TWO TIER SHIELD SYSTEM FOR HIDING SENSITIVE TEXTUAL DATA

Shafana A.R.F.

Department of Information and Communication Technology, South Eastern University of Sri Lanka, Sri Lanka.

shafana.cst@gmail.com

ABSTRACT: *Delivery of unapparent information through visual streams has always been a challenging task in this Information Era. Encryption has been assisting to hide the information over the decades, however, the drastic development in technology, has indeed jeopardized the security obtained in that approach by utilizing the backdoors of such encryption algorithms. In that juncture, to hide the existence of data itself, Steganography techniques were later introduced. This paper has combined the use of both mechanisms to ensure the secrecy, security, privacy and confidentiality of sensitive data, which first encrypts the sensitive data and later conceal it in a carrier media. The encryption is done through AES256 algorithm and Digital Images are used as carrier multimedia. At first, sensitive data are encrypted using AES256 algorithm. By employing the popular and secure Least Significant Bit (LSB) approach in Steganography, the encrypted messages are randomly embedded within a digital image to be perceived as general White Noises. The use of both mechanisms have made the process of unintended access even complicated because, though the image was suspected to contain any secret messages there is still complexity to track the cipher. Thus, this two-tier security system could be a low-cost, feasible solution to hide the secret messages in Personal Computers.*

Keywords: Steganography, Cryptography, AES256, Least Significant Bit

1. INTRODUCTION

Establishing a secret communication and hiding secret messages from unintended people have always been challenging tasks from the past. In most of the instances, for every mechanism that was developed to hide the sensitive data, a counterpart mechanism has been introduced over time. In that sense, it is the technique of Cryptography that has been commonly used in order to cipher the messages. However, the technological advancement in networks specially, has in fact deteriorated the security obtained in that approach. With the introduction of steganography, the technique to embed the data within a carrier multimedia such that the message is concealed to everyone except the intended user, the security and privacy have been rebuilt to a certain extent.

In spite of these advancements in techniques and technologies, still a loophole exists. Thus, it could be perceived that the conjunction of the two mechanisms such as Cryptography and Steganography would provide a better form of security as well as privacy to sensitive data as a robust mechanism. This paper presents an application that first encrypts the message using robust symmetric key encryption algorithm and later the encrypted message would be concealed

ISBN 978-955-627-128-1

in an image such that their existence itself is hidden. Thus, it provides a two-tier shield for sensitive data.

The main objective of this research is to develop an application that hide the encrypted secret message within a still image in order to obtain maximum privacy and secrecy in Personal Computers. The use of personal images could make the application further confidential (Al-Otaibi & Gutub, 2014).

2. METHODOLOGY

2.1 Overview

Steganography employs various type of cover objects known as carrier multimedia such as text, image, audio and media (Shikha & Dutt, 2014). The carrier multimedia that is used to conceal in this research is the digital still images. A digital image is a collection of pixels, an array of coloured dots. Each pixel of an image (RGB image) comprises of three components: one for red, one for green and one for blue. A pixel is typically represented with 24 bits, where 8 bits correspond to each of the three colours above (8 bits that represent transparency is not taken into account for this scenario). Therefore, the intensity values range from 0-255.

The Least Significant Bit (LSB) Steganography has been the most reliable approach to conceal secret messages (Atee, Ahamed & Noor, 2015). With 8 bits, the most significant value that could be represented is 128 and the least significant value is 1. Since the last four bits typically contains lower values such as 8,4,2,1 any changes in these four values do not make any visible changes in the image. Thus, the last 4 bits of each colour component would provide a plenty of space to hide an encoded message. In addition to that, blue component holds the least amount of colour information. Therefore, the last 4 bits of each component and the blue component itself is replaced with the hidden message. This would be still good and no significant changes could be perceived. The availability of such secret message in random would be perceived as general white-noises of a digital image.

2.2 The Encryption and Steganography process

At first, the plain text or the secret message is encoded using robust symmetric key algorithm, AES256, the algorithm that was chosen by U.S. National Institute of Standards and Technology as Advanced Encryption Standard (AES). The insignificant bits were then replaced with the encrypted secret message. The encrypted message would just appear as random as the picture data that was

ISBN 978-955-627-128-1

replaced. This particular replacement would not cause much significant changes in the cover image.

