IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-2, Issue-6 E-ISSN: 2347-2693

DATA HIDING IN IMAGE BY OPTIMAL RANDOM SUBSTITUTION

Nisha[1*] and Kusu[2]

[1,2]CSE, MDU Rohtak, India,*
1781990kussum@gmail.com

www.ijcaonline.org

Received: 22/05/2014 Revised: 30/05/2014 Accepted: 20/06/2014 Published: 30/06/2014

***Abstract*—** The importance of reducing a chance of the Information being detected during the transmission is being an issue now days. Some solution to be discussed is how to pass information in a manner that the very existence of the message is unknown in order to repel attention of the potential attacker. Steganography comes from Greek and literally means 'Covered writing'. Steganography is closely related to hidden channel scheme. It is the art and science of writing of hidden message in such a way that no one apart of intended recipients knows the existence of message. Steganography is often confused with cryptography because the two are almost similar in the way that they both are used to protect confidential information. The difference between the two is in the appearance in the processed output; the output of steganography operation is not apparently visible but in cryptography the output is scrambled so that it can draw attention. Applications of both are in the field of communication system, Steganography coding inside transport layer such as an MP3 file and in the defence system.

Key Words: Steganography, Spatial Domain, Transform Domain: Steganography, Spatial Domain, Transform Domain

I. INTRODUCTION

Steganography is an art of hiding communication by embedding message into an innocuous-looking cover media. Using steganography, a secret message is embedded inside a piece of unsuspicious information and sent without anyone knowing the existence of the secret message. Secrets can be hidden inside all sorts of cover information: text, image, audio, video, and so on. Most steganographic utilities hide information inside images, as it is relatively easy to implement. People refers image steganography as the art and science of invisible communication, which is to conceal the very existence of hidden message in digital images. Some facts have motivated active researches and abundant publications in the field of image steganography. For example, images can convey a large of information especially on the internet. Moreover, the non stationarity of images makes image Steganography hard to break. Nowadays, digital image has become an important channel to bear Stego information.

Aiming at detecting secret information hidden in a given image using steganographic tool, steganalysis has been of interest since the end of 1990's. It is fair to say that steganalysis is both an art and a science. The art of steganalysis plays a major role in the selection of features or characteristics to test for hidden message, while the science helps in designing the tests themselves. As more and more techniques of hiding information are developed quickly, the wide-spread availability of tools for the same has led to an increased interest in steganalysis techniques. In the last few years, many new and powerful steganalysis techniques are reported in the literature [1]. Many of these techniques are specific to different embedding methods and indeed have shown to be quite effective in this regard. Research and development of steganography precedes steganalysis and steganalysis has been forced to catch up. More recently, steganalysis has had some success and steganographers have had to consider the stealthiness of their hiding methods more carefully.

Corresponding Author: *Nisha*

In this paper we have discussed about a little contributory work on the data hiding in image by choosing the random bits from the image and compared the result with the simple LSB substitution and Random LSB substitution.

II. PRINCIPLES OF STEGENOGRAPHY

There are mainly two types of Steganography types: 1) Spatial domain embedding 2) Transform domain embedding.

a) Spatial Domain Embedding

Spatial domain embedding technique is the first technique proposed in the literature [1]. Generally, these techniques operate on the principle of tuning the parameters of cover image (e.g., the payload or disturbance) so that difference between cover image and the stego-images little and imperceptible to the human eyes. Their popularity derived from their simple algorithmic nature and ease of mathematical analysis spatial domain embedding is easy to implement, providing high payload capacity but their robustness is weaker than their counterpart. The most widely known image based algorithm is based on modifying the least significant bit. The layers of image hence known as the LSB technique.LSB based methods can be divided into two main groups: LSB replacement and LSB matching. In LSB replacement, the LSB bit of cover image is replaced with secret bits. While in LSB matching, pixels are randomly incremented or decremented by secret bits.

b) Transform Domain Embedding

Transform domain embedding includes discrete Fourier transform (DFT), discrete cosine transforms (DCT), and discrete wavelet transforms (DWT). Regardless of the domain significant transform coefficients are often selected to mix with secret signal in a way such that information hiding transparent to human eyes. These transforms may be applied block wise, or over the entire image. For the block wise transform the image is broken into smaller blocks (8*8 and 16*16 are two popular sizes), and the transform

