2-Leyer Security System for Hiding Sensitive Text Data on Personal Computers

Nouf A. Al-Otaibi
College of Computer & Information Systems, Umm Al-Qura University, Makkah, Saudi Arabia
Email: noof-awad@hotmil.com

Adnan A. Gutub
Custodian of the Two Holy Mosques Institute of the Hajj & Omrah Research, Umm Al-Qura University, Saudi Arabia
Email: aagutub@uqu.edu.sa

***Abstract*—High security system suitable to hide sensitive text-data on personal computer is proposed and implemented. The system hiding techniques involves AES cryptography followed by image based steganography as two layers to insure high security. The study involved several tests to increase the capacity within the steganography layer adopting 1 and 2 least significant bits stego methods. The study also explores the data dependency and its security effects by experimenting it on 30 different fixed size images showing interesting attractive results.**

***Index Terms*—security for personal computer, AES cryptography, image base steganography, hiding text on PC.**

I. Introduction

Hiding sensitive secret text within personal computers (PC) has privilege of the ability to utilize some of the PC available files to act as the cover media. Interestingly choosing among personal images can be assumed fully trusted confidential and only known by the PC user. This trust to hide within PC images played as real application behind image based steganography to secure sensitive text data. However, the security of the cover media, i.e. images on the PC, is based on the trust that the PC data cannot be penetrated by any means, which is difficult to assure and claim that the images are fully safe. This claim justified the need to add another security layer to insure that even for the very difficult security penetration; still the sensitive data are not harmed or used negatively. In other words, securing the data by steganography alone cannot be justified and completely relayed on, making the need to add another security layer [1]. We in this paper, present the 2-layer security system utilizing image base steganography as PC dependant layer as well as AES cryptography as independent assurance layer.

2-layers security system, i.e. cryptography layer and steganography layer are the main hiding techniques, used to insure full protection [2] of the sensitive information on a PC. Several sensitive text data examples can be expressed as clear application of our proposed system such as e-mail messages, credit card information, corporate data, etc. Steganography, as one of the layer's hiding techniques, is derived from "the Greek words stegos meaning "cover" and grafia meaning "writing" defining it as covered writing" [3]. Steganography, in general, uses any cover object of media types, i.e. text, image, audio and videos, to hide the secret data in it. After combining the secret with the cover object (making it PC dependant), the resulted file is known as the stego media.

Cryptography, as the other layer within this security system, is PC independent and completely deferent than steganography. Cryptography is mainly encrypting the secret plain text converting it to cipher text. Cryptography normally requires a secret key for the encryption/ decryption process to secure the sensitive data from the third party. In our security system, the sensitive text data passes through the crypto layer involving a security key, followed by the steganography layer resulting the output file as Stego-Image. Fig. 1 shows the main overview of the method using the two layer techniques [4].

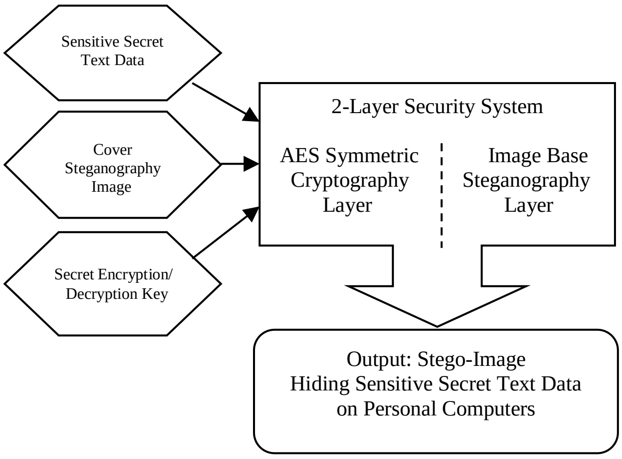

Sensitive Secret Text Data
Cover Steganography Image
Secret Encryption/ Decryption Key
2-Layer Security System
AES Symmetric Cryptography Layer
Image Base Steganography Layer
Output: Stego-Image Hiding Sensitive Secret Text Data on Personal Computers

Figure 1. Overview of the 2-leyer security system

In fact, steganography and cryptography are completely different [5]. In steganography, the sensitive text message is there, but nobody notices it or even aware that it exist [6]. However, once noticed, it can be read. Cryptography, on the other hand, is secret writing. Anybody can see the encrypted sensitive message, but

Manuscript received June 9, 2014; revised August 13, 2014.

doi: 10.12720/lnit.2.2.151-157

nobody else than intended ones can read it. Usually, crypto-methods works on the sensitive text letters to be re-arranged, or replaced by different letters, according to the specific scheme triggered by a secret key, that only the sender and receiver are familiar with [7].