The top-level architecture of the overall process is depicted in Figure 1

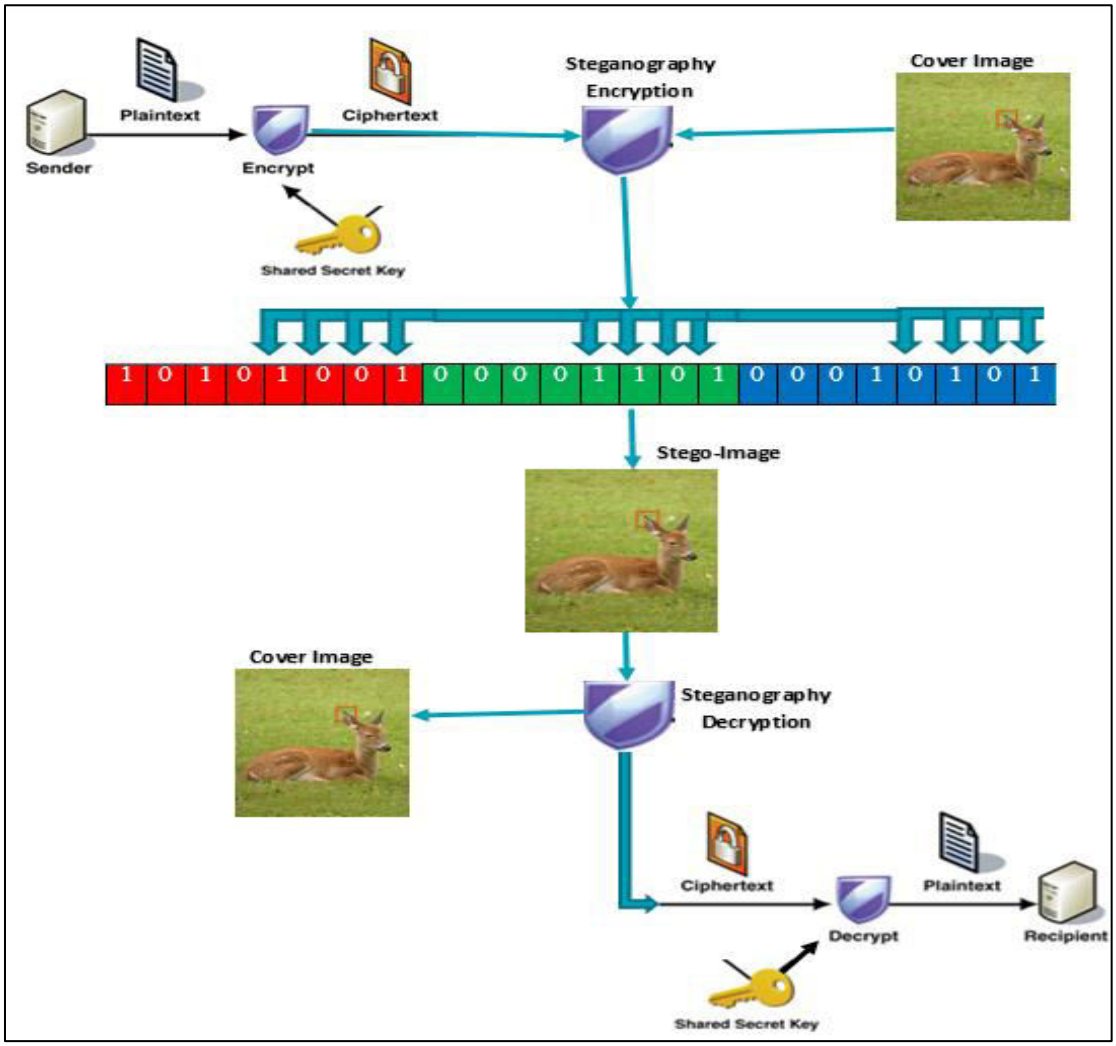

Figure 1. Top Level Architecture of the Process

2.3 Implementation of the system

The implemented security system, *Keep It Secret*, for hiding the sensitive textual data is implemented on Java Programming Platform. Running the implemented system begins with the application that prompts the user to input the secret sensitive text message (Figure 2). When “Encode Now” button is pressed, it allows the user to search for the image as cover media (Figure 3). Supported input image formats are: JPG, JPEG, PNG and GIF. This initiates both the

ISBN 978-955-627-128-1

encryption and data hiding processes which result with the request of new file name for the Stego-image (Figure 4), the image that is embedded with the user's secret data. Output image is saved in PNG format with hidden text in it.

