

Hiding Secured key in digital media

Prof. Dr. Taleb A. S. Obaid¹, Assist. Prof. Dr. Mohammed J. Khami², Dr. Lemya Gh. Shehab³

¹: College of Computer Science and Information Technology, Basra University, Iraq. e-mail: tasobaid@g mail.com

²: Basra Technical Institute, Southern Technical University, Iraq. e-mail:mjkhami@yahoo.com,

³: Basra Technical Institute, Southern Technical University, Iraq.e-mail:Lemyaaldawood@yahoo.com

ABSTRACT

Sending encrypted message may be trigger hackers and crackers challenges to break and cover the original message to tampering with message and distorting its true meaning. Cipher experts have developed various techniques to overcome the weaknesses in traditional methods. To remedy such dangerous consequences for breaking and revealing the true messages, some different steganography technique should be implemented.

The subnational goal of the Cryptography approach to provides an actual fashion to store sensitive information and transmit this information through insecure communication networks so that it cannot be read and understood by any parties except the intended recipient.

In this work, we implement some conventional encryption techniques to hide the secured key and the cipher message in two different approaches. Firstly, we hid the secured encrypted key in a ciphertext message. Secondly, we used a colored image and monochrome image to hide a secured encrypted key and encrypted message using least significant bit (LSB) technique. In order to increase the communication security, we implemented these two different fashions and then retrieve encrypted secret key and encrypted message. Vigenère encryption technique had been used to encrypt the cipher message.

Keywords: hiding text, steganography, Vigenère technique, secured key.

.....
Date of Submission: 11-09-2017

Date of acceptance: 22-09-2017
.....

I. INTRODUCTION

Caesar cipher is a monoalphabetic cipher. It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter.

Given that RC4 cipher is widely used in the wireless communication and has some weaknesses in the security. Even before the advent of the computer, the exchange of information such as official letters, military information, it was well understood that some coding device was necessary to ensure secrecy of information from the enemy who might intercept messages. Caesar cipher is a monoalphabetic cipher. It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter. [1 - 4].

With the speedy progression of computer communication and a digital data exchange in electronically way. Information security policy is becoming much more important in data storage and transmission.

If you want to send a message to a specific person or partner and you do not want it to be understood by everyone else, may intercept that message. The message may be sent via the Internet such as your credit card number. Obviously, you do not want any intruder to discover it. So, the companies' responsibilities that do business on the Internet use very sophisticated coding systems to keep this information secret from intruders. The increase in using the electronic communication leads to more security needs on the exchange of the critical information. The field that concerns this problem is called cryptography (the science of writing secret codes), so, now a day's become more important to discuss this issue [3].

The encryption/decryption secured keys are central to cryptographic operations. A secured key is a piece of variable data that is fed as input into a cryptographic algorithm to perform encryption/decryption operation. In a well-designed cryptographic scheme, the security of the scheme depends only on the security of the keys used. The real challenge facing the security of communications is to hide the key to prevent the discovery of intruders on the Internet.

Steganography may be defined as the art and science of data hiding and makes data invisible by scrambling and hiding (or embedding) them in another piece of data, known alternatively as the cover, the host, or the carrier. There is a need to hide secret information inside certain types of digital data. Storing, hiding, or embedding secret information in all types of digital data is one of the tasks of the field of steganography. This

information can be used to prove copyright ownership, to identify attempts to tamper with sensitive data, and to embed annotations, for more details see[6 - 9]

Organizations should encrypt their data before transmission to guarantee that the data is safe during transmission. Usually, the data is sent over the public network should be encrypted; using appointed technique;and is decrypted by the intended recipient. Data encryption works by running the plain text through a special encryption key. Both the sender and the receiver should know this key which may be used to encrypt and decrypt the data as shown in figure (1).