In this paper we proposed and implemented the two layers technique, i.e. cryptography and steganography, to benefit from both and give the best possible security dedicated for PC applications . The cryptography layer is using the well known standard AES crypto algorithms. The steganography layer is adopting the image based steganography hiding the encrypted data in the least significant bit (LSB) and trying to improve it by increasing the LSBs [8].

The paper is organized as follows. The next section, Section 2, will give a background on related work or similar ideas where we are describing several methods utilizing image steganography with cryptography to secure information that are found suitable for PC data hiding. Section 3 presents our proposed 2-layer security system design and modeling issues, followed by a brief explanation of the implementation in Section 4. Section 5 gives a briefing of possible improvement in the capacity found suitable in the system stego layer to adopt 2LSB as well as 1LSB. Simple studies relating the security of the system and data dependency are presented in Section 6. We show different scenarios of fixing/changing the secret sensitive text and observing the security effect on different images observing interesting comparison results. Section 7 summarizes the work in the conclusion giving some ideas of related possible future work.

II. Related Work

Several methods are found in the literature suitable for PC security applications. Interestingly, we are focusing on the ones utilizing cryptography and steganography assumed suitable for PC security applications. For example, Vikas Tyagi in [1] is describing a method for integrating cryptography and steganography together through image processing. The work started by clarifying the way for encryption of the secret text before hiding it in the image. Then, the encrypted data is to be hidden in the image through the least significant bit (LSB) image based steganography. The paper did not describe the crypto algorithm used but showed advantage of practical implementation benefits with acceptable security. The research used random size of key that is flexible according to size of the data. This made the third party disability to predict the size of key and data easily.

Mehdi Hussain presents image steganography LSB technique in [7]. He used the well known method to hide data bits in an image by changing the LSB of each RGB image pixels color byte. The method described storing 3 bits in each pixel by changing LSB bit of the red, green, and blue color components, since every color is represented by a byte. The research showed real advantage of using LSB to hide secret data where the change in the pixels will have very low effect and unnoticed in observation.

Domenico in [9], proposed image steganography and cryptography system (ISC) for securing data transfer. He is using images as cover objects for steganography and secret key for the cryptography. The performance of the proposed Image-Based Steganography and Cryptography (ISC) system was presented in his work. He compared his results with another algorithm in the literature known as F5 showing improved results. It was found that the comparison with F5 is replacing the least-significant bit of a DCT coefficient with message data which may be degrading the fairness of the analysis. The work in [9] makes F5 decrements its absolute value in a process called matrix encoding claiming as a theoretically unbreakable cryptographic method based on image based one-time pad steganography.

Mohammad in [10] proposed a technique to implement steganography and cryptography together to hide the data into an image by two steps. The first step, finds the shared stego-key between the two communication parties by applying Diffie Hellman Key exchange protocol [10]. The second step makes the sender use the secret stego-key to select pixels that will be used to hide secret data. Each selected pixel will be used to hide 8 bits of data by using LSB method. Although the method showed real interesting security features, it was very complicated with high unpractical overhead.

Harshitha [11] proposed a security method in which the secret message is first encrypted and then hidden in cover file with steganography. The encryption of the message is randomly permuted using the secret key. The steganography used was based on the LSB algorithm for both embedding and extraction process. All the testing results showed interesting features generated by Matlab experimentations.

Shailender Gupta in [12] used two crypto techniques, i.e. Rivest Shamir Adleman (RSA) algorithm and Diffie Hellman algorithm, to encrypt the data. Then encrypted data is hidden using LSB steganography to insure acceptable security. The encrypted data as well as the image pixels are all considered in their binary form. The secret encrypted bits replace the least significant bit (LSB) within every pixel. The presented results showed comparison between using RSA and Diffie Hellman as crypto methods. Interestingly, it was reported that the use of encryption in steganalysis does not affect the time complexity when Diffie Hellman algorithm is used instead of RSA algorithm.

