Periodicals of Engineering and Natural Sciences ISSN 2303-4521
Vol. 8, No. 2, June 2020, pp.703-707

Hiding encrypted text in image steganography

Hassanain Raheem Kareem[1], Hadi Hussein Madhi [2], Keyan Abdul-Aziz Mutlaq[3]
[1] Mathematics Dep., College of Education, Misan University, hassanainraheem@uomisan.edu.iq
[2] College of Nursing, Misan University, hadihm8@uomisan.edu.iq
[3]Computer Center, Basra University, Basra, 61004, Iraq, keyan.alsibahi@uobasrah.edu.iq

Abstract

A mobile phone widely used nowadays and becomes more powerful than a computer for a few years. It can do the same function that a computer can do. Day after day the mobile phone has developed and become more important, but the confidential information remains to keep the challenge of security. This paper proposes a method for keeping the information by hiding text in an image. The proposed method increases randomization depending on the random key. It enhances security via encrypting the covered image with the key. The proposed method implemented by Java Platform Micro Edition (J2ME), since it supports a lot of APIs and features to mobile applications.

Keywords: Steganography, Cryptography, DES algorithm, 3DES algorithm, J2ME

Corresponding Author:

Hassanain Raheem Kareem
Mathematics Department, College of Education
Misan University
Misan, Iraq
E-mail: hassanainraheem@uomisan.edu.iq

1. Introduction

The digital information has an important feature which is creating and publishing unlimited numbers of their copies. So, the information will publish to public, then a problem of protecting them will be arise. There are several types of information like film, music, image, document and software. therefore, a big problem of working with these types of information [1]. A secure communication between two peers should be ensured, therefore there many ways are used for that purpose. Information hiding is used for preventing an intruder to detect them. Steganography is a technique which used to hide the information and send them to the sender with converted format. Mobiles can be used for exchanging the information without security, so it may be hacked. For providing privacy and protecting the information from persons who can hack them, steganography technique is used for embedding the information and hide its presence from an observer[2]. Another technique provides the security for the information which is cryptography. It keeps information over the network via converting the plaintext into cipher text. Several types of cryptography are used which are symmetric, asymmetric, and hashing. Cryptography algorithm uses the same key for encryption and decryption processes is called symmetric cryptography, while asymmetric cryptography uses different keys for encryption and decryption [3]. The objective of this research is to protect the information in the mobile, and this is done in two stages, in the first stage Steganography technique used to hide the information and send it, and in the second stage a proposed encryption algorithm to encrypt information.

2. Related work

Rahul Joshi, Lokesh Gagnani et. al introduce an important method of steganography and they emphases on digital images for reviewing the steganography. They explain that different requirements require different application for steganography technique[4]. Rahul Joshi, Lokesh Gagnani et. al introduce a discussion for method of Least Significant Bit. They declare the method replaces bits of secret message with Least Significant Bit of cover image [5]. Ge Huayong and Huang Mingsheng cover steganalysis and steganography principle and

concept, generalize embedding method of transform domain and spatial domain. They discuss image steganography and explain specification of its performance [6]. Shiladitya Pujari and Sripati Mukhopadhyay propose new method of image steganography based on dividing the secret image into units of characters equally, units' number is random. The cover image is segmented into squires with random number. Each squire hide its peer of message unit in fashion of pseudo-random[7]. Mohammad Shirali Shahreza presents a method of sending the information as hidden in a picture via password using website. The receiver must download the picture and use the password to extract its information. Site address sends via SMS to the receiver[8]. This paper proposes a method for hiding the information behind the image after compress it. It depends on a random key to enhancing the scattering of hiding information. Also, it implemented via J2ME which provides a lot of APIs to speed up the development process.

3. Material and methods

3.1 Triple data encryption standard (3DES)

It is an enhanced algorithm to DES and similar to it, but it operates thrice. There are some drawbacks of DES such as weak key, violated by Brute Force Attack, and small size of the key. These drawbacks are overcome via the 3DES algorithm. 3DES repeats the DES algorithm three times with triple keys. The keys are the same or different relay on the type.