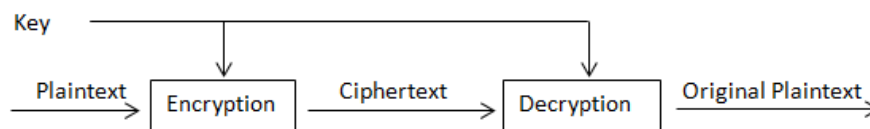


Figure 1: an encrypting system with a key.

Vigenère Cypher

The Vigenère cipher encrypts its inputs by using the key and the plaintext as indices into a fixed lookup table: the Vigenère square, each row in the square is derived from the row above by circularly shifting it one place to the left. Recovery of the plaintext from the ciphertext requires the key.

To encrypt, replicate the letters in the key so the key and plaintext are the same lengths. Then, drive each ciphertext letter by lookup in the Vigenère square: use the key letter as the row index and the plaintext letter as the column index. If the key **K** and the plaintext **P** are *n* letters long, form the ciphertext result **C** by indexing into the Vigenère square **V**, as follows:

$$C(n) = V(K(n), P(n))$$

Decryption simply reverses the process, using the key letter to determine the row index and the ciphertext letter to determine the column index, which is the plaintext letter [10 - 13].

Example (1):

Implement Vigenère technique to encrypt the given plaintext:

'COLLEGE OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY, DEPARTMENT OF COMPUTER INFORMATION SYSTEMS', and the key: 'COMPUTER SCIENCE'. The result of Matlab code is as in figure(2).

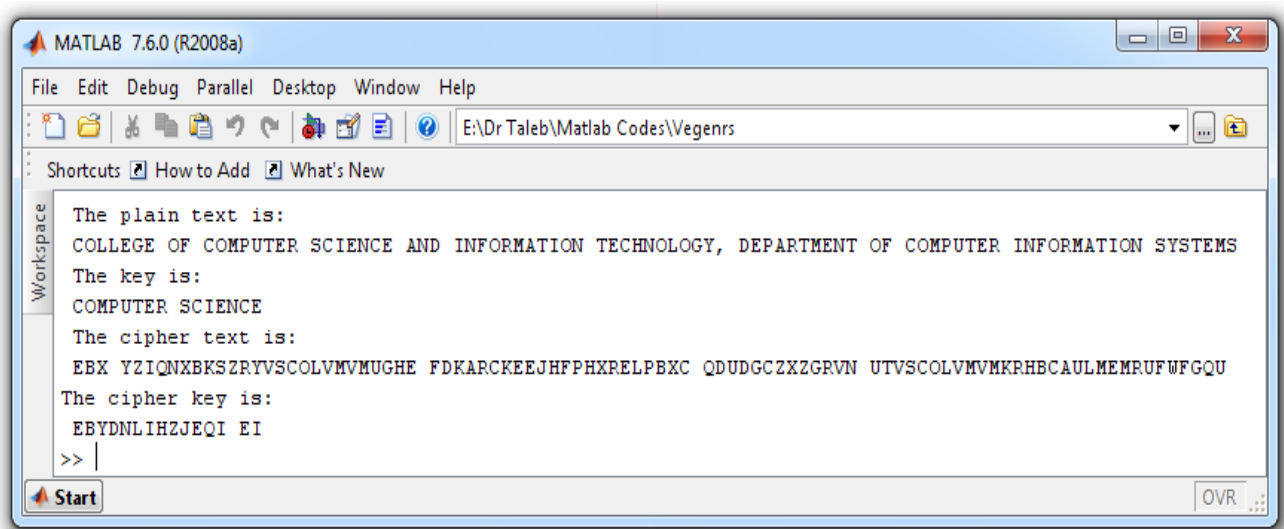


Figure (2), Implementation of encryption/decryption in Vigenère technique.

Hiding a secured Key in a text

The proposal work used new structure fashion to hide a secure key within a cipher message. The secret key may be embedded in the cipher message in the different fashions. These fashions may include; appending the key in the tail of the cipher message, the front of cipher message, in the first half only of the cipher message, in the second half, or in random locations... etc. In this work, the secret key is hidden in either character of

cipher message. However, let cipher message array P[], secured key array K[], and a new array N[] which represents an embedded key incipher message. The results of the processes are: $N[1]=P[1]$, $N[2]=K[1]$, $N[3]=P[2]$, $N[4]=K[2]$,... etc.