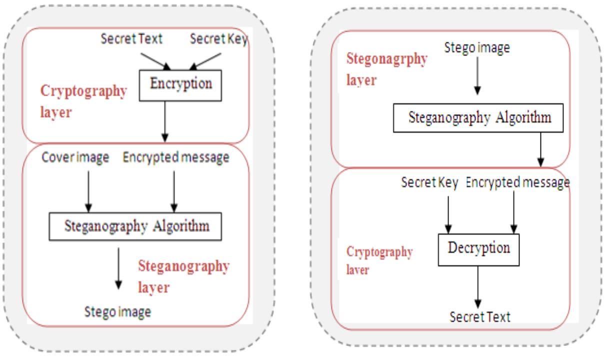
A last explored method for hiding encrypted secret message inside a cover file has been introduced by Joyshree Nath in [13]. He proposed an algorithm for encrypting the secret message with relation to the work proposed in [14]. The work modified the idea of play fair method into a new platform where they can encrypt or decrypt any file. Their method is dependent on the random text-key which is to be supplied by the user. They introduced a new randomization method for generating the randomized key matrix to encrypt plain text file and to decrypt cipher text file. They also introduced a new algorithm for encrypting the plain text multiple times increasing security by increasing system complexity.

All the above methods have been well thought-out to propose our 2-layer security system for hiding sensitive text data can be suitable for personal computers. Our method uses cryptography and steganography as two independent layers with all their security features [15]. The system added more studies relating the steganography layer to the PC images bits and the secret sensitive text data bits. Next sections will describe the design and implementation of our system and its comparisons in more depth.

III. The 2-Layer Security System Modeling

To insure high security suitable for PC applications, benefiting from the several methods introduced in Section 2 above, our proposed system utilizes both cryptography and steganography. In fact, cryptography and steganography are both exploited as separate layers to give the best possible security with independent security, capacity, and reliability measures and improvement adjustments.

The two-layers system can be observed as a process flow graph (Fig. 2) clarifying the storing point of view as well as the retrieving point of view. The cryptography layer is using the well known standard AES crypto algorithm, i.e. the sensitive text is going through the symmetric key encryption using Rijndael AES algorithm. The secret key used in encryption in the storing flow graph is needed as is in the decryption process when retreiving the data is desired. This AES key can be of several lengths, i.e. 128, 192 and 256 bits, which results in 10, 12 and 14 rounds of crypto layer operations, respectively. Our system data length is fixed to 128 bits.



Storing sensitive secret text data   Retrieving back secret text data

Figure 2. Process flow graph of the proposed 2-Layer security system

The crypto layer input as well as intermediate data can be considered as a matrix with four rows and four columns called states. Each element of the matrix is composed of eight bits. AES is based on a design principle known as a substitution-permutation network, combination of both Substitution and Combination, and is fast in both software and hardware as explained in [9].

The AES algorithm has four basic transformations, as observed in Fig. 3, described briefly as follows:

1). Sub Byte Transformation - a nonlinear transformation applied to the elements of the matrix. This first step in each round is a simple substitution.

2). Shift Rows Transformation - a cyclical shift operation with constant offsets, applied to the rows of the matrix

3). Mix Columns Transformation - the third step is a resource intensive transformation on the columns of state under which the four elements of each column are multiplied by a polynomial, essentially diffusing each element of the column over all four elements of that column.

4). Add Round Key Transformation - performs modulo 2 (XOR) operation with the round key, which is obtained from the initial key by a key expansion procedure. The encryption flow starts with the addition of the initial key to the plaintext. Then, the iteration continues for (Nr - 1) rounds (Nr being the total number of rounds). In last round, the Mix Column step is bypassed. AES can be understood in more depth in many resources such as [10].

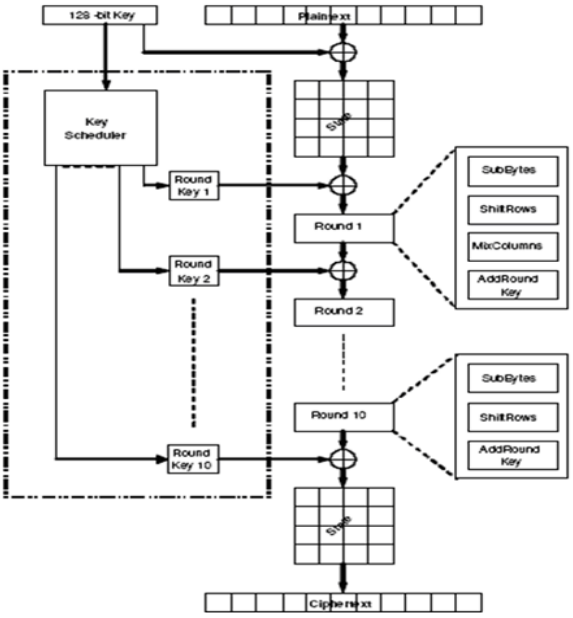


Figure 3. Block diagram of AES algorithm

The steganography layer in our system is adopting the image based steganography as in [1] hiding the encrypted data coming out of the cryptography layer in the. In fact, we improved the system capacity trying to increase the hidden bits in the image using several least significant bits (LSBs) instead of only one as will be clarified in the next section.

