International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 06 | June -2017 www.irjet.net p-ISSN: 2395-0072

SECURING HIGH CAPACITY DATA HIDING USING COMBINED DATA HIDING TECHNIQUES

Isaac Anokye[1] , Joseph Kobina Panford[2], James Ben Hayfron-Acquah[3]

[1]Postgraduate Student, Kwame Nkrumah University of Science and Technology, Kumasi, Ghana
[2,3]Senior Lecturers, Kwame Nkrumah University of Science and Technology, Kumasi, Ghana

---

Abstract - In recent times, the need for digital communication has increased dramatically and as a result, the Internet has become the effective and faster means of communicating digitally. However, the security of information over the internet has become a major issue. As a result, a new domain dedicated to information security has evolved and is known as data hiding. Steganography, cryptography and password are three different types of data hiding techniques. Steganography hides messages inside some other digital media. Cryptography, on the other hand obscures the content of the message and password authenticate users to have access to resources. Research in various institutions shows communication teams face problems of sending sizeable amount of message and securing this message so that it gets to the intended user. The main objective of this research is to provide security to data as well as achieving high payload. In this paper, a message is first encrypted and is giving a password. The encrypted message is then hidden using Least Significant Bit (LSB) image steganography. In order to prove the efficiency and the security level of this system, the system was tested and analyzed using statistical framework and the ultimate aim was achieved. The system is estimated to give up to about 97% accurate results.

Keywords: Cryptography, Steganography, LSB image Seganography, Password, Payload.

1. INTRODUCTION

In recent times, the Internet has become the effective and faster means of communicating digitally. Nevertheless, data on the Internet has become susceptible to copyright infringement and piracy and therefore requires secret communication.

1.1 Statement of problem

Thorough research in security services and banking institutions shows that, communication teams of these institutions face problems of sending sizeable amount of message and securing this message so that it gets to the intended user without the data being intercepted by unauthorized users.

1.2 Research Objectives

- Provision of visual and statistical resistance to attacks, and
- Achieving more payloads in data hiding.

1.3 Research Questions

The research questions are as follows:

- Will the use of password, transposition cipher cryptography, and least significant bit image steganography help protect messages from being intercepted by unauthorized users?
- Will the use of LSB image steganography help in hiding more data?

1.4 Significance of the study

Most of the previous studies in data security are centered on steganography, password or cryptography. But steganography alone is never secured let alone cryptography and password. But when combining these methods, three layers of protection can be attained which will then satisfy the three data embedding requirements.

This report will emphasize on the need to develop a scheme that satisfies the three data hiding requirements such that a message which is meaningful can be highly protected by combining three basic data hiding techniques so that the message gets to its intended user without being intercepted by unauthorized users.

2. LITERATURE REVIEW

The chapter two is concerned with reviewing other people's work that is related to this study. The main aim for this paper work is to secure high capacity data hiding using combined data hiding techniques.

Chadramouli et al. (2001) presented "Analysis of LSB Based Image Steganography Techniques." This approach gives an analysis of LSB based steganography techniques. The embedding capacity of LSB method can be increased by using two or more least significant bits. At the same time, not only

the risk of making the embedded message statistically detectable but also the image fidelity degrades.

Lee et al. (2000) proposed "High capacity image steganographic model." They presented a variable-sized LSB embedding scheme in which the number of LSBs used for message embedding /extracting depends on the local characteristics of the pixel. The advantages of LSB-based method are easy to implement. Unfortunately, the hidden message is accessible due to a slight modification from the active warden.

Marvel et al. (1999) presented "Spread spectrum image steganography (SSIS)." They proposed an image steganographic method that hides and recovers the message within digital imagery. The SSIS incorporated the use of error-control codes to correct the large number of bit errors.

Silvia et al. (2004) presented a "Robust Steganography using Bit Plane Complexity Segmentation." They proposed steganography algorithm based on bit plane complexity segmentation which permits to implement hiding information into images for its save transmission through a non-secure channel. In this paper a specific secret-key image based steganographic model proposed which uses an image as the cover data and the secret information is embedded in the cover data to form the stego data which is also an image. The stego image has been divided into several segments using normalized cut method and each segment containing the parts of the embedded message transmit separately to the receiver. This work proposes a novel algorithm with higher security features so that the embedded message cannot be hacked by unauthorized user.

Palette based images, such as GIF images, are popular image file format commonly used on the internet. GIF images are indexed images where the colours used in the image are stored in a palette. GIF images can also be used for LSB steganography although extra care should be taken.

According to Fridrich et al. (2001) who presented "Detecting LSB steganography in color and gray-scale images" They proposed that if one changes the least significant bit of a pixel, it could result in an entirely different colour since the index to the colour palette gets modified. One possible solution to this problem is to sort the palette so that the colour differences between consecutive colours are minimized. The strong and weak points regarding embedding information in GIF images using LSB is that since GIF images only had a bit depth of 8, the total amount of information that could be embedded will be less. GIF images are vulnerable to statistical attacks as well as visual attacks, since the palette processing which has to be done on the GIF image leaves a clear signature on the image. This approach was dependent on the file format as well as the image itself, since a wrong choice of image could results in the message being visible.

