International Journal of Engineering & Technology, 7 (2.20) (2018) 30-32

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Secure message exchange using text to image encoding

Swastik Barik[1]*, J. Manikanta Sai[2], Ch. Prasannanjaneyulu Reddy[3], P. Kalyan Chakravarthy[4]

[1]Department of Computer Science and Engineering, KLEF Deemed to be University.
[2]Department of Computer Science and Engineering, KLEF Deemed to be University.
[3]Department of Computer Science and Engineering, KLEF Deemed to be University.
[4]Asst Professor, Department of Computer Science and Engineering, KLEF Deemed to be University.
**Corresponding author E-mail:swastik42barik@gmail.com*

Abstract

The work focuses mainly on data security problems while transferring data through a network, using text-to-image encryption. This approach creates an image out of the textual data using steganography, which allows the sender and the intended recipient to hide their confidential data while transmitting through the network. First, binary representations of the text data are made, then the binary data is used to create an image by using it as pixel intensities. This image is then merged with a colour image to obtain the final encrypted image. The main objective of the work is to demonstrate an encryption scheme that is reliable and easy to implement.

Keywords: *Text to image encryption, grayscale image, RGB image.*

1. Introduction

Today, to hide important documents, misinformation is used so that confidential information is protected and different methods have been developed to achieve this [2]. This can be done in many ways such as manipulating the data so that it is unreadable to the attacker. Steganography, on the other hand, is a technique in which a secret message is encoded inside an image and a person cannot see any hidden message in the image. The cover containing the confidential data is then transmitted to the recipient. The recipient can retrieve the message with a secret key provided by sender. In this paper, we discuss an encryption scheme that uses traditional cipher techniques as well as concepts of steganography to convert the given plaintext into an encrypted form and further convert it into an image and merge it with a colour image cover.
Here, we have used MATLAB tool to make it convenient for us while handling the text to image conversion and merging of images. It has very useful in-built functions which are capable of complex operations with very less code. The entered text is converted into its ASCII equivalent which is further converted into its equivalent binary. This binary data is arranged in matrix data structures and a noise image is generated from this data. The noise image is further merged with another image after offsetting.

2. Steganography and cryptography

2.1. Steganography

Steganography [15] [13] is the process of embedding the data or plaintext in a particular image, without changing the image itself. Every image has some redundant data bits which are simply repetition of bits that represent the same colour pixels. The redundant bits of the image are replaced with the data bits. Such a trap is completely confidential. This type of standard uses a cover image in which the data, the personal information transmitted and the encoding coding algorithms must be integrated into the image.

2.2. Cryptography

Cryptography [15] [13] refers to the practice of manipulating the data into a form that is recognized only by people for whom it is meant. It has existed in the human society since ancient times. For example, Caesar Cipher is a very basic cipher, in which the each of the letters is replaced by another letter a fixed number down the alphabets. This was utilized by Julius Caesar to communicate secretly, hence the name Caesar Cipher. Further researches in the field of cryptography gave rise to modern encryption schemes like AES and DES. However, modern cryptography does limit to encryption through traditional methods.
Elliptic Curve Cryptography is cross domain encryption concept that involves utilizing the properties of elliptic curves to design encryption methods. There are other cross domain encryption concepts other than this.

3. Analysis of digital image

A digital image [14] consists of many picture elements called pixels. The images that we see are collections of pixel arrays that are arranged in a specific order. Thus each pixel has a fixed position as defined by the rows and columns of the matrix it is contained in. Along with the position, another parameter comes into play is intensity. Every pixel has its own intensity which represents a particular shade. There are two types of images-black & white or grayscale and colour. Grayscale images are composed of pixels that only range from highest to lowest shades of gray. Since each binary bit can represent either 0 or 1, an 8-bit intensity range can represent 256 shades. All grayscale images are 8-bit images with gray intensity varying from 0 to 255. On the other hand, colour images also known as RGB images are composed of three different intensity components namely Red (R), Green (G) and

Blue (B). Each intensity category is of 8-bit range varying from 0 to 255. Since colour images contain 3 x 8-bit intensity ranges, they are also called 24-bit images.

4. Overview of encryption schemes

The plaintext is fed to the input dialog of the tool which then is optimized for being read into an array [1]. This array is subjected to various transformations which serve as the encryption for the data. As for the steganography part i.e. merging of images and hiding the data in redundant bits, follows the encryption.

The plaintext is converted into its ASCII equivalent. The ASCII character encoding is a very widely used character encoding as well as it covers all the characters that are used in general text documents. Since every character has its unique numerical code, it is easy to distinguish them.

The array containing the coded numerical equivalents of the characters are subjected to decimal to binary conversion. Thus each character has its binary representation. This binary data serves as the base for creating a noise image using MATLAB functions.

This noise image can be further randomized if offsetting is done before converting the binary data into image. Offsetting is the process of adding random bits to make a value appear different. The original value can be obtained simply by subtracting the added value. The obtained noise image is then merged with a colour image which serves as the cover image [1].

Decryption of the image to obtain back the data involves the reverse of all the operations in exact reverse order. The scheme is meant to be symmetric in nature to reduce the complexity without sacrificing the security aspect.

