Research Paper

Volume : 3 | Issue : 4 | April 2014 • ISSN No 2277 - 8179

Suitability of LSB Substitution based Steganography for Digital Images: A Study

Engineering

KEYWORDS : LSB Substitution, Cryptography, Steganography

Dr. Aruna Kumar Mishra — Assistant Professor, IMS Unison University, Dehradun, India.

Er. Purabee Purnasha Mishra — Assistant Professor, IMS Unison University, Dehradun, India.

ABSTRACT

Advancement in processing speed of computers and the penetration of broad band gave rise to different sophisticated techniques of cryptography. Presently as the analog images are almost obsolete there is a need for fresh look into the digital image steganography as a way of embedding data. It has wide applications in present Internet age such as secure transmission of confidential data, maintain copyright etc. But the major question is that which technique to be used without changing the quality of the images or least affecting the quality of images.

This paper focuses on the suitability of Least Significant Bit(LSB) Substitution method as a technique of Steganography.

In this study the Digital Images with date emebeded in it and the digital images without data are shown to the respondents to find out if there is any change in the quality of the images and whether the respondents can differentiate the images.

Introduction:

Increased use of computer technology has caused an increase in computer related crimes and forced the companies to recognize the importance of data security. The major issues are the misuse of computer technology by employees, to the theft of confidential data by computer hackers and also the data retrieval from both internal and external storages. So there is increased trend in sophisticated attacks. Sophisticated compression and encryption techniques are needed by Government and various organizations to reduce the growing demand of data security without any perceptible reduction in quality of the multimedia data. Very rapid growth of digital multimedia data has opened up the possibility of hiding important information inside multimedia files without any degradation in quality and also without affecting the application of those files. Steganography or cryptography in digital images is a way of communication between two users without a visible communication channel. So there is a urgent need to further study the various techniques and there suitability in digital image cryptography as it provides an important way of securely transmitting data at a very cost effective way to any part of the world and has wide applications in various fields.

Literature Review:

In LSB substitution method of encoding the last bit of the image byte is encoded that contains the data to be hidden. Digital image consists of a matrix of color and the intensity values. Gray scale image is of 8 bits/pixel and full color image is 24 bits/pixel . In LSB Substitution method bits of the message are directly put into the least significant bit plane of the cover image .It is very simple method and has high perceptual transparency. This method has the limitation of low in robustness, low tamper resistance, sensitive to cropping, rotation, filtering, etc. But the method has the ability to embed data in image, audio and text covers.

De Vleeschouwer et. al.(2003) proposed a method for lossless data hiding technique against high quality JPEG compression. This technique can be used for the purpose of semi-fragile authentication. The technique can be used if the image does not change at all or even if the image undergoes some compression, the hidden data can be extracted and the authentication can be checked. Semi-fragile authentication is more practical compared to fragile authentication as it allows some modification such as compression. The basis of their algorithm comes from the patchwork theory. As per this theory, each bit of the message is associated with a group of pixels, e.g., a block in an image.

Yuan et.al. (2006) proposed an integer wavelet based multiple logo-watermarking scheme for copyright protection of digital image. A visual meaningful binary logo is used as watermark. The process of watermark embedding is carried out by transforming the host image in the integer wavelet domain. To construct a blind watermarking scheme, wavelet coefficients of HH and LL bands are modified depending on the watermark bits. To add the security, permutation is used to preprocess the watermark. From the experimental results it was observed that the proposed method was robust to a wide variety of attacks. Comparison with the existing methods showed the superiority of the proposed method.

Xiao and Wang (2008) proposed a semi-fragile image watermarking scheme based on the theory of Laplacian sharpening which can tolerate Laplacian sharpening but fragile to neighborhood averaging and median filter.

Zhao and Sun (2008) used HVS masking characteristics to develop a semi-fragile watermarking scheme, which can accept mild JPEG compression but is susceptible to filtering, noise addition.

Woo et.al.(2009) proposed scheme embeds a downscaled version of an image into the image's discrete wavelet transform sub bands. The scheme provides content authentication by allowing high quality JPEG compression, minor local distortion, and minimal noise insertion. Other changes such as histogram equalization, cropping, rotation, and mean filtering are classified as malicious attacks because it affects the visual quality of the image. The scheme does not require a reference image during content authentication. Tampered regions can be located correctly, and its original content can be recovered. The approximately recovered content could give the user an idea of the original image appearance. The watermark information is secured by a secret key that randomizes the watermark pixel positions. The single transform, correlator detector, and down-scaled processing spaces of the scheme offer low computational costs.

Yang et.al. (2010) proposed a novel semi-fragile watermarking scheme in image spatial domain. The scheme embedded the duplicated watermark bits into sub-blocks of the host image by adaptive LSB substitution and had low computation cost. Due to the usage of the HVS masking mode during adaptive LSB substitution, the watermark is adaptive to the original image feature, which ensures high visual quality of watermarked image. An effective classification rule for image authentication was developed, which could differentiate effectively malicious attacks from incidental attacks. Experiment results showed that the proposed scheme had good robustness to incidental attacks, while it was very fragile to malicious attacks. Moreover, this algorithm can localize maliciously tampered regions accurately (marked by white pixels).