The main idea used in the image based steganography hiding in LSBs can be explained by an example of embedding the number 200. When the number 200, which is 11001000 in binary representation, is embedded into the least significant bits of the three pixels as part of the image, the resulting grid is as follows:

Pixel 1: 0010110**1**	0001110**1**	1101110**0**
Pixel 2: 1010011**0**	11000101	0000110**1**
Pixel 3: 1101001**0**	1010110**0**	01100011

Notice that the LSB of the last byte of Pixel 3 is not affected due to the completion of embedding all the secret bits in the image; so it is kept unchanged.

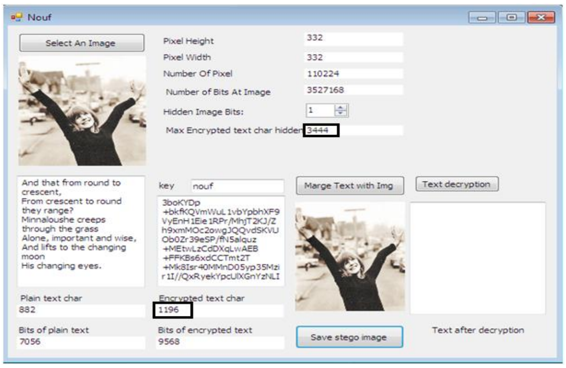
IV. The Security System Implementation

The 2-layer security system for hiding sensitive text data on personal computers is implemented on a visual basic programming platform. We used visual basic language Tenth Edition due to its flexibility, wideness spread, and easy to learn, such that any programmer can simply find it and redesign the system and verify our work. The aim of this implementation is to study the 2-layer security system idea in depth and to test different situations to enhance this important academic research field. The implementation is putting a target of helping security crypto designers and programmers to improve our system idea and make it practically usable. Another interesting feature found in our software platform, i.e. visual basic language tenth edition, is its availability of many libraries of pictures that can be taken as advantage of it in all testing experimentations.

Running the system implementation begins with the software asking for the secret sensitive text data message and the secret key, which is representing starting the operation of the crypto layer. Within this layer process, the program converts each character of the sensitive secret text into an array of binary bytes to be encrypted using AES. The second layer, i.e. steganography layer, also asks for an RGB image as cover media, such that its pixels are also converted into binary form. This stego layer can start its process at the same time while crypto layer is running, i.e. preparing the image as binary bits, but cannot start hiding data except after ciphertext is generated from the crypto layer. Each pixel within the RGB image has 3 channels, namely red, green and blue (RGB) representing a byte of 8 bits each. Therefore, using the least significant bits (LSB) image based steganography in our original system hides 3 bits in each pixel.

A. Hiding the Sensitive Data Example:

The implementation interface of the 2-layer security system presented is shown in Fig. 4. The interface shows the bits statistics that are generated and used by the crypto layer and the stego layer together. The process of hiding sensitive text starting by AES encryption followed by the image based steganography describes an example of hiding sensitive data in a picture as shown in Fig. 4.



Pixel Height 332
Pixel Width 332
Number Of Pixel 110224
Number of Bits At Image 3527168
Hidden Image Bits: 1
Max Encrypted text char hidden 3444

And that from round to crescent,
From crescent to round they range?
Minnaloushe creeps through the grass
Alone, important and wise,
And lifts to the changing moon
His changing eyes.

key nouf

```
3boKYDp
+bkfKQVmWuL1vbYpbhXF9
VyEnH1Eie1RPr/MhjT2KJ/Z
h9xmMOc2owgJQQvdSKVU
Ob0Zr39eSP/fN5alquz
+MEtwLzCdDXqLwAEB
+FFKBs6xdCCTmt2T
+Mk8Isr40MMnD05yp35Mzi
r1I//QxRyekYpcUlXGnYzNLI
```

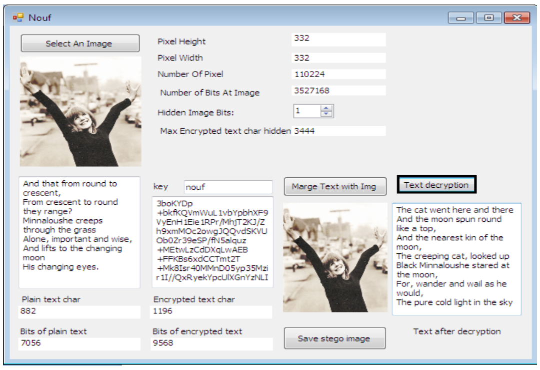
Plain text char 882
Encrypted text char 1196
Bits of plain text 7056
Bits of encrypted text 9568

Figure 4. The system interface showing bits statistics as well as the process of hiding sensitive text starting by AES encryption followed by the image based steganography.