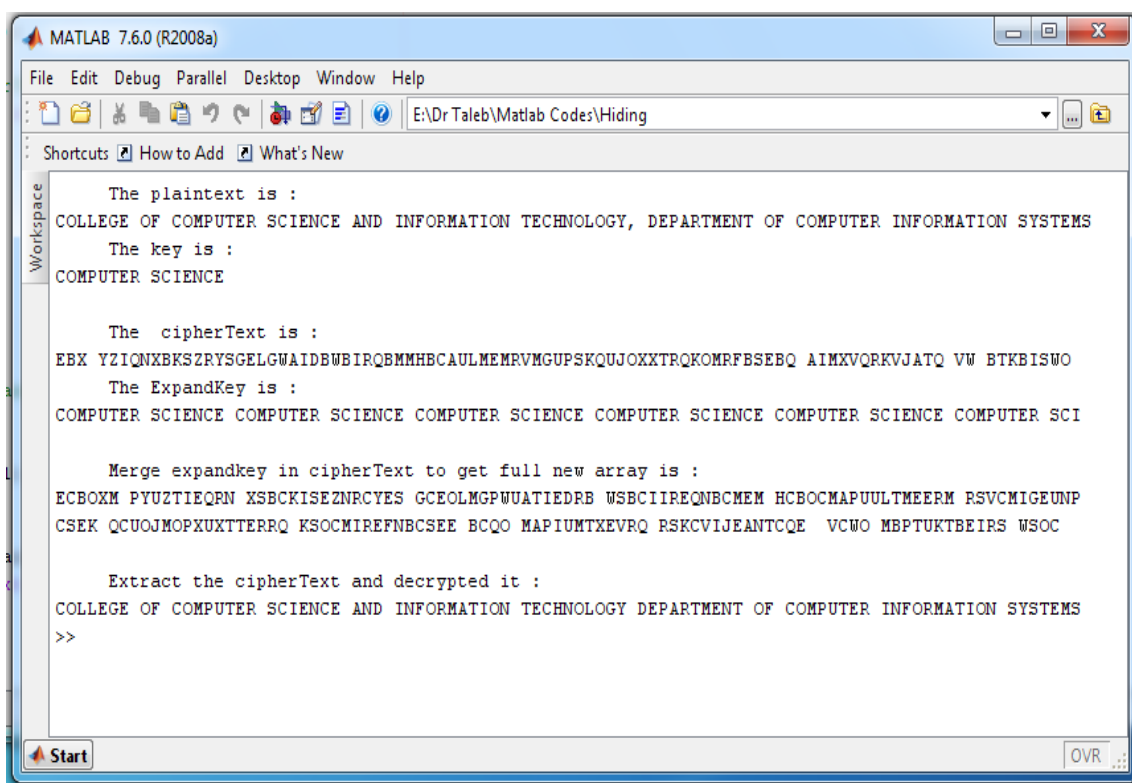
To implement the proposal technique, firstly extended the key length to be as a message length. As a result, the size of the new array will be doubled off the original message size. This approach will enhance the security of communication by hiding the key to decrepit the original message.

Example (2):

Hide a key ="COMPUTER SCIENCE ", in the message "COLLEGE OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY, DEPARTMENT OF COMPUTER INFORMATION SYSTEMS".