Chincholkar, Y.D. and Gutte, R.S. (2012) on the other hand presented "steganography comparisons on one and two LSB positions". In their research, an encrypted plain text was embedded in an image. The message hidden in the cover image had the length of ninety characters therefore in an attempt to embed more than 90 characters, the Mean Square Error increases and corresponding decrease in Peak Signal To Noise Ratio was observed. Therefore when payloads were increased to more than 90 characters, the Peak Signal To Ratio of the mages fell below 30(dB) thereby creating an impression of distorted image.

3. METHODOLOGY

A system for embedding a sizeable amount of text data in an image with the use steganography, cryptography and password is proposed in this research.

Transposition cipher cryptography and Least Significant Bit image steganography together with password were employed here in order to improve the amount of data embedded in an image and also help to develop an unnoticeable image after the embedding process so as to solve the problem of unauthorized data access. When steganography is implemented to cryptographic data with password, the security of that data is highly increased. A text data in this method is first encrypted with the help of transposition cryptography. This encrypted data is then given a password and the resultant data is then hidden in an image using LSB image steganography. It is noted that hiding a message using LSB image steganography only is never greatly secured but combining cryptography with password will make the data highly secured such that even if attackers defeat the steganographic technique to detect the message from the stego image, password would still be required to get the encrypted data and cryptographic decoding method would also be required to decrypt the encrypted data.

The proposed framework is illustrated in figure 1.

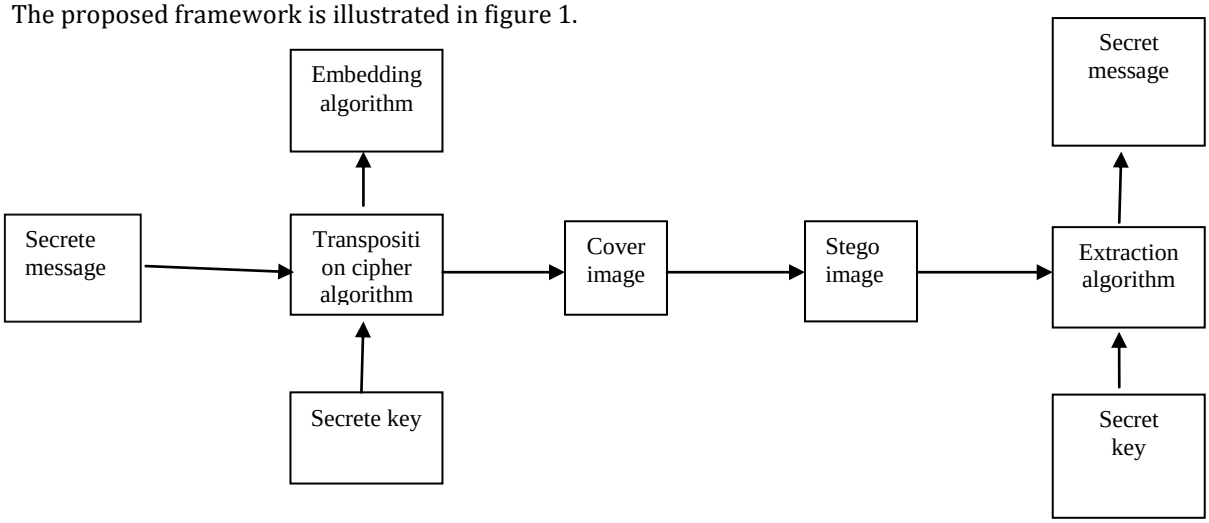

Figure1: Graphical representation of the program

4. RESULTS AND INTERPRETATION

This research work is done to ensure that high capacity data is encrypted and hidden in an image with password so as to make the data highly secured. The figure 2 to figure 4 depict the images before and after the embedding of data.

Figure 2(a): Hebi cover image

Figure 2(b): Hebi stego image

Figure 3(a): lotus cover image

Figure 3(b):lotus stego image

Figure 4(a): Sunflower cover image

Figure 4(b): Sun flower stego image

After the embedding process, MADLAB computer application was used to calculate for the experimental results. Table 1 and Table 2 were deduced from the experimental results calculated for analysis.

When the embedding data increases, the Mean Square Error also increase, and this will cause the Peak Signal To Noise Ratio(PSNR) also to decrease and vice versa. The PSNR is expressed in decibels (dB). PSNR values falling below 30 dB indicate a fairly low quality image that is image alteration can be noticeable due to data embedding. Hence, high quality image after embedding should be 30 dB and above. The experimental results obtained point out clearly that the embedding process did not introduce any perceptual deformation and for that matter higher PSNR was obtained. To determine the deformation caused by the embedding process in the cover image, the PSNR of some images was observed after the embedding process. It was clearly seen that the PSNR persistently moved beyond 30dB as shown in Table 1 which means that image distortions after embedding process could hardly be seen by the human eye.