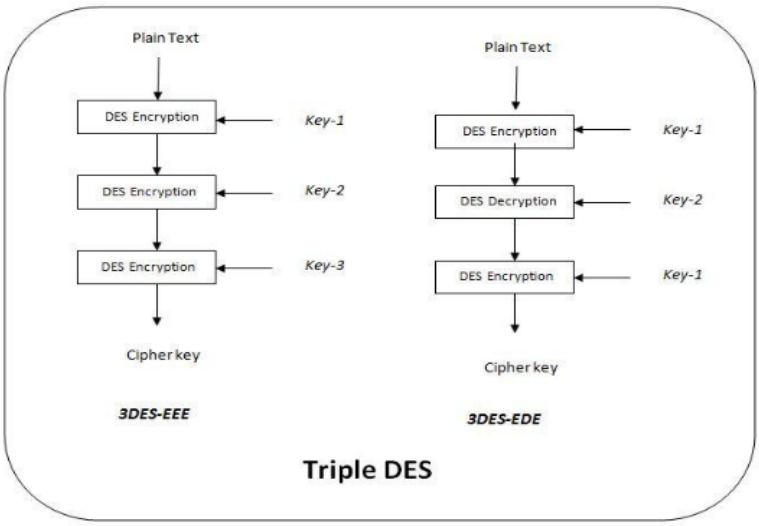

Figure1. flowchart of 3DES algorithm[9]

There are two types of 3DES such:

1- 3DES-EEE: encryptions of 3DES are working with different keys.
2- 3DES-EDE: it performs two encryptions and one decryption in-between. It uses two keys, first and third keys are same, with different key for second operation.

3.2 Proposed method

This paper states hiding a text behind an image via segmenting the image into block 8*8 bits. First of all, the image is compressed to decrement the data sent over the network. An estimation for measuring a signal to noise is used in this paper to specify the quality of the original image compared with the compressed image. The quality is delimited by a unique number called Peak Signal to Noise Ratio (PSNR). The original image represents the signal while the noise is an error obtains from the compression. The perception of humans is used as an approximation for quality comparing compression codec, so the reconstruction of the image may be the same for different compression. Higher PSNR acts in high quality. Then the proposed algorithm generates a random key that specifies the position of hiding text at image. The main idea of steganography is embedding data (text in this paper) into the image in order to provide s[9]ecurity to the message. The secret message can

be sent over the network without affright of violating the privacy of the message. The proposed method then encrypts the hiding data and image to increase security. A counter is used in this paper to count message length. Then check if there is text to be hidden in order to read and adjust all text in the message. Text bits are hidden by using XOR operation between text bit and image bit. The proposed method uses the key (generated previously) to specify a bit position in the image which is applied with text bit. In order to provide better security, the proposed encrypt the resulting image and the key via the 3DES algorithm. The following pseudo-code represents an algorithm of the proposed method:

STEP1: Load image after compression.
STEP2: Load the text to be hidden.
STEP3: Check if there is any text to read.
STEP4: Count the length of text.
STEP5: Generate random key has the same length as text.
STEP6: Hide text in image bit per bit via XOR operation their position is specified according to the key.
STEP7: Encrypt the key and resulting image using the 3DES algorithm.
STEP8: Send the key and resulting image to the receiver.

The recipient of the message must decrypt it via a 3DES algorithm then get the key and covered image. The key specifies the position of the bit which hides the information, XOR operation should be implemented between the original image and resulting image to obtain the original text. The original image is sent in another way to the recipient.

The proposed method is implemented via Java Platform Micro Edition (J2ME) which provides a set of APIs for developing applications suitable to Resource-Constrained devices such as mobile phones. It is used as runtime implementation which helps in the portability of code and increase of flexibility of mobile devices. It provides MIDlets which aims to deploy dedicated applications. J2ME is a set of configurations, each of them tailors to devise class, therefore it suitable to wide of devices. Configuration represents Virtual Machine and set of classes that aim for providing an environment of application programming. A profile completes the configuration by inserting classes to fund features convenient to a particular collection of devices. Two configurations are available in J2ME are CLDC (Connected Limited Device Configuration) and CDC (Connected Device Configuration). CDLC is specified to limited memory devices, instead, CDC is specified to resource-constrained, small devices like auto telematics. CLDC includes the collection of APIs fund features for devices of resource-constrained like mobile phone, therefore it is dependent on the proposed method. Mobile Information Device Profile (MIDP) used in this paper to provide a collection of Java libraries that provides the environment for creating applications in limited resources devices. MIDP is a package found in Java Archive (JAR) file.