Solution:

We provide a secured key that intendant to be hidden in the required message. In our work, we called the Vigenère technique to encrypt the message. As mention previously we have to extend a secured given key and embedded in the cipher message in either location. The result of hiding secured key in the cipher message shown in the figure (3).



```
Workspace
The plaintext is :
COLLEGE OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY, DEPARTMENT OF COMPUTER INFORMATION SYSTEMS
The key is :
COMPUTER SCIENCE

The cipherText is :
EBX YZIQNBKSZRYSGELGWAIDBWBIRQBMMHBCAULMEMRVMGUPSKQJJOXTRQKOMRFBSEBQ AIMXVQRKVJATQ VW BTKBISWO
The ExpandKey is :
COMPUTER SCIENCE COMPUTER SCIENCE COMPUTER SCIENCE COMPUTER SCIENCE COMPUTER SCIENCE COMPUTER SCI

Merge expandkey in cipherText to get full new array is :
ECBOXM PYUZTIEQPN XSBCKISEZNRCEYES GCEOLMGPWUATIEDRB WSBCCIREQNBCMEM HCBOCMAPUULTMEERM RSVCMIGEUNP
CSEK QCUOJMOPXUXTTERRQ KSOCMIREFNBCSEE BCQO MAPIUMTXEVRQ RSKCVIJEANTCQE VCWO MBPTUKTBEIRS WSOC

Extract the cipherText and decrypted it :
COLLEGE OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY DEPARTMENT OF COMPUTER INFORMATION SYSTEMS
>>
```

Figure 3: Hide a secured key in the cipher message

Steganography

In general the researchers use image steganography, is the science of hiding data inside cover images for security. Images have a lot of visual redundancy in the sense that our eyes do not usually care about subtle changes in color in an image region. One can use this redundancy to hide text, audio or even image data inside cover images without making significant changes to the visual perception. Image steganography is becoming popular on the internet these days since a steganographic image, which just looks like any other image, attracts a lot less attention than an encrypted text and a secure channel. The goal of steganography is to transmit a message through some innocuous carrier such as (text, image, audio, and video) over a public communication channel where the existence of the message is buried. Steganography may define as the hiding of a secret message within an ordinary message and the extraction of it at its destination, [13], [14].

Least Significant Bit (LSB)

Least Significant Bit (LSB) steganography is a simple algorithm where higher bits of the color channels of hidden text/image (secret message) are stored in lower few bits of the color channels in the cover image. Image

files can hide secret message without their size being affected too much. It's called steganography, and it allows you to hide a secret message in images without anyone from knowing. In this method, the least significant bits of some or all of the bytes of an image may be changed with bits of the original message. The LSB embedding technique has become the basis of several techniques that hide a secret message within required media (text, images, video, and audio) carrier data. LSB embedding can also be implemented to a variety of data formats and types. However, LSB embedding is one of the most important steganography techniques in use today. To reflect the message it needs to be hidden, LSB replacement steganography flips the last bit of each of the data values. Consider an 8-bit grayscale bitmap image where each pixel is stored as a byte. And it also represented in a gray scale value, [15]. In our proposal, we used the two lowest bits of the covered image, i.e. the 8-bit and 7-bit, to hide the message and the secret key, respectively. Using the two lowest bits of an image required the size of both the message and a secret key are identical.

Example 3:

Hide the message: "COLLEGE OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY, DEPARTMENT OF COMPUTER INFORMATION SYSTEMS" and the secret key: 'COMPUTER SCIENCE', first in colored cover image figure (4, a), the obtained image is as shown in figure (4,b). And then hiding the same text message and key in mono color image figure (5, a), and the new modified mono color image is as in figure (5, b). The extracted text message and text of the used secret key are shown in figures (4), (5), and (6).