The picture used as cover image has 332x332 pixels as its size. The implementation example [9] uses the sensitive secret text data message as the poem "The cat and the moon" for William B Yeats (1865-1939). The algorithm first encrypt the sensitive text data (the poem) with the secret key "nouf" and analyze the encrypted text bits against the "max encrypted text char hidden", which is dependent on the image based steganography LSB technique. The button "Marge text with img" cannot be active except if the image is able to hold all the encrypted bits. The output of hiding the sensitive data in the 2-layer system is imbedded into the cover stego image. This hiding process output stego image can be saved within the PC by clicking the button "save stego image".

B. Retrieving Back the Sensitive Data Example:

The interface shown in Fig. 5 can be used as an example of retrieving sensitive data that was hidden using the 2-layer security system. By pressing the button "Text decryption" the program will operate retrieving back the secret sensitive text data. It starts by sensing the LSBs within the stego image collecting the bits together forming the ciphertext. Generating the ciphertext is representing reversing the stego layer process. Then, the ciphertext is needs the secret key as inputs to the reverse crypto layer that decrypts the ciphertext generating back the secret sensitive data message, following Fig. 2 process of retrieving back secret text data.



Pixel Height 332
Pixel Width 332
Number Of Pixel 110224
Number of Bits At Image 3527168
Hidden Image Bits: 1
Max Encrypted text char hidden 3444

And that from round to crescent,
From crescent to round they range?
Minnaloushe creeps through the grass
Alone, important and wise,
And lifts to the changing moon
His changing eyes.

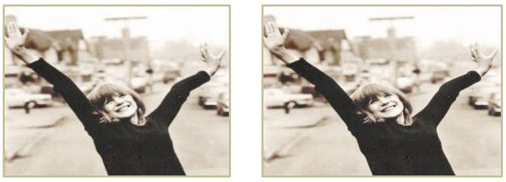
key nouf

```
3boKYDp
+bkfKQVmWuL1vbYpbhXF9
VyEnH1Eie1RPr/MhjT2KJ/Z
h9xmMOc2owgJQQvdSKVU
Ob0Zr39eSP/fN5alquz
+MEtwLzCdDXqLwAEB
+FFKBs6xdCCTmt2T
+Mk8Isr40MMnD05yp35Mzi
r1I//QxRyekYpcUlXGnYzNLI
```

The cat went here and there
And the moon spun round like a top,
And the nearest kin of the moon,
The creeping cat, looked up
Black Minnaloushe stared at the moon,
For, wander and wail as he would,
The pure cold light in the sky

Plain text char 882
Encrypted text char 1196
Bits of plain text 7056
Bits of encrypted text 9568

Figure 5. The retrieved sensitive data from the 2-layer system interface.



Original image Stego image

Figure 6. Image changes cannot be observed due to steganography

C. Compareson Between Original Image and Stego Image:

To check for the system security of the stego layer using 1LSB image based steganography, both original and stego images are observed as shown in Fig. 6. As observed in the example of Fig. 6, the different between the original image and the Stego image cannot be observed. It is so low such that no one can guess its usage in the information hiding process. The security is high because we just use the LSB in hiding information and the change in image is almost unnoticeable.

V. Capacity Improvement Study in the Steganography Layer of the System

To study improving the capacity within the second layer stego-images, i.e. when hiding the encrypted sensitive data within images, we tested a picture hiding bits within different Least Significant Bits (LSB), namely 1LSB, 2LSB, 3LSB, 4LSB, 5LSB, 6LSB, and 7LSB. These tests are considered differently from what is presented in [16] and [17], which can be in some relation to the improvement of experimentations in [18]. In fact, all our exploration analysis have been performed assuming changing the bits showing real interesting results (as shown in Fig. 7).

