INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN: 2278 – 0211 (Online)

Tamper Detection Using Enhanced Random LSB Techniques

V.Baby Vennila
Associate Professor,Department of IT,
Vivekanandha college of Engineering for Women, Tamilnadu,India

N.P.Ilakkia
Department of IT,
Vivekanandha college of Engineering for Women, Tamilnadu,India

Abstract:

The Tamper detection of images places an important role in the production of visual content, which is handled during transmission of the visual content. In each image there is an lsb bit in each pixel, which is independent of the appearance or visual content of the image. So hiding the data in the image is applicable using enhanced Random LSB. In the existing technology, watermarking technique is used to send and receive the data . The goal of blind image forensics is to determine the authenticity of an image without using an embedded security scheme. With the broad availability of digital images and tools for image editing, it becomes increasingly important to detect malicious manipulations. Consequently, image forensics has recently gained considerable attention.

Key words: *Random LSB, Tamper Detection, Image Forensics*

1.Introduction

Image processing is any form of signal processing which takes the image such as photographs or frames of video as input and the output of image processing can be either an image or a set of characteristics related to the image. Now, an image is an array of numbers that represent light intensities at various points (pixels). These pixels make up the image transfer faster than data. In computer vision, image processing can be done using digital images. A digital image is composed of pixels which can be thought of as small dots on the screen. A digital image is an education of how to color each pixel. Each image can be divided into number of pixels. Above are some information about the pixels in images.

Image steganography, the stealthy embedding of information into digital pictures, stands for a means protection of responsive information and the congregation of aptitude. Steganalysis, the recognition of this concealed information, is an essentially tricky problem and needs a more meticulous examination. On the contrary, the hider must cautiously examine a means to security sneakiness. A rigorous framework for examination is required, both from the point of view of the steganalyst and the steganographic.

The method of hiding secret message over a media, such as image, text is frequently named as steganography. This is because the word “Steganography” comes from the Greek word meaning “covered writing”. An image steganographic scheme is one variety of steganographic systems, where the furtive (secret) message is hidden in a digital image with some hiding system. The intented person can then use a correct implanting process to get better the unknown message from the image. The original image is called a cover image in steganography, and the message embedded image is called a stego image.

Steganography conveys science to the art of hiding information. The reason of steganography is to bring communication via a conduit of misunderstanding such that the existence of the message is both hidden and difficult to extract efficiently when discovered. Basically the information hiding process in a Steganoraphic system starts by identifying a cover medium’s redundant bits. The embedding process creates a stego medium by replacing these redundant bits with data from the hidden message. The basic principle is to make the communication incoherent to individuals who do not possess the right keys. The first step in steganography is to pass both the secret message and the

cover message into the encoder. Inside the encoder, one or several measures will be implemented to embed the secret information into the cover message.

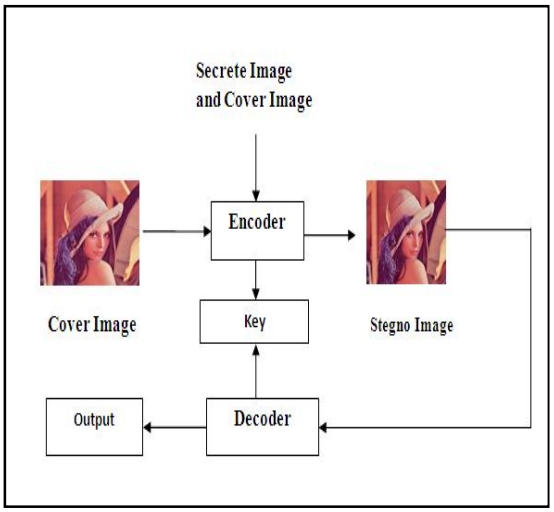

Figure 1: Architecture of Random LSB

As long as people have been able to communicate with one another, there has been a desire to do so secretly. Two general approaches to covert exchanges of information have been made: one is communicated in a way comprehensible by the proposed method is more secure, another one is placing the key before transmission so there is no disadvantage in our system. Obviously both of this technique can be used in parallel to improve space to you. Both of this technique can be used together in tandem to improve privacy. The ceremonial lessons of these process, cryptography and steganography, encompasses the change and its more complicated during development. Methods for hiding information into cover or host media, such as audio, images, and video, were developed. Steganography normally is subjected to a smaller amount cruel attack, on the other hand much statistics has is to be inserted.