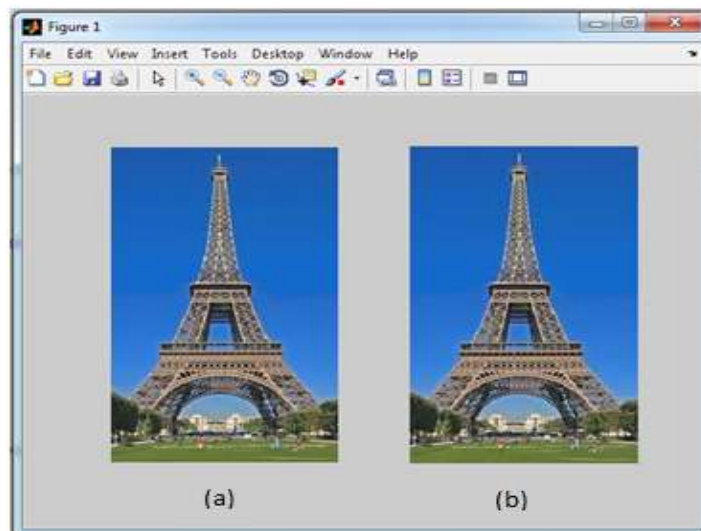


Figure (4): (a) The original cover color image, (b) the modified cover color image.

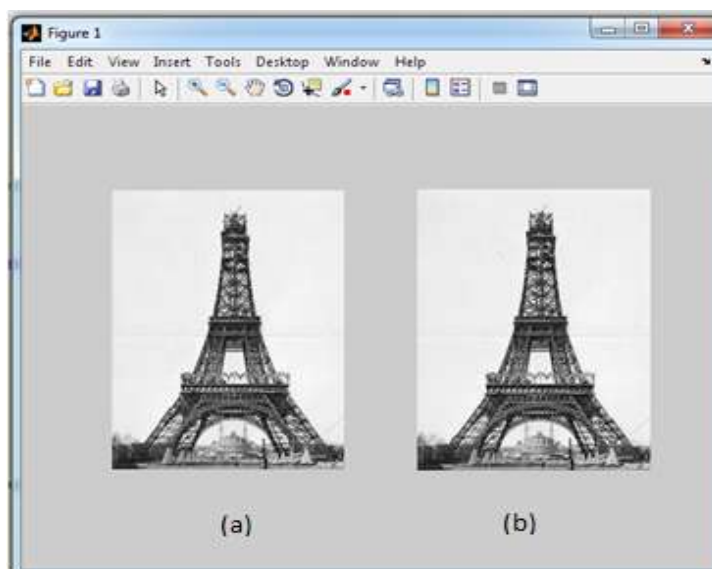


Figure (5): (a) The original mono cover image, (b) the modified mono color image.

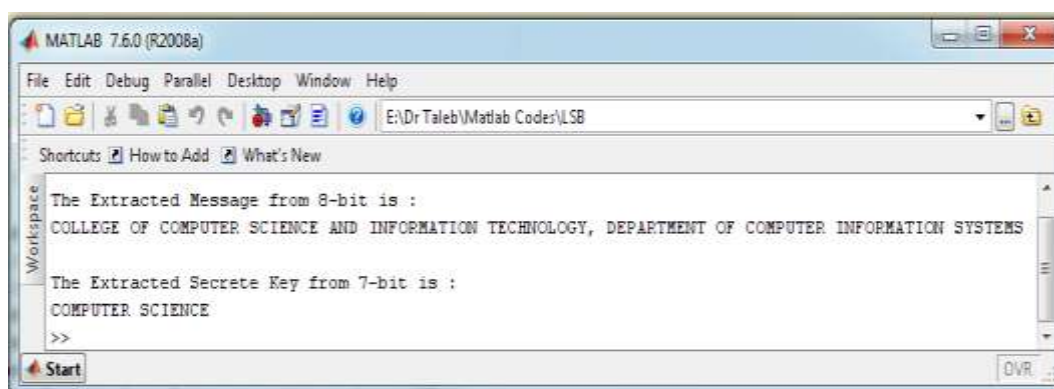


Figure (6): Extracted original text of the secret message and encrypting key.

II. CONCLUSION

The central to cryptographic operations are cryptographic keys. A key is a piece of variable data that is fed as input into a cryptographic algorithm to perform encryption/decryption operation. In a well-designed cryptographic scheme, the security of the scheme depends only on the security of the keys used.