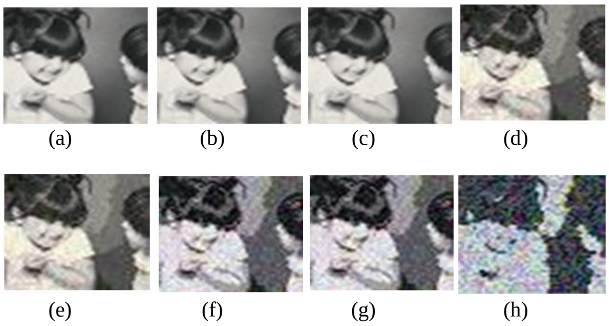


Figure 7. Capacity Improvement Study in Second Layer: a) Original Image, b) Stego-Image: 1LSB Changed, c) Stego-Image: 2LSB Changed, d) Stego-Image: 3LSB Changed, e) Stego-Image: 4LSB Changed, f) Stego-Image: 5LSB Changed, g) Stego-Image: 6LSB Changed, h) Stego-Image: 7LSB Changed

It can be noticed clearly that the change of 1LSB or 2LSB does not show difference while more than that, i.e. 3LSB, 4LSB, 5LSB, 6LSB, and 7LSB, are resulting in degrading the pictures quality and showing distortion. This capacity study made the steganography used in the second layer of our security system justified to focus on the possibility of changing the 1LSB and 2LSB only.

Our work used 2LSB image based steganography in the stego layer to increase the capacity of the hidden sensitive text. The capacity within the stego layer increased from 3 bits/pixel to 6 bits/pixel. Theoretically the study of the security did not depend on the observation alone, we made a detailed study testing the difference between 1LSB and 2LSB on the changed bits. Because this study depends heavily on the data bits values, 30 different pictures have been involved as detailed in the next section.

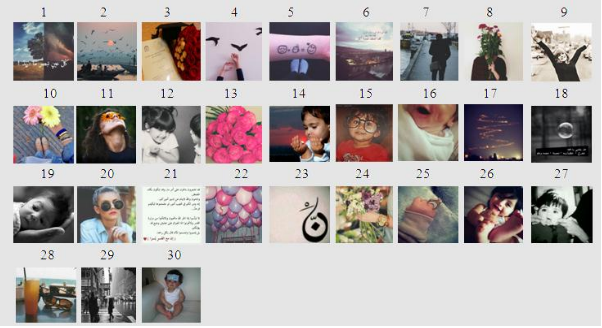


Figure 8. The fixed size 30 images used to study the system security and its relation to data dependency within the second layer image based steganography for 1LSB and 2LSB.

VI. System Security and Data Dependency Analysing 1LSB vs. 2LSB

The same secret sensitive text message, i.e. the poem "The cat and the moon", is used to be hidden on different pictures as first testing study. Then, the picture is fixed and the testing tries different secret sensitive text data.

A. Fixing Sensitive Secret Text-Data and Changing Stego-images:

In this test, we select 30 different PC images (Fig. 8) all within same size of 332x332 pixels to be used as cover images for the stego layer.

The test compares adopting the two acceptable least signification bit image based steganography, i.e. 1LSB and 2LSB. Using 1LSB for hiding the secret message of 7065 bits can hide 3444 character in the image of size 332 x 332.

Using the two least signification bit (2LSB) steganography as the stego layer capability increased the capacity of hiding information with acceptable security.

The security testing of fixing the sensitive text to be hidden and changing the pictures cover image resulted in changing the bits, i.e. 1LSB and 2LSB, based on the data used. This gives the real indication of the security of the system which can be dependant completely on the data available that cannot be expected, as shown in Fig. 9.

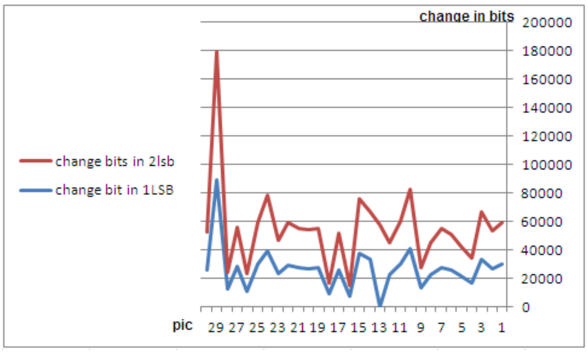


Figure 9. Number of bits changed within the 30 pictures due to hiding the sensitive text with the 2-layer system utilizing 1LSB and 2LSB.

The changed bits in Fig. 9 is comparing between using 1LSB and 2LSB for every image. Observe that the stego layer with 2LSB is always giving higher bits change compared to the 1LSB, which is expected.