A work of steganalyst may be a company examining retiring emails to stop the leaking of proprietary information, or an aptitude gatherer hopeful to identify announcement between challengers. The original cover is not reachable, the figure of steganography apparatus is big, and each device might boast numerous acceptable restrictions. Typically a perception on the individuality of cover images is used to establish a conclusion marker that arrest the effect of data hiding and allow discrimination between ordinary images and those surround hidden data. We have consequently seen an iterative process of

steganography and steganalysis: a steganographic method is detected by a steganalysis instrument; a new steganographic method is invented to foil detection, which again turns vulnerable to an enhanced steganalysis. In this paper we discuss about Random Lsb and Tamper Avoidance in detail.

2.Related Work

With the development of digital signal processing (DSP), information theory and coding theory, steganography has went into ‘‘digital’’. In the empire of this digital world, steganography has created an atmosphere of corporate caution that has spawned various interesting applications, thus its continuing evolution is guaranteed. Cyber-crime is believed to benefit from this digital revolution. Hence an immediate concern is to find out best possible attacks to carry out steganalysis, and simultaneously, finding out techniques to strengthen existing steganographic techniques against popular attacks like steganalysis. The innocent files can be referred to as cover text, cover image, as appropriate. After embedding the secret message it is referred to as stego-medium. A stego-key is used to control the hiding process so as to restrict detection and/or recovery of the embedded data.

One of the most popular and commonly used steganographic algorithms for information hiding in digital images is the LSB insertion method. It is a simple algorithm that swaps the least significant bit in some bytes of the cover medium with a sequence of bytes containing the secret data to hide. However, though the LSB algorithm hides data in the cover medium (image), its imperceptibility to statistical steganalysis is relatively low. This is mainly because the significant bits of the secret message are hidden in the cover medium in a linear and deterministic pattern. The secret message is normally embedded in a cover medium known as a stego file in a way that totally conceals the existence of any form of communication going on.

The main terminologies used in that paper Steganographic systems are: the cover message, and secret key and embedding algorithm. The cover message is the carrier of the message such as image, video, audio, text, or some other digital media. The secret message is the information which is needed to be hidden in the suitable digital media. The secret key is usually used to embed the message depending on the hiding algorithms. The embedding algorithm is the way or the idea that usually use to embed the secret information in the cover message.

In determining the fixed-point representation of a floating point data path, we must consider both the most-significant and least-significant ends. Reducing the relative bit position of the most-significant bit reduces the maximum value that the data path may represent, sometimes referred to as the dynamic range. On the other end, increasing the relative bit position of the least-significant bit (toward the most-significant end) reduces the maximum precision that the data path may attain. A fixed-point data path means that results or operations may exhibit some quantity of error compared to their floating-point counterparts. This quantization error can be introduced in both the most-significant and least-significant sides of the data path.

The "Encryption phase" uses two types of files for encryption purpose. One is the secret file which is to be transmitted securely, and the other is a carrier file such as image. In the encryption phase the data is embedded into the image using "Least Significant Bit algorithm" (LSB) by which the least significant bits of the secret document are arranged with the bits of carrier file such as image, Such that the message bits will merge with the bits of carrier file. In this procedure LSB algorithm helps for securing the originality of image. The image in which data is hidden i.e. the carrier file is sent to the receiver using a transmission medium. The receiver receives the carrier file and places the image in the decryption phase. In the decryption phase, the original text document or audio or video file can be revealed using the appropriate password.

3.Problem Definition

The aim of the project is to hide the data and secret image over a cover image using Enhanced Random least significant. Steganography algorithm is used to send the stego file to the destination where the recovering of the secret data and image is done and to detect the tampering in case any tamper is made in receiver side.

4.Problem Solution

The proposed technique should provide better security while transferring the data and image messages from one end to the other end. The main objective of our paper is to hide the message or a secret data into an image which acts as a Cover file having secret data and to transmit the stego to the destination strongly without any modification. If any distortions occur in the image or on its resolution while inserting the secret message into the image, or if there is a chance for an unauthorized person to modify the data, this is called as tampering and occurrence of tampering is detected here. So, the data and image

encryption into a cover image with key and decryption and steganographic plays an important role in this project.