Steganography is performed individually on each block. DCT domain embedding technique is most popular one Mostly because of the fact that DCT based image format are widely available in public domain as well as the common output format of digital cameras. Embedding in DCT domain is simply done by altering the DCT coefficients.DWT domain based embedding technique is quite new and not as well developed or analyzed as technique which operate on DCT or DFT. But such technique will gain popularity a JPEG2000 compression becomes more popular. Stego Jasper embedding technique based on wavelet operates on JPEG2000 images. Embedding is done by modifying least significant bits of selected wavelet coefficients

III. FLOW CHART OF EXPERIMENT

Encoding:

Encoding as we all know is the technique of change the format or shape of data so that it cannot be understand. The flow chart of encryption of data in image is given below:

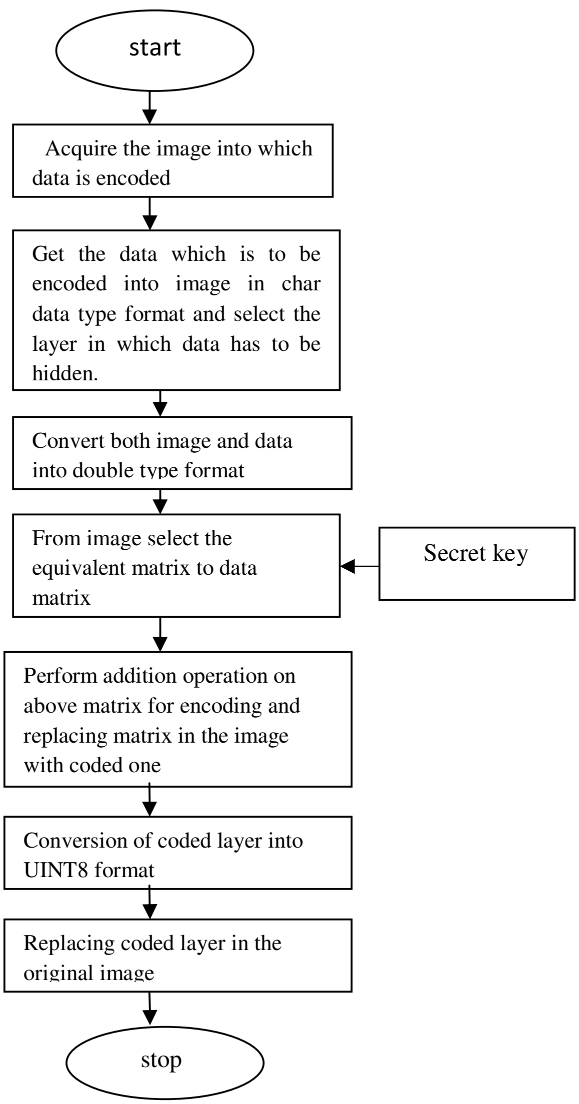

Fig 1: Flow chart of encoding

We use the secret key as a messenger that is used on the both sides (Encoding and Decoding) .secret key is known to only recipient, by using the secret key he/she can decode the data.

Decoding:

Decoding is done after encoding. In this experiment we have done decoding to get back the original data or message that we have hidden in the image.

To decode the data as given in the flow chart select layer in which the data is encoded and select the coded matrix and perform reverse operation as we perform in the case of encoding. After that one can get the original data.

