International Journal of Scientific Engineering and Research (IJSER)
www.ijser.in
ISSN (Online): 2347-3878
Volume 1 Issue 2, October 2013

Data Hiding Technique Depended on Pseudorandom Sequences

Z.Wai[1], S. Than[2]

[1]University of Computer Studies, Mandalay, Myanmar

[2]Computer University, Myitkyina, Myanmar

Abstract: ***Due to increasing the technologies, security is very important in many areas. Steganography and Cryptography are two popular ways of sending vital information in a secret way. In this proposed system, an image steganographic technique is presented by combining cryptographic and steganographic techniques. In this proposed scheme, secret messages are encrypted before embedding it into the cover image which gets high security to secret data. RC4 algorithm is used to encrypt secret messages and LSB based data embedding technique is used to hide encrypted messages. To hide encrypted messages into BMP image file, pseudorandom sequences are used. These sequences are generated by BBS (Blum Blum Shub) Pseudorandom Number Generator. In this method, message may be embedded to 1-LSB of container image if random sequence generates "1" as PRNS. In contrast, the message can be embedded to 2-LSB of container image. If an attacker wants to get the original messages, he must know secret key and random sequences. This proposed system intends for data confidentiality and data integrity. This proposed model gives two tier securities to secret data. This can be used for many applications in computer science and other related fields.***

Keywords: BBS, random sequences, RC4, security, steganography

1. Introduction

Nowadays, Internet becomes essential and fastest media for communication. In data communication, it is susceptible to face many problems such copyright protection, hacking, eavesdropping etc. Hence the requirement of the secure communications is needed. Cryptography and Steganography are the two fields available for data security [1]. Steganography is often combined with cryptography to provide an additional layer of security. Using cryptography, data is encrypted and then transmitted. On the other hand, steganography hides the messages in an image file and then the image is transmitted. It is possible to combine the techniques by encrypting message using cryptographic technique and then hiding the encrypted message using steganographic technique [2]. This paper proposes the security system by combining these two techniques. The resulting stego-image can be transmitted without revealing that secret information is being exchanged. Furthermore, even if an attacker detects the message from the container image, he would still require the cryptographic decoding key to recover the original message [3].

In these methods, stream cipher RC4 algorithm is used for data confidentiality and message authentication. In RC4 algorithm, encryption is about 10 times faster than DES and a particular RC4 key can be used only once. After enciphering the plaintext (original message), these encrypted messages are embedded in BMP image file by using LSB steganographic technique. Least Significant Bits (LSB) insertion is a simple approach to embed secret information in image file. Altering the LSB will only cause minor changes in color, and thus is not usually noticeable to the human eye. This system improves the security of the data by embedding the encrypted text (ciphertext) and not the plaintext in an image.

This paper is organized as follows. Section 2 contains the related works. In section 3, overview of LSB steganographic technique is discussed in this paper. Section 4 describes the steganographic method in BMP image file. Overview system of this paper is described in section 5. Implementation and evaluation result is illustrated in section 6. Finally, conclusion is described in section 7.

2. Related Works

Nowadays security has become one of the most significant problems for information technology. Many users want their information to be secure. Cryptography and steganography can solve this issue. Encryption and steganography are the preferred techniques for protecting the transmitted data. In [4], Mamta Juneja et al. presented a technique that combined steganography and encryption technique. The goal of this application was to help users to maintain their data's confidentiality. They described steganography tools based on LSB algorithms. In [5], Neha Sharma et al. proposed a system that combines the effect of two methods such as cryptography and steganography to enhance the security of data. The authors also used MD5 hashing algorithm to provide the integrity of message contents. They can't evaluate their system by steganographic tools. In [6], Yoendra Kumar Jai and R.R.Ahirwal presented a novel image steganography method. This method used LSB method and private stego-key. In this paper, they embedded binary bit stream in 24 bits color image or in 8 bits gray scale image. According to their results, their proposed system is better than the existing methods and better security. Experimental results verify that the proposed model

is effective and efficient. In [7], the authors explained LSB embedding technique and presented the evaluation for various file formats. They don't analyze their techniques with other steganographic techniques.