Research Methodology:

The primary objective of this study is:

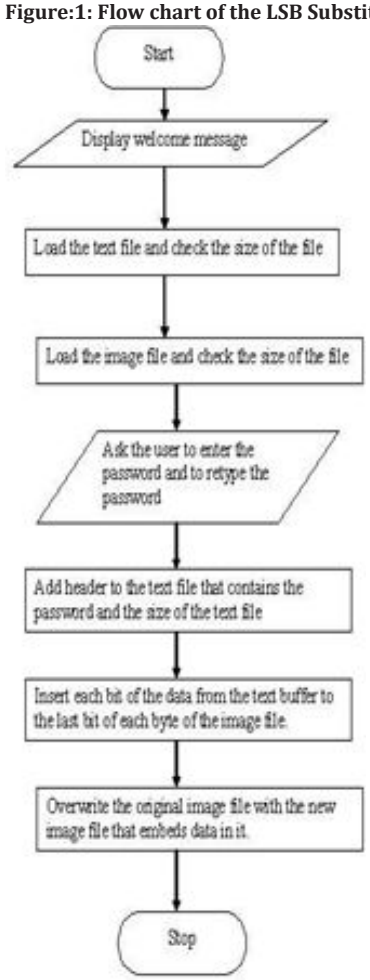
To test the suitability of LSB Substitution method in digital image Steganography.

The secondary objectives of the present study are

- To develop a code for secure LSB Substitution and retrieval of data from digital images
- To test the images by the respondents to find if any perceptual difference in the images

In this study LSB Substitution technique is used to hide data into the image files. Data is embedded in such a way that it is perceptually and statistically undetectable. This technique is truly secure as it is impossible to extract the data from the image without the key. The technique that is used in the code can be called Least Significant Bit (LSB) substitution technique. The program is developed in VC++ 6.0 IDE which works well for bitmap image files. At the end experimental data analysis is done to find the quality of image files after data hiding in them. For other formats such as JPEG which is extensively used the program need to be modified and further research is required to be conducted.

Figure:1: Flow chart of the LSB Substitution Code:



Experimental result:

To determine the quality of the data embedded images, the author performed a series of blind visual tests. For each test image, two randomly selected images "A" and "B" were repeatedly displayed side by side to a viewer. The ordered pair (A,B) was randomly selected as (original, data embedded) or (data embedded ,original).The viewer was asked to select image "A" or "B" that was visually more pleasing. This test was performed 10(Ten) times for each image. There was no time limit that the viewer could spend on each set of images. A total of 12 viewers took part in the blind test. As a result, the watermark for each test image was visually tested 12X10=120 times.

The results of the test are shown in the following table:

Table: 1: Test results

Test Image	Total no. of tests	No. of times the original image without data selected	Preferred original to data embedded (%)
Picture 1	120	65	54.16
Picture 2	120	57	47.50
Picture 3	120	66	55
Picture 4	120	64	53.33
Picture 5	120	65	54.16
Picture 6	120	62	51.66
Picture 7	120	55	45.83
Picture 8	120	61	50.83

In the above table fourth column shows the average result for each picture.

As we can see from the table, the original images and the data embedded images were preferred almost equally well by the viewers within the sampling error. The experimental result confirms the validation of the LSB substitution technique of data hiding.

So it can be concluded from the data of the table that the hidden data is visually undetectable and causes no degradation to the original image or the host image.

Conclusion and scope for future work:

This study analyses the Least Significant Bit substitution technique of data hiding in detail. From the experimental result that was obtained it can be concluded that the technique is an effective way of data hiding in images without degrading the quality of images significantly. The proposed technique also provides for authentication of the receiver as it also stores the password along with the data. The code for demonstrating the LSB substitution technique was developed in VC++ 6.0 IDE. The major limitation of the code is that it can be applied only for BMP files. The code or the program can be further extended to hide data in other formats such as JPEG which is more extensively used in communication through Internet. This study analyses and demonstrates data hiding only in the image files where as data can be hidden in audio and video files also without degrading the quality of the host signal. There is a need to develop techniques which will retain data even after compressing the image for transmission. The data cannot be retrieved by the presently proposed technique if the image file goes through lossy compression after hiding the data in it. Though the LSB substitution technique works perfectly well for lossless compression further research can be carried out to find new techniques to hide data in the other multimedia files. Encryption techniques such as DES and PGP can be combined with the LSB substitution technique for better data security than the proposed LSB substitution technique. For many applications, it is desirable to get a data hiding scheme that is robust to most intentional and non-intentional attacks which can be further studied.

REFERENCE

1. C. De Vleeschouwer, J. F. Delaigle and B. Macq, 2003. Circular interpretation of bijective transformations in lossless watermarking for media asset management, IEEE Tran. Multimedia, vol. 5, pp. 97-105. | 2. Woo, C.S., D. Jiang and P. Binh, 2009. Semi fragile watermark with self authentication and self recovery. Malaysian J. Comput. Sci., vol.2, pp: 64-84. | 3. Xiao, J. and Y. Wang, 2008. A semi-fragile watermarking tolerant of Laplacian sharpening. Proceedings of the International Conference on Computer Science and Software Engineering, Wuhan, China, (ICCSSE'08), IEEE Computer Society, pp: 579-582. | 4. Yang H., Sun X. and Sun G., 2010. A Semi-Fragile Watermarking Algorithm using Adaptive Least Significant Bit Substitution. Information Technology Journal, vol.9, pp:20-26. | 5. Yuan Y., Huang D. and Liu D,2006. An Integer Wavelet Based Multiple Logo-watermarking Scheme. First International Multi-Symposiums on Computer and Computational Sciences (IMSCCS'06), vol.2,pp. 175-179. | 6. Zhao, Y. and X.H. Sun, 2008. A semi-fragile watermarking algorithm based on HVS model and DWT. Proceedings of the International Conference on Computer Science and Software Engineering, Wuhan, China, (ICCSSE'08), IEEE Computer Society, pp: 638-641. |