and store in N.

Step3: Select the Ith pixel, generate Fibonacci series

Step4: Calculate mod.

b) If mod=0, extract from Red

c) If mod=1, extract from Green

d) If mod=2, extract from Blue

Step5: Add LSB into message.

Step6: If I<=N, Set I=I+1, Else generate ASCI code and display the message.

4. CONCLUSION

The main aim of steganography is to embed secret message into cover image without knowledge of unauthorized parties. The proposed system is based on achieving this aim and compares the existing and proposed system. The proposed system is tested on various set of images with different watermarks for data hiding. The proposed system gives 94% accurate results.

Table 1 Comparison of Adaptive LSB substitution method

Input Image	LSB3	Jae Giyu	Proposed System
PSNR	37.92	38.98	49.32
Accuracy	86.52	88.62	94.02

The above table shows that our proposed system shows 49.32 PSNR and accuracy of 94% which is better than the existing stegano systems.

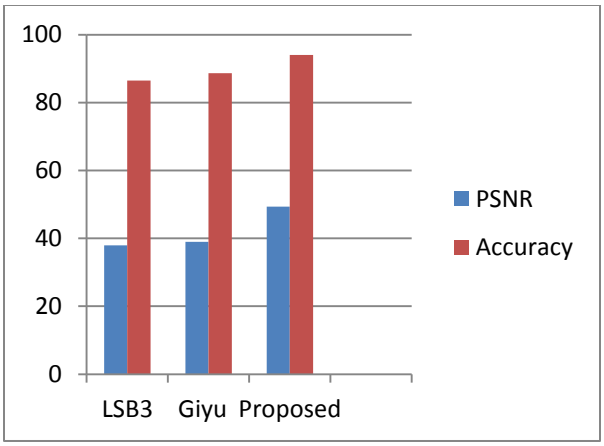

Fig 1. Bar Graph showing comparison between existing and proposed system.

The above bar graph shows two bars comparing the PSNR and Accuracy of existing and proposed system. This also show that our proposed system is much efficient than existing ones. The imperceptibility and robustness of proposed method shows better performance in comparison to other approach.

5. REFRENCES

[1] Vijay Kumar Sharma, Vishal Shrivastavaa, Steganography Algorithm for Hiding Image In Image By Improved LSB Substitution By Minimize Detection.

[2] Gurpreet Kaur, Kamaljeet Kaur, Image Watermarking Using LSB (Least Significant Bit).

[3] Amit Singh, Susheel Jain, Anurag Jain, Digital watermarking method using replacement of second Least Significant Bit(LSB) with inverse of LSB

[4] Nayan K. Dey, Suman K. Mitra, Ashish N. Jadhav, Hybrid Scheme for Robust Digital Image Watermarking Using Dirty Paper Trellis Codes.

[5] Lahouri Ghoti, Ahmed Bouridane, Mohammad K. Ibrahim, and Said Boussakta, Digital Image Watermarking Using Balanced Multiwavelets.

[6] Amir Houmansadr, Shahrokh Ghaemmaghami, A Digital Image Watermarking Scheme based on Visual Cryptography.

[7] Neil F. Johnson2, Zoran Duric1, and Sushil Jajodia2, recovery of Watermarks from Distorted Images.

[8] Henri Bruno Razafindradina and Attumani Mohamed Karim, Blind and Robust Images watermarking based on Wavelet and Edge Insertion.

[9] Prabhishek Singh, R S Chadha, A survey of Digital Watermarking Techniques, Applications and Attacks.

[10]Vinita Gupta, Mr. Atul Barve, A Review on Image Watermarking and its Techniques.