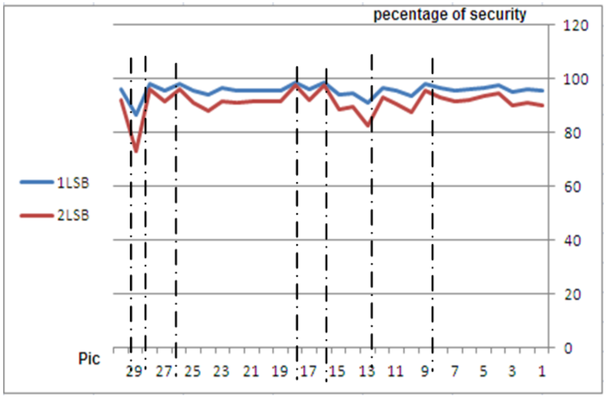


Figure 10. Percentage of security difference in the 30 pictures utilizing 1LSB and 2LSB in hiding the sensitive text with the 2-layer system.

We formalized the security difference percentage based on the bits changed within every image based on the 1LSB and 2LSB resulting the values shown in Figure 10. These results (Fig. 10) are based on the real security percentage and not subject to personal observations. Notes that Picture 29 is giving the lowest security percentage in both 1LSB and 2LSB techniques. However, several pictures, i.e. 9, 16, 18, 26, 28, are giving better percentage of security using 2LSB compared to pictures 13, 29 using 1LSB, which is completely unexpected. In other words, some pictures may be giving higher security as well as higher capacity when compared to others, which insists on running the hiding process on different pictures and then choosing the best suitable option.

B. Fixing Stego-Images and Changing Sensitive Secret Text-Data:

In this test, we use the picture number 9 from Fig. 8 but with smaller size 100 x 100 to test hiding within it two different sensitive secret messages: sensitive text-1 and sensitive text-2. Our 2-layer security system hided this text-1 and text-2 data both using the normal crypto layer technique and the steganography layer technique. However, the stego layer focuses on the previously described 2LSB steganography technique. The sensitive secret text data are:

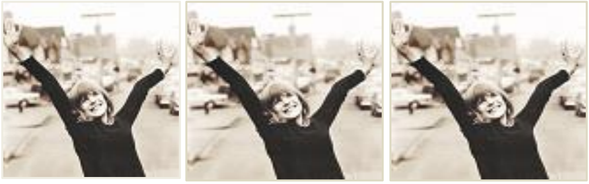
First one: (sensitive text-1): “The last prophet, Muhammad [peace be upon him] was born in Makkah on Monday, 12th Rabi al Awwal. He was born as an orphan. He was brought up by his grandfather. His uncle, Abu Talib, took care of him when he was eight years old. When he was ten or twelve years old, he used to look after the sheep around Makkah.

Muhammad was loving, kind, generous, helpful and honest man. He was an example of prefect character. He lived a very simple life. He was fair in his dealings with all people whether they are friends or enemies' .He was known as Al-Sadiq and Al-Amin.

He was injured by Quraish but he completed his duty. So, we must follow him and interrupt all people who try to deform something about his life. And what happen in Denmark nowadays is an example of this deed. We should face every person try to assault him; this is one of our duties towards him". This sensitive text-1 had 870 characters as plain text. When encrypted by the system crypto layer the ciphertext generated resulted in 1176 characters.

Second one: (sensitive text-2): “Most people who bother with the matter at all would admit that the English language is in a bad way, but it is generally assumed that we cannot by conscious action do anything about it. Our civilization is decadent and our language — so the argument runs — must inevitably share in the general collapse. It follows that any struggle against the abuse of language is a sentimental archaism, like preferring candles to electric light or hansom cabs to aeroplanes. Underneath this lies the half-conscious belief that language is a natural growth and not an instrument which we shape for our own purposes”. This sensitive text-2 had 601 characters as plain text. When encrypted as ciphertext resulted in 812 characters. Our 2-layer security system hides this text-1 data using 2LSB technique.

Picture 9 is chosen for this test because it gave the best percentage of security shown in Fig. 10. The two different sensitive texts have been hidden and the resulted output stego image is shown in Fig. 11. It has been notesd that both secret text data, i.e. sensitive text-1 and sensitive text-2 are not showing differences in the pictures. In fact, observing these pictures resulted that some PC images may give similar characteristics when different hiding secret texts, but this needs further exploration and theoretical study.



Original image Stego image text-1 Stego image text-2

Figure 11. Comparing original and stego-image within the 2-layer security system hiding the sensitive text-1 and the sensitive text-2

VII. CONCLUSION

In this work we have shown how to design 2-layer security system for hiding sensitive text data on personal computers. We used cryptography layer to insure PC independent security and stegonagraphy layer that is fully dependant on the PC data available. The system is implemented on visual basic platform showing interesting results. The system steganography layer embedded data in the image using several LSB attempts to enhance capacity without degrading security, which resulted in accepting the security of 1LSB and 2LSB methods. The system implementation tested the relation between the data to be secured and the cover images on the PC and its security effects by experimenting it on 30 different fixed size images showing interesting attractive results.