Table 1: Mean Square Error(MSE) and Peak Signal To Noise Ratio(PSNR) valuefor the original and stego images

Cover Image	Stego Image	Amount of embedded data	MSE %	PSNR (dB)	Amount of extracted data
Sun (147KB)	Sun stego(147KB)	607 Bytes	0.62	30.05	607 Bytes
Lotus(147KB)	Lotus stego(147KB)	607 Bytes	0.41	31.42	607 Bytes
Hebi (147KB)	Hebi stego(147KB)	607 Bytes	0.57	31.71	607 Bytes

Table 2: Image parameters for cover and stego image

	Before Steganography			After steganography			
Image	**Mean**	**Standard Deviation**	**Entropy**	**Image**	**Mean**	**Standard Deviation**	**Entropy**
Hebi	122.7032	100.2805	6.8457	Hebi stego	122.6980	100.2759	6.8707
Lotus	225.3907	47.2974	5.0209	Lotus stego	225.3674	47.2824	5.1097
Sun	142.9557	54.7812	7.6939	sun stego	142.9557	54.7812	7.6939

From table 2, it can be clearly seen that there is no considerable variation that exist in the mean, standard deviation and entropy of original image and the stego image. It is hereby noticed that with respect to image parameters, the degree of difference in the stego image is very minimal as compared to the cover image.

Comparing this study to that of Gutte and Chincholkar which also hides encrypted data in a cover image, it was observed that, the length of plain text that can be embedded in Gutte and Chincholkar's study was 90 characters and for that matter in an attempt to embed more than 90 characters, the Mean Square Error will increase and corresponding decrease in Peak Signal To Ratio will be observed. Therefore when payloads were increased to more than 90 characters, the PSNR of the images fell below 30 dB thereby creating an impression of distorted image.

In this paper, payloads were increased to more than 90 characters to the size of 607KB and yet the Peak Signal To Ratio values ranges from 30 dB and above indicating high image quality.

The experimental results also indicate that figures of the mean, standard deviation and entropy of image before and after embedding of data are closely the same.

Therefore, since there have not been any significant change in the image parameters of both original and stego image, the procedure gives an excellent cover up of information and minimizes the possibility of the hidden information being noticed. That is indicating a complete safe and sound steganography system. Then again, the data hidden can be obtained devoid of any loss of data. Another most important benefit of this study is that, the system has got password to authenticate the user before he or she gets access to the encrypted data thereby boosting the security aspect of the system.

5. CONCLUSION

This project was meant to secure high capacity data hiding. This proposed technique helps to spot out a very brilliant data hiding method. The ultimate aim of image steganography is to hide the very existence of data that is embedded in an image, but it is realized that steganography alone is not a brilliant idea for data secrecy. The same thing applies to encryption and password. Nevertheless when these three techniques are put together, three layers of protection will be attained thereby boosting security aspect of the data. It is now deduced that, when a text data is encrypted, given it a password and it is finally hidden using the LSB image steganography, data embedding requirements such as robustness, security and capacity are assured and therefore a sizeable amount of data can be hidden in an image. Hence the final image which is nw the stego image can be sent out without any fear of the secret message been revealed. Then also, in the case of an unauthorized user defeating the steganography method to find out that there is something hidden in the stego image, the person will have to provide a password to authenticate him or her to that resource and then again provide a decoding algorithm to decode and get access to the encrypted data.

In order to prove the efficiency and the security level of this system, the system was tested and analyzed using statistical framework

In conclusion, the ultimate aim for this research which is to provide a system that is able to bring out additional security to text data hidden in an image was achieved.

REFERENCES

P.C. Wu, W.H. Tsai, A steganographic method for images by pixel-value differencing, Pattern Recognition Letters

24 (2003) 1613-1626

N.N. El-Emam, Hiding a large amount of data with high security using steganography algorithm, Journal of Computer Science 3 (2007) 223-232.

Gutte, R. S. and Chincholkar, Y. D. (2012) "Comparison of Steganography at One LSB and Two LSB Positions", International Journal of Computer Applications, Vol.49,no.11, pp.1-7.

Dickman, S.D. (2007), "An Overview of Steganography", JMU-INFOSEC-TR-2007 002, http:// citeseerx.ist.psu.edu/viewdoc/summary? doi=10.1.1.137.5129.

Dunbar, B. (2002). "A detailed look at Steganographic Techniques and their use inan Open-Systems Environment", SANS Institute 2002, pp.1-9,http://www.sans.org.

Lee, Y-K. ; Bell, G., Huang, S-Y., Wang, R-Z. and Shyu, S-J. (2009), "An Advanced Least-Significant-Bit Embedding Scheme for Steganographic Encoding",

PSIVT 2009, LNCS 5414, Springer, pp. 349–360.

Smith, C. (2001), "Basic Cryptanalysis Techniques",SANS Institute 2001, GSEC Version 1.2f, http://www.sans.org.

Kaur, R., Singh, B. and Singh, I. (2012), "A Comparative Study of Combination of Different Bit Positions In Image Steganography", International Journal of Modern Engineering Research, Vol.2, Issue.5, pp-3835-3840.

Kruus, P., Caroline, S., Michael, H. and Mathew, M.(2002), "A Survey of Steganographic Techniques for Image Files", Advanced Security Research Journal, Network Associates Laboratories, pp.41-51.