3. LSB Steganographic Technique

This technique is to embed the bits of the message directly into the least significant bit plane of the cover image in a deterministic sequence. Modulating the least significant bit does not result in a human perceptible difference because the amplitude of the change is small. The implementation of LSB method is quite easy and it is a popular method. To hide a secret message inside an image, a proper cover image is needed. Because this method uses bits of each pixel in the image, it is necessary to use a lossless compression format, otherwise the hidden information will get lost in the transformations of a lossy compression algorithm. Digital image steganography is accomplished by using a common principle called least significant bit insertion. Each pixel contains a number of bytes that describe the color and appearance of the pixel. Depending on the resolution of that image, there are a set number of bytes for each pixel. When the LSB are removed from an image, it can be viewed as a gradient of redundant bits that resembles a black and white star burst. These bits are not really necessary for the integrity of the photography so these are the bits that are manipulated [8].

There are many insertion techniques in LSB. They are 1-bit insertion, 2-bit insertion, 3-bit insertion and 4-bit insertion [9]. This LSB method involves utilizing a single least significant bit of one of the RGB bytes of a 24-bit image for message concealment. As the color value is not changed much, it will not considerably alter the visual appearance of color and image [9].

In this system, a BMP image file is used as a carrier to hide message. Least Significant Bit (LSB) insertion [10] is a simple approach for embedding information in image file. LSB technique is the most popular steganographic technique employed with graphics image files.

3.1 Pros and Cons of LSB Insertion

The advantages of LSB embedding are its simplicity and many techniques use these methods. It is easy to understand and comprehend to employ. LSB embedding is also allowed the high perceptual transparency. It gives the low degradation in the image quality and growingly commercial software is available which follow this approach.

However, there are many weaknesses when robustness, tamper resistance, and other security issues are considered. LSB doesn't change the quality of image to human perception but this scheme is sensitive a variety of image processing attacks like compression, cropping etc [7]. Furthermore, an attacker can easily remove the message by removing (zeroing) the entire LSB plane with very little change in the perceptual quality of the modified stego-image [10].

4. LSB Data Hiding in BMP

Images are the most popular cover media for steganography and can be stored in a straight-forward bitmap format (such as BMP) or in a compressed format (such as JPEG). There are many applications for digital steganography of images, including copyright protection, feature tagging, and secret communications.

In this system, BMP image file is used as a container file. So if we were to modify the least significant bit (LSB) for every byte specifying color intensity, a human won't see the difference when the modified image is displayed. This is a very good opportunity for hiding information in the bitmap image. This is an advantage for hiding data without raising suspicion.

The BMP file format is an image file format used to store bitmap digital images. In uncompressed bmp files and many other bitmap file formats, image pixels are stored with a color depth of 1,4,8,16,24 or 32 bits per pixel. An alpha channel for transparency may be stored in a separate file or in fourth channel that converts 24 bit images to 32 bits per pixel. Uncompressed bitmap files such as BMP files are typically much larger than compressed image file formats for the same image. For example an image of 1058 * 1058 pixels in png format occupies about 287.65 KB while in 24 bit BMP file it occupies about 3358KB [11].

A bitmap file has two main parts, the header and the data. The header, consists of 54 bytes, has two sub blocks: Bitmap Header, and Bitmap Information. Bitmap Header, 14 byte, is used to identify the file as a valid bitmap image and Bitmap Information is composed of the next forty bytes of the file.

5. Proposed System Design

By combining cryptography and steganography, this system can provide main security requirements, data confidentiality, Integrity and message Authentication (CIA). There are many encryption algorithms but RC4 encryption algorithm is used in this system for data confidentiality. After enciphering the original message, these encrypted messages are embedded in BMP image file by using LSB method. Altering the LSB will only cause minor changes in color, and thus is usually not noticeable to the human eye. The embedding process is based on pseudorandom number generator. Blum Blum Shub (BBS) generator is used in this system to generate the random sequences. According to these random sequences, encrypted messages are embedded in BMP image file. In this method, message may be embedded to 1-LSB of container image if random sequence generates "1" as PRNS. In contrast, the message can be embedded to 2-LSB of container image.