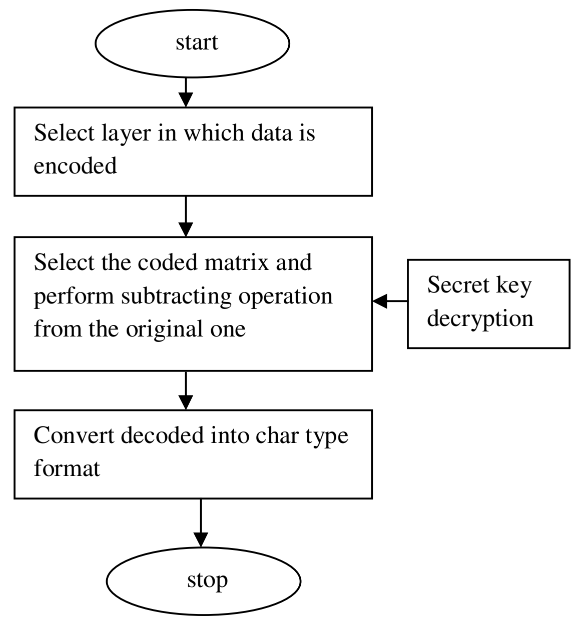

Fig 1: Flow chart of decoding

IV. EXPERIMENT RESULTS:

Fig 3: Original image

V. CONCLUSIONS

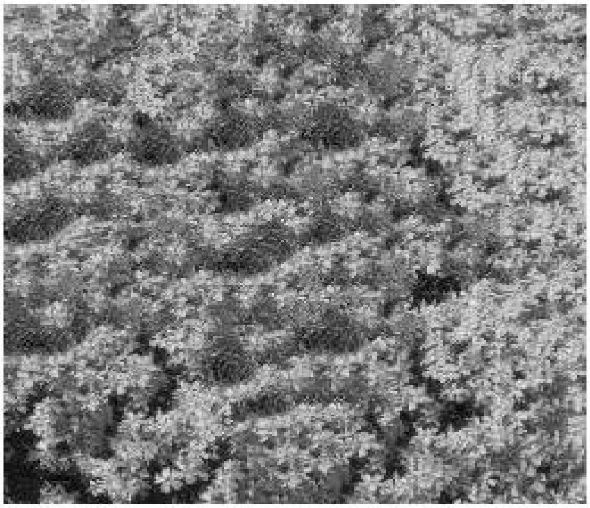

Fig 3: coded image

From the flow chart of encoding and decoding and the experimental results shows that there is no difference between the cover image and stego image.Further from the evaluation of the histogram, we conclude that all the result is same. Advantage of this method is that it is easy to implement and large data is hide into the image.Fig 3: coded image

Fig 4: Decoded original image

AKNOWLEDGEMENT

The authors acknowledge all the researchers for their contribution to make new advancements in Steganography technique by enhancing capacity and stability measures. Secondly special thanks to **Dheeraj** for their esteem guidance in this project and Computer Science And Engineering for providing excellent labs and all other resources for the completion of this work.

REFERENCES

[1]. YambemJinaChanu, Themrichon Tuithung, Kh. Manglem Singh "short survey on image steganography and steganalysis techniques" ,978-1-4577-0748-3/ 2012 IEEE.

[2]. GeHuayong , Huang Mingsheng, Wang Qian, "Steganography and steganalysis based on digital images "978-1-4244-9306-7 2011IEEE conference on image and signal processing.

[3]. Vijay Kumar,Dinesh Kumar, "Performance evaluation of DWT based image steganography" 223-228 ,2010 IEEE 2nd international advance computing conference .

[4]. R.Amrittharajan,Sandeepkumarbehera,AbhilashSwarup, "Colour guided colour image steganography " universal journal of computer science and engineering technology 16-23,oct. 2010

[5]. Prabakran.G, Bhavani.R " A modified secure digital image steganography based on discrete wavelet transform", 1096-1100, 2012 IEEE

[6]. Chi-Kwong Chan□, L.M. Cheng "Hiding data in image by simple LSb substitution", the journal of the pattern recognition society, pattern recognition 37(2004) 469-474

[7]. R.Amritharajan,r.akila,P.Deepikachowdavarapu,"A comparative analysis of image Steganography" international journal of computal applications (0975-8887) ,volume 2-No.3,May-2010.

[8]. W.Bender,D.Garhul,N.Morimoto,A.Lu," Techniques for data hiding" IBM System journal VOL.35,NOS 3&4,199

[9]. Hide and seek: An introduction to steganography, 1540-7993,2003 IEEE security and privacy

[10]. SANS institute infosec reading room :steganography : past, present ,future

[11]. MiroslavDobsicek :Modern Steagnography