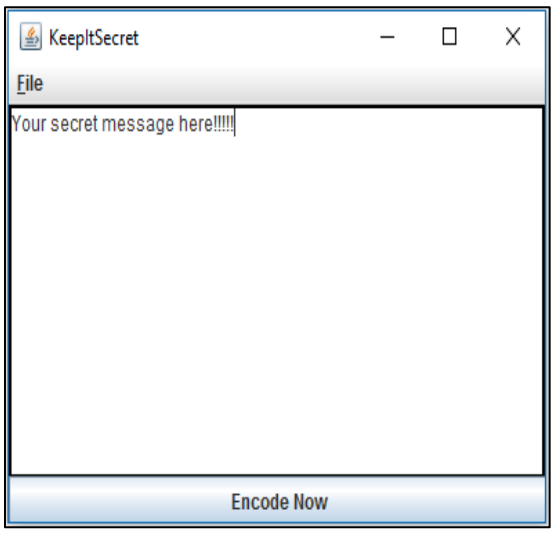

Figure 2. Interface to input secret message

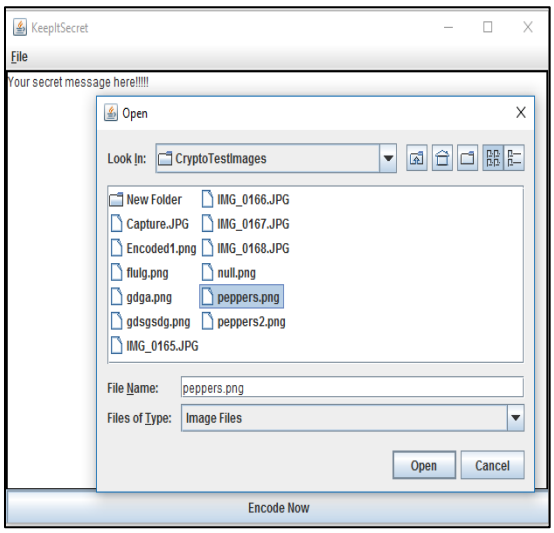

Figure 3. Interface to select cover image

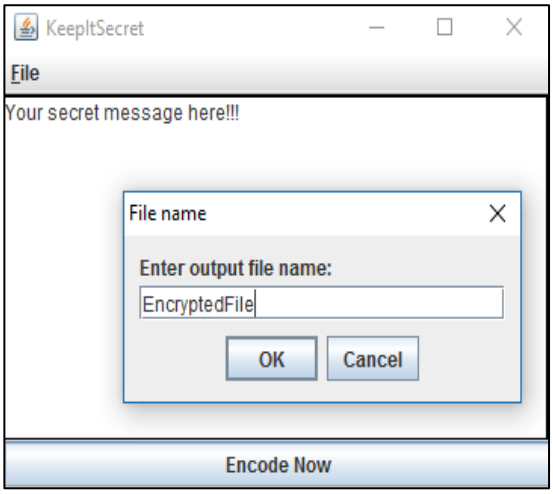

Figure 4. Interface to save Stego-image

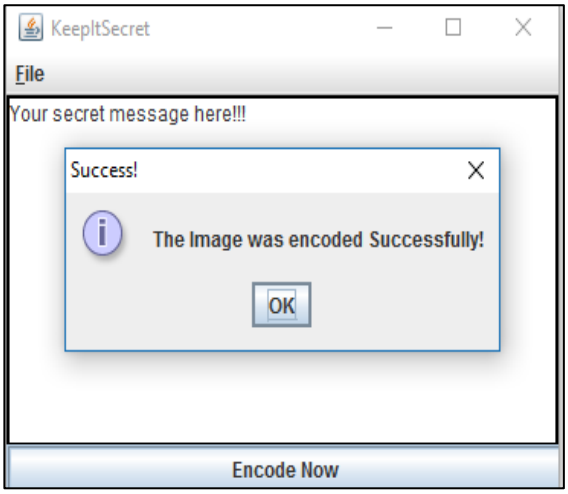

Figure 5. Message displayed at successful encryption

The similar procedures are done to reveal the hidden text message by means of inputting a Stego-image where the message is displayed to the user.