International Journal of Scientific Engineering and Research (IJSER)
www.ijser.in
ISSN (Online): 2347-3878
Volume 1 Issue 2, October 2013

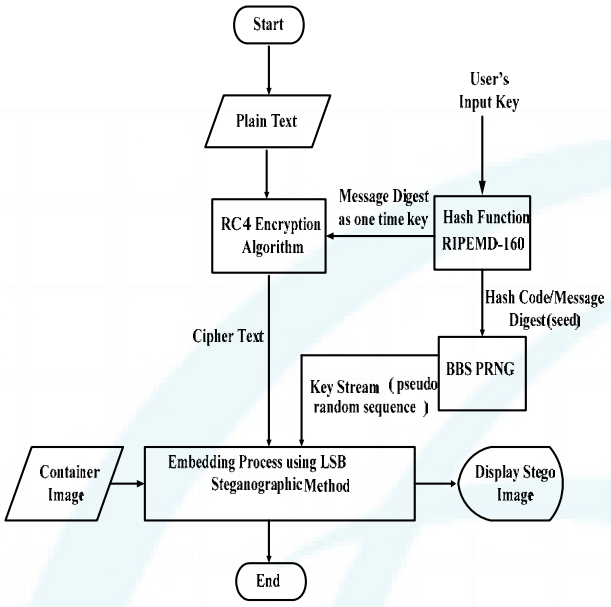

Figure 1: Overview of Data Embedding Technique

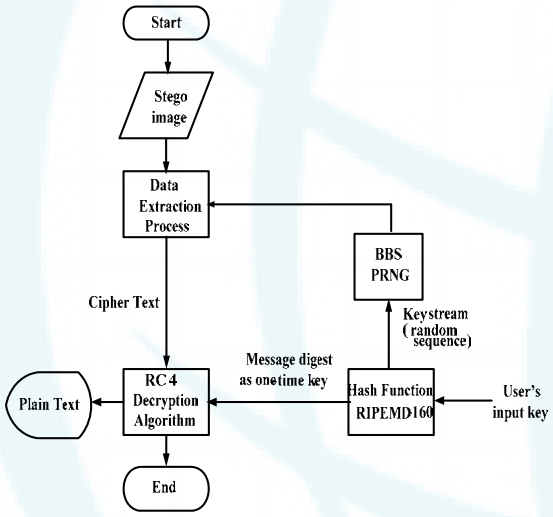

Figure 2: Overview of Data Extraction Technique

6. Experimental Result and Evaluation of Proposed System

In this section, a number of experiments which are used to investigate the effectiveness of our proposed method will be performed. In our experiments, we use 5 text files as secret messages. The size of embedded text files are 2 KB, 4 KB, 6 KB, 8 KB and 10 KB. We use 6 BMP image files as the cover image. These BMP files are different sizes and shown in figure-3. In each image, all 5 testing encrypted messages (2 KB, 4 KB, 6 KB, 8 KB and 10 KB) are embedded. Then we analyze the stego image by PSNR (peak signal to noise ratio) and MSE (mean square error) parameters.

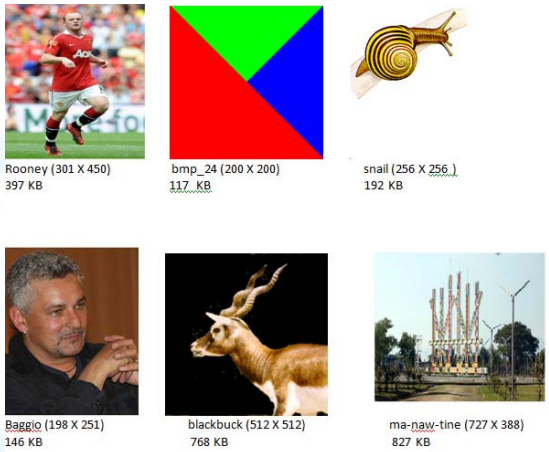

Figure 3: Testing Images for Proposed System

6.1 Image Quality Measures (IQMS)

In order to evaluate the success of the proposed method, some of the well-known IQMs are employed: Mean Squared Error (MSE), and Peak Signal to Noise Ratio (PSNR). The quality measure of PSNR is defined with, Peak signal-to-noise ratio, often abbreviated PSNR, is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. Because many signals have a very wide dynamic range, PSNR is usually expressed in terms of the logarithmic decibel scale. If the PSNR value is greater than 45 for a stego-image, then we can treat it as a good quality image [12].