5.Major Performance Objectives

The main objective of the project is to argue the possessions which help to transmit the secret message or information over a network without any modifications. The individuality of information is:

- Ease of use.
- Accurateness.
- Faithfulness.
- Privacy.
- Truthfulness.

6.Proposed Approach

6.1.Random LSB

In Random lsb technique a random number is generated by using Pseudo Random Generator and hides bits of secret image and secret text into the Random least significant bits (RLSBs) of the pixels within a carrier image, called the cover image. The accepted approach to achieve this, is the random period technique. Both message parties contribute to a stego-key, k practical as a beginning for a random number generator. The production is a random sequence o,…, o n where n is the length of message bits. This sequence is then used by the sender to generate a sequence of pixel indices, x_i where

$X_i = o_i$

- $Xi=oi-1+oi,$ I >=2 …..…….. (1)

Message bit, i is embedded in the Lsb of Pixel thus, the order in which the secret message bits are embedded would be determined pseudo-randomly. Since the receiver knows the key k, he/she can reconstruct k_i and therefore the entire sequence of pixel indices, y_i.A similar method was proposed where a pseudo-random permutation depending on a stego-key split into three pieces k1, k2, k3, was applied to randomly spread the message bits over the LSBs of the cover image. Other steganographic methods that employ the random LSB insertion have been presented and Random LSB

insertions are intended to make it harder for an attacker to detect the embedded secret message with attacks such as the visual attacks and statistical attacks.

6.2.Sender Side

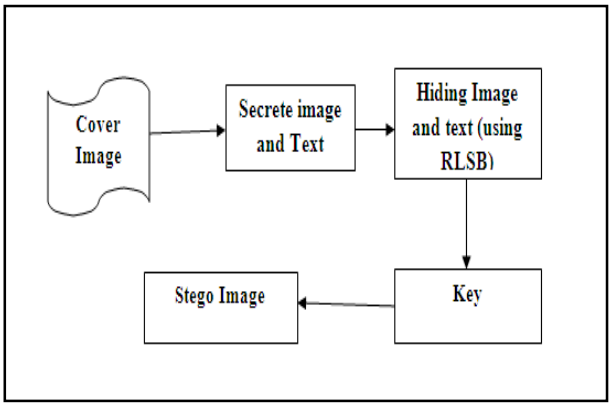

Figure 2: Insertion of text and Image Using R-Lsb in Sender Side

In Sender Side the Cover Image is Choosed and for hiding the secret image and text is placed to hide the image and text in the cover image using Random Lsb. if there is change in any of Lsb bit tamper detection is made or else no modification in secret text and secret image . Let us consider the cover image (c_s) And Secret image (I_s) and text (t_s).the hiding is made using Enhanced Random Lsb algorithm. The random number is generated using random number generator (a_{is}).finally a key is used for hiding those cover and secret image, text. Let the sender side equation is

- $S = c_s + (I\ s\ (a_{1s}) + t\ (a_{2s}) + k_s$ ..... (2)

6.3.Receiver Side

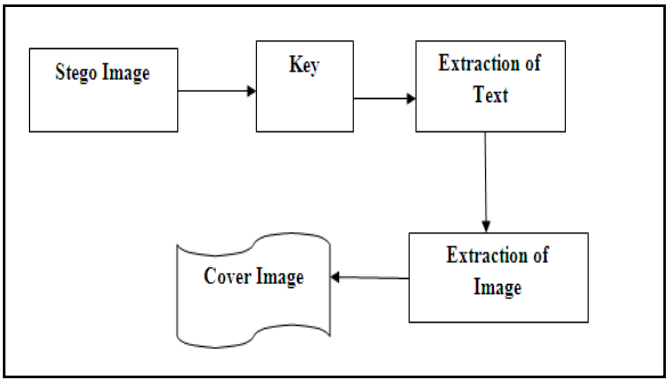

Figure 3: Extraction of text and Image Using R-Lsb in Receiver Side

In Receiver Side the Stegno Image is Choosed to Retrieve the secret image and text ,after placing the correct key. If key is correct the image is Retrieved from the cover image else nothing is get retrieved from cover image. Let us consider the cover image (c_r) And Secret image (I_r) and text (t_r).the hiding is made using Random Lsb algorithm. The random number is generated using random number generator (a_{ir}).finally key is used for Extracting those cover and secret image, text. Let the receiver side equation is

$$\mathbf{r = s_r + (I_r\,(a_{1r}) + t\,(a_{2r}) + k_r} \quad \ldots\ldots\ldots (3)$$