5. Text-to-Image conversion

The binary data that is given as input to a MATLAB function which creates an image by taking the binary bits as pixel intensity data. The image is thus created according to the intensity data generated out of the plaintext. Thus a noise image is created. If the plaintext is small in length, then the image appears as a barcode. If the input is of huge length then the image appears to be noisy. Thus large number of characters can be represented by minute pixels. The figure bellow shows the images generated by different text lengths:

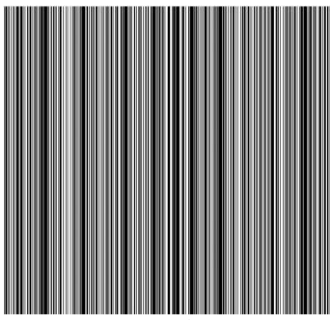

Fig. 1: Barcode image for short text length

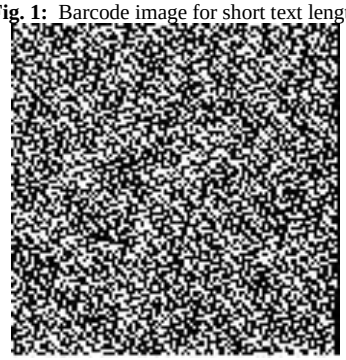

Fig. 2: Noise image for long text length

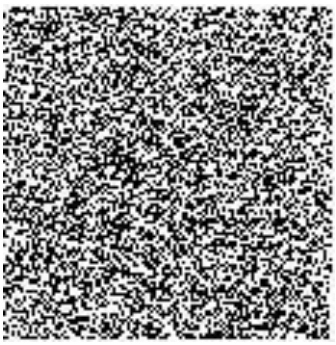

Fig. 3: Noise image after offsetting

6. Merging images

After the creation of the noise image, it is merged with a colour image cover. The created noise image is a gray 8-bit image because the decimals on conversion give 8-bit values. Thus we take advantage of the 24-bit intensity data available from the coloured cover image. The 24-bit image has a huge diversity of shades which makes it difficult to extract the hidden data from the image. The figure bellow show the effect of merging:

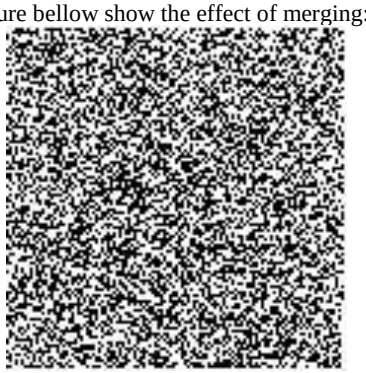

Fig. 4: Offset noise image

Fig. 5: Colour cover image

Fig. 6: Final encrypted image

7. Histogram analysis of encrypted image

Histogram is a kind of bar graph that gives us insight into the frequencies of certain parameters in a distribution. Here we have used histogram analysis to observe the variation in different pixel intensities. The pixels represent the real data as they are generated

according to the text. Thus the same pixels get repeated for the reoccurrences of a certain character. Thus it is also very important to select a proper cover image i.e. an image with high colour variation. This will generate a near uniform histogram thereby fooling the attacker try to carry out a histogram analysis attack.

8. Conclusion

Today, information exchange is the backbone of every field. The whole world is heavily dependent upon information exchange. Information may either be casual or confidential but in the wrong hands makes us vulnerable and exploitable. Some organizations may require to transfer huge amounts of texts securely. The encryption scheme is very effective in such kinds of situations. It not only encrypts the text but also uses offsetting and merging with another image which makes up for a 3-phase encryption. Huge amounts of textual data can be accommodated into a single image. Thus it provides compression also.

The scheme can be further improved further if colour images are used throughout the process. It will provide a greater range of intensity values thus increasing the complexity in extracting hidden data. The compression aspect of the scheme after adding colour image cover are left for future research.

References

[1] Rahulkrishna PK, Eshwari R, Shree Harsha NJ, Divyashree E & Gururaj C, "Enhanced Network Security Using Text to Image Encoding", *International Conference on Smart Sensors and Systems (IC-SSS)*, (2015).

[2] Stallings W, *Cryptography and Network Security Principles and Practice*, 5th Ed, Prentice Hall Publishers, (2011).

[3] Gonzalez RL & Woods RE, *Digital Image Processing*, 3rd Ed., Prentice Hall Publishers, (2006).

[4] Paul AJ & Nair LR, "Matrix based Substitution and Diffusion Procedure for Fast Image Encryption", *International Journal of Computer Applications*, Vol.80, No.3, (2013).

[5] Vidhu S & Dutt K, "Steganography: The Art of Hiding Text in Image using Matlab", *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol.4, No.9, (2014).

[6] Younes MAB & Jantan A, "A new steganography approach for images encryption exchange by using the least significant bit insertion", *International Journal of Computer Science and Network Security*, Vol.8, No.6, (2008), pp.247-257.

[7] EL-Emam. NN, "Embedding a Large Amount of Information Using High Secure Neural Based Steganography Algorithm", *International Journal of Computer, Electrical, Automation, Control and Information Engineering*, Vol.2, No: 11, (2008), pp.3806- 3817.

[8] Kumar A & Sharma R, "A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique", *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol.3, No.7, (2013), pp.363-372.

[9] Johnson NF & Jajodia S, "Exploring Steganography: Seeing the Unseen", *IEEE Computer*, Vol.31, No.2, (1998), pp.26-34.

[10] Thangadurai K, "An analysis of LSB based image steganography techniques", *IEEE International Conference Computer, Computer Communication and Informatics (ICCCI)*, (2014), pp.1-4

[11] Walia E, Jain P & Navdeep N, "An Analysis of LSB & DCT based Steganography", *Global Journal of Computer Science and Technology*, Vol.10, No.1, (2010), pp.4-8.

[12] Kavitha KK, Koshti A & Dunghav P, "Steganography using least significant bit algorithm", *International Journal of Engineering Research and Applications*, Vol.2, No.3, (2012), pp.338-341.

[13] http://searchsecurity.techtarget.com/

[14] http://sites.google.com/site/learnimagej/image-processing/what-is-a-digital-image/

[15] http://www.wikipedia.org/