PSNR is used in many image processing applications and considered as a reference model to evaluate the efficiency of other objective image quality evaluation methods. PSNR as a metric computes the peak signal-to-noise ratio, in decibels, between two images [13].

On the other hand, MSE measures the statistical difference in the pixel values between the original and the reconstructed image. The mean square error represents the cumulative squared error between the original image and the stego-image. A lower MSE value means a better image quality i.e lesser distortion in the cover image while the higher the PSNR value the better the quality of the image. PSNR and MSE are defined as shown in the following respectively [13].

$$PSNR = 10\log_{10}\left(\frac{R^2}{MSE}\right) \quad (1)$$

$$MSE = \frac{\sum_{M,N}[I_1(m,n) - I_2(m,n)]^2}{M * N} \quad (2)$$

M and *N* are the number of rows and columns in the input images, respectively. Here, R is the maximum possible pixel value of the image. When the pixels are represented using 8 bits per sample, this is 255. The PSNR and MSE values are calculated for original and stego images and the results are as shown in Table-1 to Table-5.

International Journal of Scientific Engineering and Research (IJSER)
www.ijser.in
ISSN (Online): 2347-3878
Volume 1 Issue 2, October 2013

Table 1: Results for PSNR and MSE values for 2 KB encrypted messages

Cover Images	*PSNR Value*	*MSE Value*
Rooney	61.198	0.049349
bmp_24	55.9193	0.1664
snail	58.0875	0.101
Baggio	56.8551	0.13414
blackbuck	64.1024	0.025284
ma-naw-tine	64.3588	0.023834

Table 2: Results for PSNR and MSE values for 4 KB encrypted messages

Cover Images	*PSNR Value*	*MSE Value*
Rooney	59.0227	0.081435
bmp_24	53.7802	0.27231
snail	55.9693	0.16449
Baggio	54.6549	0.22263
blackbuck	61.9499	0.041504
ma-naw-tine	62.2959	0.038325

Table 3: Results for PSNR and MSE values for 6 KB encrypted messages

Cover Images	*PSNR Value*	*MSE Value*
Rooney	56.4789	0.14628
bmp_24	51.2738	0.48495
snail	53.3317	0.30194
Baggio	52.147	0.39663
blackbuck	59.3634	0.075291
ma-naw-tine	59.6836	0.069939

Table 4: Results for PSNR and MSE values for 8 KB encrypted messages

Cover Images	*PSNR Value*	*MSE Value*
Rooney	55.4496	0.18541
bmp_24	50.1605	0.62666
snail	52.3083	0.38217
Baggio	51.055	0.51001
blackbuck	58.2706	0.096832
ma-naw-tine	58.587	0.090028

Table 5: Results for PSNR and MSE values for 10 KB encrypted messages

Cover Images	*PSNR Value*	*MSE Value*
Rooney	54.3555	0.23852
bmp_24	49.0645	0.80655
snail	51.1713	0.49653
Baggio	50.0242	0.64663
blackbuck	57.2606	0.12219
ma-naw-tine	57.53	0.11484

According to the table-1 to table-5, the proposed method can get PSNR and MSE values for different file sizes. When embedded secret data size is less, PSNR is high and MSE is low. We can see clearly this testing result by these tables. According to the testing results, the lowest file size (2 KB) has the lowest MSE value and highest PSNR value. Moreover, the highest file size (10 KB) has the lowest PSNR value and highest MSE value. We can get good quality images by testing our method because of PSNR value is greater than 45 for all stego images.

6.2 Histogram Analysis

The degradation of the quality of images can also be visually noticed by applying the histogram analysis. In statistics, a histogram is a graphical display of tabulated frequencies, shown as bars. It shows what proportion of cases fall into each of several categories: it is a form of data binning. So, we have compared the histogram of three different images where the histogram is calculated for R, G and B channel separately [12]. The image histogram for 2 KB encrypted message is computed for the original image and stego image and it is shown in Fig. 4, 5, 6, 7, 8 and 9. The histograms of both the images are quite similar. Hence the proposed technique is found to withstand statistical attacks based on histogram analysis.