3. RESULTS AND DISCUSSION

Different grayscale as well as true images were used as host images in the study. The used host images are presented in Fig. 6 and Fig. 7 respectively. The figures give a comparative view of images before and after embedding using the proposed method.

ISBN 978-955-627-128-1

Figure 6. a) Images before embedding secret messages

Figure 6. b) Resultant images embedded with secret messages

Figure 6. The gray scaled host images

Figure 7. a) Images before embedding secret messages

Figure 7. b) Resultant images embedded with secret messages

Figure 7. The true coloured host images

ISBN 978-955-627-128-1

The visual perspective of the above pairs of images reveals that the images before embedding and the embedded images are appearing to be identical. The obtained results were also tested in MATLAB and respective histograms were plotted as depicted in Fig. 8. And, the results proved to be positive, since there is no remarkable differences between the histograms of cover image and stego-image despite both having different file sizes.

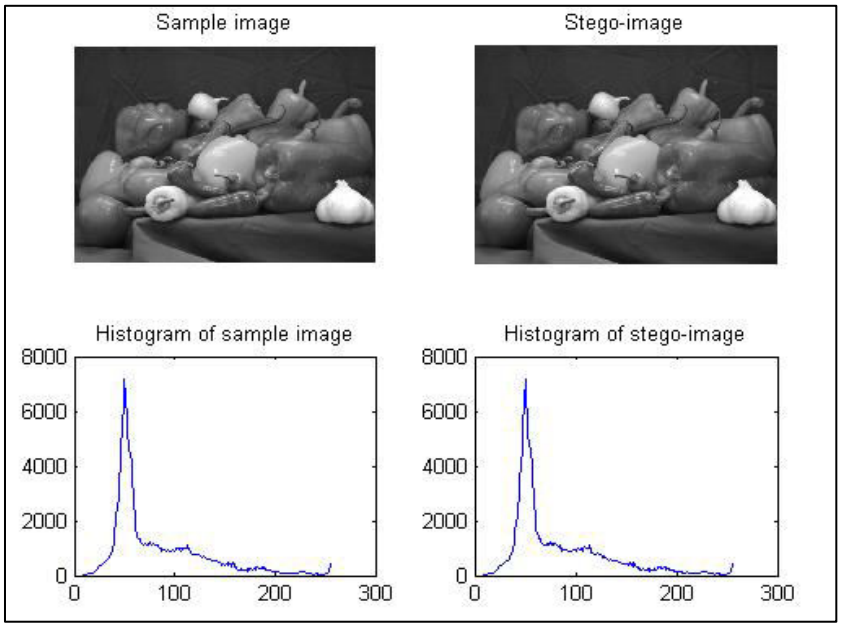

Figure 8. Histograms of a Cover image and its Stego-image

The current study has been successful in implementing a security system that is appropriate to hide sensitive data in Personal Computers. As future work, the current application will be upgraded as a portable application based on mobile platforms ie. Android as well, such that an innocuous communication comprising secret messages between intended users could also be established.

4. CONCLUSION

This paper proposes and presents a security system that allows its users to hide sensitive and secret messages such as passwords, e-mail messages, credit card information within an image, such that it is protected from unintended users. The study has combined cryptography and Steganography to provide a better security and privacy. The use of both have made the process of unintended access even complex because even if the image was suspected to contain any secret messages there is still complexity to track the cipher. Thus, this security system could be a low-cost, feasible solution to hide the secret messages in Personal Computers.

ISBN 978-955-627-128-1

5. REFERENCES

Al-Otaibi, N.A. & Gutub, A.A. (2014). *Flexible Stego-System for Hiding Text in Images of Personal Computers Based on User Security Priority*. Proceedings of 2014 International conference on Advanced Engineering Technologies (AET-2014), Dubai, 243-250.

Atee, H.A., Ahmad, R. & Noor, N.M. (2015). Cryptography and Image Steganography Using Dynamic Encryption on LSB and Color Image Based Data Hiding. *Middle-East Journal of Scientific Research*. 23 (7): 1450-1460

Shikha & Dutt, V.K. (2014). Text Steganography. *International Journal of Advanced Research in Computer Science and Software Engineering*. 4 (10): 615-616

ISBN 978-955-627-128-1