The proposed approach in this work uses the secured key is embedded firstly in the text message and secondly in a covered image. The main intention of the project is to develop a steganography application that provides good security. The proposed approach provides good security and can protect the message from attacks through sending unsecured channels. The covered image resolution doesn't significantly change and may be negligible when we embed the message and the key into the covered image. So, it is not possible to damage the data by unauthorized personnel. We had used the Least Significant Bit algorithm in this work for developing the application which is faster and reliable and the compression ratio is moderate compared to other algorithms. The future work on this project is to improve the compression ratio. Although the Least Significant Bit Algorithm is easy and well secure, we can improve its performance to a certain extent by varying the carriers as well as using different keys at random bits for encryption and decryption.

REFERENCES

- [1]. Tonni Limbong, Parasian D.P. Silitonga, "Testing the Classic Caesar Cipher Cryptography using of Matlab", *International Journal of Engineering Research & Technology (IJERT)*, ISSN: 2278-0181, Vol. 6 Issue 02, 2017,
- [2]. Kashish Goyal, Supriya Kinger, "Modified Caesar Cipher for Better Security Enhancement", *International Journal of Computer Applications (0975 – 8887)*, Volume 73– No.3, July 2013
- [3]. Debnath Bhattacharyya, Asmita Haveliya, and Tai-hoon Kim, "Secure Data Hiding in Binary Text Document for Authentication", *Appl. Math. Inf. Sci.* 8, No. 1L, 371-378 (2014).
- [4]. Seifedine Kadry, Mohamad Smaili, "An Improvement of RC4 Cipher Using Vigenère Cipher", *International Journal of Computational Intelligence and Information Security* Vol. 1 No. 3, May 2010.
- [5]. Al Sweigart, "Hacking Secret, Ciphers with Python", 2013, ISBN 978-1482614374
- [6]. L. Y. Por, B. Delina, "Information Hiding: A New Approach In Text Steganography", 7th Wseas Int. Conf. On Applied Computer & Applied Computational Science (Acacos '08), Hangzhou, China, (2008)
- [7]. David Salomon "Data Privacy and Security: Encryption and Information Hiding" Springer Science & Business Media, May 20, 2003.
- [8]. Harshitha K M, Dr. P. A. Vijaya, "Secure Data Hiding Algorithm Using Encrypted Secret message ", *International Journal of Scientific and Research Publications*, Volume 2, Issue 6, June 2012, ISSN 2250-3153.
- [9]. L. Y. POR, B. Delina, "Information Hiding: A New Approach in Text Steganography", 7th WSEAS Int. Conf. on Applied Computer & Applied Computational Science (ACACOS '08), Hangzhou, China, April 6-8, 2008.
- [10]. Jean Mark Gawron, "Modular Arithmetic", San Diego State University, 2005, <http://www.rohan.sdsu.edu/~gawron>
- [11]. Mozghan Mokhtari, Hassan Naraghi, " Analysis and Design of Affine and Hill Cipher", *Journal of Mathematics Research* Vol. 4, No. 1; February 2012
- [12]. Thomas Baigneres, Pascal Junod, Yi Lu, Jea, "A Classical Introduction to Cryptography Exercise Book", Springer Science & Business Media. 2006

- [13]. VeenuArora, ,Raninderhillon, "Steganography– Information Hiding in Source Code Language "International Journal of Computer Science and Information Technologies, Vol. 4 (6), 2013, 826-829, ISSN: 0975-9646.
- [14]. Neha Gupta and Prof. Manoj Sharma, "An Approach to Hiding of Encrypted Text Information behind Word Document File ", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 11, November 2013, ISSN: 2277 128X
- [15]. Vanitha T,Anjalin D Souza, Rashmi B, SweetaDSouza, "A Review on Steganography – Least Significant Bit Algorithm and DiscreteWavelet Transform Algorithm", Int Jo of Innovative Research in Computer and Communication Engineering, Vol.2, Special Issue 5, October 2014

Prof. Dr. Taleb A. S. Obaid. "Hiding Secured key in digital media." International Journal of Engineering Research and Applications (IJERA), vol. 7, no. 9, 2017, pp. 58–63.