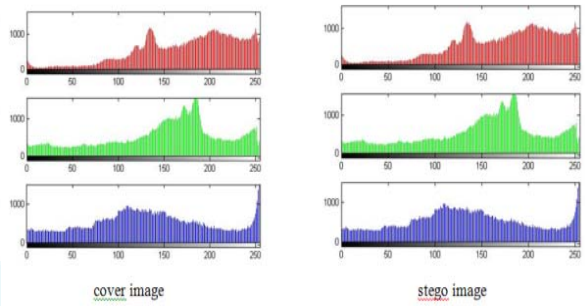

Figure 4: Histogram of Original and Stego for Rooney.bmp

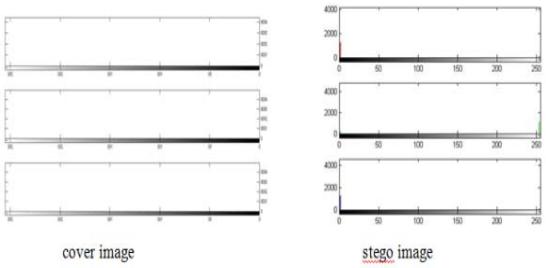

Figure 5: Histogram of Original and Stego for bmp_24.bmp

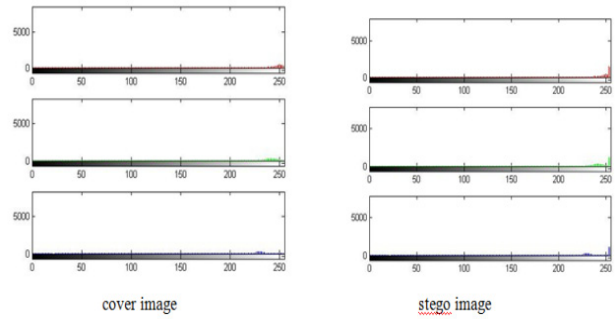

Figure 6: Histogram of Original and Stego for snail.bmp

International Journal of Scientific Engineering and Research (IJSER)
www.ijser.in
ISSN (Online): 2347-3878
Volume 1 Issue 2, October 2013

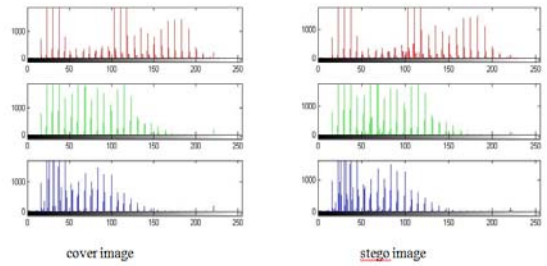

Figure 7: Histogram of Original and Stego for Baggio.bmp

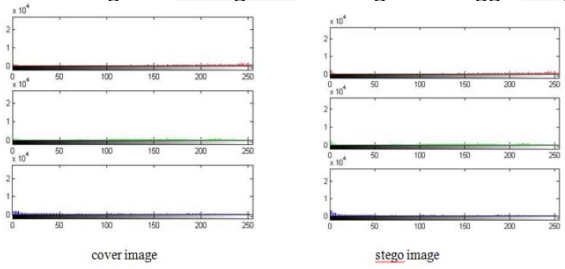

Figure 8: Histogram of Original and Stego for blackbuck.bmp

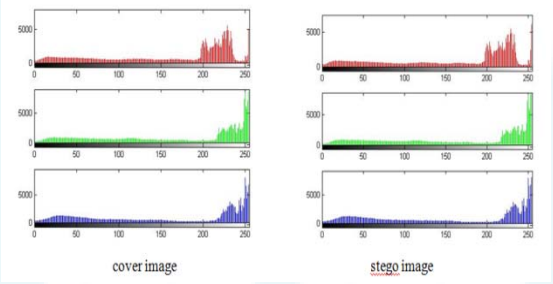

Figure 9: Histogram of Original and Stego for ma_naw_tine.bmp

7. Conclusion

This system presents a LSB modified data hiding method for image steganography applications. This method modifies LSB 1 and LSB 2 of the cover image according to PRNG sequences. The stego image minimizes the difference between the original values of the cover pixels and the stego-images. The increasing PSNR intends to provide high secret communications, so the attacker can't notice the differences between the original cover image and stego-image. Two techniques, namely encryption and PRNG based embedding are used in LSB embedding to enhance its security. If an attacker wants to get the original messages, he must know secret key and random sequences. Experimental results show that proposed system gets high PSNR and low MSE for good image quality. Finally, we can conclude that the proposed technique for data hiding is useful for secret data communication.