7.Random Least Significant Bit Algorithm (R-LSB)

- Step 1: Choose the stego Image (color)

  Choose the Steganography image.
- Step 2: Select the Extract Image (color)

  To extract the secret Image
- Step 3: Text for Extraction.

  To place the output Text
- Step 4: The Text must be extract outside of the Cover Image.
- Step 5: Output Image (qs)

  Cover Image is now found in receiver side

  Go to Exit
- Step 6: Above steps are possible only if key values correct
- Step 7: If any modification is made

  Tamper is detected

  Else
- Step 8: Tamper is not detected

  Exit
- Step 9: Information is kept Secured Using Key.

8.Result And Discussion

The hiding and extraction of image is made with high reliability without any distortion of data with the help of Random Least Significant Bit. The tampering detection of image also is quite achieved.

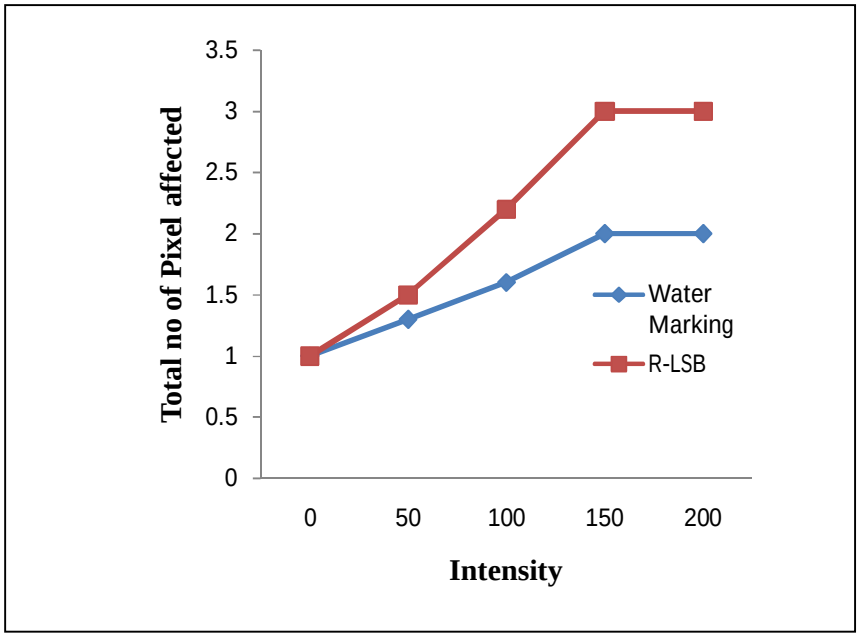

Figure 4: Intensity of R-LSB

The non-uniform approach obtains better results considering a number of bits greater than 4 .It is worth nothing that the non-uniform quantization describes a single block making use of one bits instead of 12 bits used by uniform quantization.