4. Results

The two-color images with 256x256, 250x360 pixels is used for testing process, the images are Lena and Tree as in figure 2:

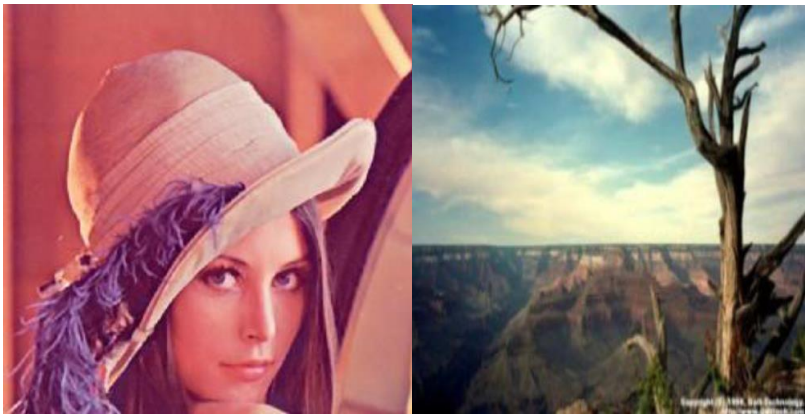

Figure 2. Lena image vs. tree image

To measure the performance between the two images the following factors are used in the proposed method to obtain the differences between the original image and stego image:
1- MSE: it gives the square of the error between stego and cover (original) image. The image distortion is indicated as an error. It is calculated mathematically by a 2D equation such:

$$\text{MSE} = \frac{1}{mn} \sum_{i=0}^{s-1} \sum_{j=0}^{r-1} st\_im(i,j) - co\_im(i,j) \quad (1)$$

Where s, r are st_im (stego image) size.
2- PSNR: it determines an image quality. It is calculated mathematically using the following equation:

$$\text{PSNR} = 10.\ (\frac{(value\ of\ graylevel)2}{MSE}) \quad (2)$$

3- NC: it specifies a similarity between stego image and cover image. It's determined by the following equation:

$$\text{NC} = \sum_{i=0}^{s-1} \sum_{j=0}^{r-1} st\_im(i,j) * co\_im(i,j) \ / \sum_{i=0}^{s-1} \sum_{j=0}^{r-1} (co\_im(i,j))2 \quad (3)$$

Table 1 : NC , PSNR and MSE Comparison

	Image	Pixels	NC	PSNR	MSE
1	Lena	256x256	1	52.0235	0.10024
2	Tree	360x250	1	55.0016	0.03602

5. Conclusions

The proposed method depends on XOR operation to hide the information, this leads to minimizing the number of processes. The processor implements its operation fast and easily. The proposed method depends on APIs for implementing the application, this saves the time of development and reliability of the application. The proposed method introduces two levels of security to enhance it, the first one is hiding the information, and the second is the encryption algorithm. It depends on the random key to hide the information; this leads to making the same information may hide in a different way for the same image. The covered image and key send after encryption while the original image sends by another technique (for user opinion), this increases the randomization of the security.

6. References

[1] S. Tayeb *et al.*, "Toward metadata removal to preserve privacy of social media users," in *2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)*, 2018: IEEE, pp. 287-293.

[2] A. Rai and S. Jain, "Modified RSA Cryptographic System with Two Public keys and Chinese Remainder Theorem," *International Journal of Computer Science and Engineering*, vol. 4, no. 7, 2017.

[3] T. K. Hazra and S. Bhattacharyya, "Image encryption by blockwise pixel shuffling using Modified Fisher Yates shuffle and pseudorandom permutations," in *2016 IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, 2016: IEEE, pp. 1-6.

[4] Y. Kang, F. Liu, C. Yang, X. Luo, and T. Zhang, "Color image steganalysis based on residuals of channel differences," *Comput. Mater. Continua*, vol. 59, no. 1, pp. 315-329, 2019.

[5] Y. Zhang, D. Ye, J. Gan, Z. Li, and Q. Cheng, "An image steganography algorithm based on quantization index modulation resisting scaling attacks and statistical detection," *Comput. Mater. Continua*, vol. 56, no. 1, pp. 151-167, 2018.

[6] B. Li, Z. Li, S. Zhou, S. Tan, and X. Zhang, "New steganalytic features for spatial image steganography based on derivative filters and threshold LBP operator," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 5, pp. 1242-1257, 2017.

[7] S. Pujari and S. Mukhopadhyay, "An Image based Steganography Scheme Implying Pseudo-Random Mapping of Text Segments to Logical Region of Cover Image using a New Block Mapping Function and Randomization Technique," *International Journal of Computer Applications,* vol. 50, no. 2, pp. 40-46, 2012.

[8] M. Kuri and T. Sarode, "Steganography Combined with RKO Technique for Visual Cryptography," *IJCAT International Journal of Computing and Technology,* vol. 1, no. 4, 2014.

[9] A. S. Raut, H. N. Shinde, S. R. Vidhale, R. V. Sawant, and V. A. Kotkar, "Enhancing Security using Location of Mobile Users."