References

[1] R.Amirtharajan, R.Akila, P.Deepika Chowdavarapu," A Comparative Analysis of Image Steganography", International Journal of Computer Applications (0975-8887), Volume 2-No.3, May 2010

[2] Wai Wai Zin, "LSB Based Random Byte Data Embedding", International Conference on Computer Applications, ICCA 2012, February 28th-29th, Yangon, Myanmar

[3] Christian Cachin, "An Information-Theoretic Model for Steganography", In Proceedings of 2 nd Workshop on Information Hiding (D. Aucsmity, ed.), Lecture Notes in Computer Science, Springer, 1998.

[4] Mamta Juneja, parvinder Singh Sandhu, "Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption", 2009 International Conference on Advances in Recent Technologies in Communication and Computing.

[5] Neha Sharma, Mr.J.S.Bhatia, Dr(Mrs) Neena Gupta, "An Encrypto-Stego Technique Based Secure Data Transmission System", PEC, Chandigarh, May, 2005

[6] Yogendra Kumar Jain, R.R. Ahirwal, "A Novel Image Steganography Method With Adaptive Number of Least Significant Bits Modification Based on Private Stego-Keys", International Journal of Computer Science and Security, Vol-4, Issue-1.

[7] V. Lokeswara Reddy, Dr.A.Subramanyam, Dr.P.Chenna Reddy, "Implementation of LSB Steganography and its Evaluation for Various File Formats", International Journal of Advanced Networking and Applications, Volume:02, Issue: 05, Pages: 868-872 (2011)

[8] P.Singh, Balkrishan, "Java implementation of Least Significant Bit Embedding for Hiding Data", Indian Science Abstracts, SSN: 0019-6339, Volume 45, No. 12, June 16, 2009

[9] Kevin Curran, Karen Bailey, "An Evaluation of Image Based Steganography Methods", International Journal of Digital Evidence, Fall 2003 Volume 2, Issue 2.

[10] Muhalim Mohamed Amin, Subariah Ibrahim, Mazleena Salleh, Mohd Rozi Katmin, "Information Hiding Using Steganography", Department of Computer System & Communication Faculty of Computer Science and Information System, University Technology Malaysia, 2003

[11] Rajanikanth Reddy Koppola, "A High Capacity Data Hiding Scheme in LSB Based Image", Thesis: The Graduate Faculty of the University of Akron, May 2009.

[12] Sudipta Kr Ghosal, "A New Pair Wise Bit Based Data Hiding Approach on 24 Bit Color Image using Steganographic Technique", IEMCON 2011 Organised By IEM in Collaboration with IEEE on 5th and 6th January.

[13] Gabriel Macharia Kamua, Stephen Kimani, Waweru Mwangi, "An enhanced Least Significant Bit Steganographic Method for Information Hiding", Journal of Information Engineering and Applications, ISSN 2224-5782 (print) ISSN 2225-0506 (online), Vol-2, No.9, 2012.

Author Profile

Wai Wai Zin received the B.C.Tech and M.C.Tech degrees from University of Computer Studies, Mandalay in 2002 and 2006, respectively. From 2006, she served at Computer Univesity (Myitkyina) as an

Assistant Lecturer. Now she is a PhD candidate at University of Computer Studies, Mandalay. Her interested field is cryptography and steganography.

Than Naing Soe has got bachelor degree from Magwe University in 1995 and got Master degree (Master of Information Science MISc) from UCSY (University of Computer Studies, Yangon) in 2000. And then he has got degree of ME (IT) from MEPhI (Moscow Engineering Physics Institute), Russia in 2004 and got degree of PhD (IT) from MEPhI in 2007. He is now Associate Professor of Computer University (Myitkyina). He is interested in the areas of Cryptography, Information security, Network security and GIS.