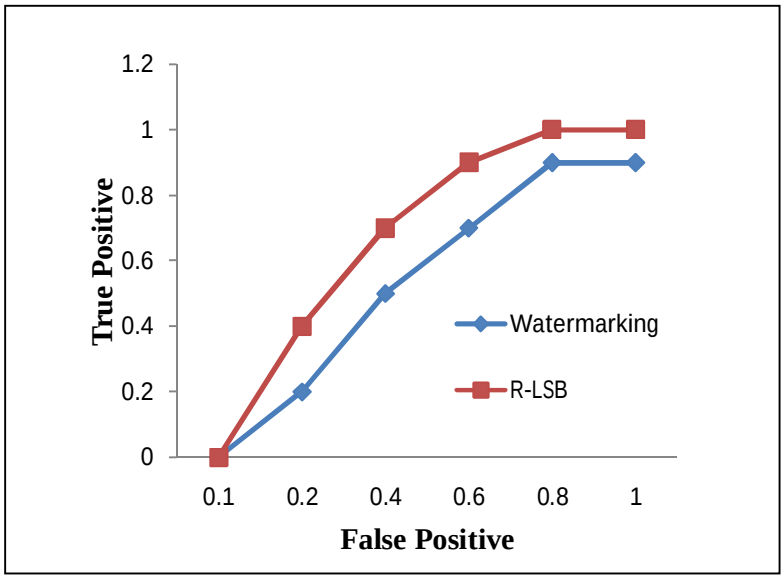

Figure 5: Tampering detection comparison through R-LSB.

9.Conclusion

A method of information hiding using steganography, mainly edge detection filter has been offered, which is a way for classification of dissimilar colour to spot dark area of

image. The hiding of the text and secret image in selected dark places but the information is not put honestly in those pixels and put in low bits of every eight bit pixel. It makes use of the Three advantageous approaches, one is Random Least significant bit insertion , second is Grey level approach with edge detection, third is Randomization. The RLSB insertion was worn to implant the message in to the cover image. The variety of pixel to drive in was critical, ever since the RLSB insertion modifies the pixels. Customized pixels in areas of the image where there are pixels that are most similar to their neighbors were a large amount further noticeable to the normal eye. To work out this, difficulty edge pixel were indiscriminately preferred to embed the message. The benefit of RLSB is its simplicity to implant the bits of the message honestly into the RLSB plane of cover image. Also its perceptual simplicity makes the change to the cover-image cannot be traced by human eye. On the contrary, the RLSB is very responsive to any variety of filtering or handling of the stego-image. Using the advance edge detection along with random least significant bit method directs to high security. Even with a little thing as an image, the surrounded image is just like the creative one.

10.Reference

1. Chi-Kong Chan, L.M. Cheng, "Hiding data in images by simple LSB substitution" Department of Computer Engineering and Information Technology, City University of Hong Kong, Hong Kong, August 2003.
2. Rita Rana1 & Er.Dheerendra Singh "Steganographic-Concealing Messages in Images Using LSB Replacement Technique with Pre-Determined Random Pixel and Segmentation of Image", Vol. 2, No. 4, August, 2010 1793-8201.
3. Shreelekshmi R, M Wilscy and D. Ker," A Weighted Stego Image Detector for Sequential LSB Replacement", Third International Symposium on Information Assurance and Security.
4. Nitin Jain, Sachin Meshram, Shikha Dubey,"Image Steganographic Using LSB and Edge – Detection Technique ", International Journal of Soft Computing and Engineering (IJSCE).
5. Juan José Roque, Jesús María Minguet," SLSB: Improving the Steganographic Algorithm LSB".
6. Pin Zhang," Detecting Image Tampering Using Feature Fusion", 2009 International Conference on Availability, Reliability and Security.
7. Ferdinando Di Martino Salvatore Sessa," Fuzzy Transforms and Fragile Watermarking Tamper Detection on Coded Images", July 2011.
8. Pierre-Alain Fouque, David Pointcheval ," Hardness of Distinguishing the MSB or LSB of Secret Keys in Diffie-Hellman Schemes".
9. M.Sivaram ," STEGANOGRAPHY OF TWO LSB BITS", International Journal of Communications and Engineering.
10. Kwangsoo Lee1, Andreas Westfeld2, and Sangjin Lee1," Category Attack for LSB Steganalysis of JPEG Images".
11. Jessica Fridrich," Reliable Detection of LSB Steganography in Color and Grayscale Images".
12. Tao Zhang, Xijian Ping," Reliable detection of lsb steganographic based on the difference image histogram", ICASSP 2003.
13. Jessica Fridrich and Miroslav Goljan , "On Estimation of Secret Message Length in LSB Steganographic in Spatial Domain".
14. C. T. Li, Digital fragile watermarking scheme for authentication of JPEG images, IEEE Proceedings on Vision Image and Signal Processing, IEEE Press 151 (6), pages 460–466, 1994.

15. C. T. Li and Y. Yuan, Digital watermarking scheme exploiting nondeterministic dependence for image authentication, Optical Engineering, 45 (12) : 127001–6, 2006