As future work, we want to improve the crypto layer by testing different other symmetric key algorithms as well as exploring the possibility of benefitting from asymmetric key cryptography. We plan studying different ways to improve the capacity and the security of the system for PC applications. We want to modify the method to make it supporting other languages like Arabic, which may need some more research.

ACKNOWLEDGMENTS

We would like to thank Umm Al-Qura University for supporting this research. Thanks to Shaqra University for giving the corresponding author: Nouf the opportunity to be teaching assistant and allowing her to continue MS at UQU - Makkah.

REFERENCES

[1] V. Tyagi, "Data hiding in image using least significant bit with cryptography," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 2, no. 4, pp. 120-123, April 2012.

[2] K. Patel, S. Vishwakarma, and H. Gupta, "Triple security of information using steganography and cryptography," *International Journal of Emerging Technology and Advanced Engineering*, vol. 3, no. 10, pp. 642-646, October 2013.

[3] K. Patel, S. Utareja, and H. Gupta, "A survey of information hiding techniques," *IJETAE*, vol. 3, no. 1, pp. 347-350, January 2013.

[4] D. Sarmah and N. Bajpai, "Proposed system for data hiding using cryptography and steganography," *International Journal of Computer Applications*, vol. 8, no. 9, pp. 7-10, October 2010.

[5] R. Mathe, V. Atukuri, and S. K. Devireddy, "Securing information: Cryptography and steganography," *IJCSIT*, vol. 3, no. 3, pp. 4251-4255, 2012.

[6] G. Vennice, Tv. Rao, M. Swapna, and J. Sasi kiran, "Hiding the text information using steganography," *International Journal of Engineering Research and Applications*, vol. 2, no. 1, pp. 126-131, Jan. 2012.

[7] M. Hussain and M. Hussain, "A survey of image steganography techniques," *International Journal of Advanced Science and Technology*, vol. 54, pp. 113-124, May 2013.

[8] Mrs. Kavitha, K. Kadam, A. Koshti, and P. Dunghav, "Steganography using least signicant bit algorithm," *International Journal of Engineering Research and Applications (IJERA)*, vol. 2, no. 3, pp. 338-341, May 2012.

[9] D. D. Bloisi and L. Iocchi, "Image based Steganography and Cryptography," *Computer Vision Theory and Applications*, vol. 1, pp. 127-134, 2007.

[10] V. Jain, L. Kumar, M. Sharma, M. Sadiq, and K. Rastogi, "Public-key steganography based on matching method," *Journal of Global Research in Computer Science*, vol. 3, no. 4, pp. 26-29, April 2012.

[11] K. M. Harshitha and P. A. Vijaya, "Secure data hiding algorithm using encrypted secret message," *IJSRP*, vol. 2, no. 6, June 2012.

[12] S. Gupta, A. Goyal, and B. Bhushan, "Information hiding using least significant bit steganography and cryptography," *I. J. Modern Education and Computer Science*, vol. 6, no. 1, pp. 27-34, June 2012.

[13] J. Nath and A. Nath, "Advanced steganography algorithm using encrypted secret message," *International Journal of Advanced Computer Science and Applications*, vol. 2, no. 3, pp. 19-24, March 2011.

[14] A. Nath, S. Ghosh, and M. A. Mallik, "Symmetric key cryptography using random key generator," in *Proc. International Conference on SAM-2010*, Las Vegas, USA, vol. 2, pp. 239-244, July12-15, 2010.

[15] C. Kommin, K. Ellanti, and S. Asadi, "Image based Secret communication using double compression," *International Journal of Computer Applications*, vol. 21, no. 7, pp. 6-9, May 2011.

[16] G. Kaur and A. Kochhar, "A steganography implementation based on LSB & DCT," *International Journal for Science and Emerging Technologies with Latest Trends*, vol. 4, no. 1, pp. 35-41, November 2012.

[17] M. Juneja and P. Sandhu, "An improved LSB based steganography technique for RGB color images," in *Proc. 2nd International Conference on Latest Computational Technologies*, June 2013, pp. 10-14.

[18] Deepali, "Steganography with data integrity," *International Journal of Computational Engineering Research*, vol. 2, no. 7, pp. 190-193, November 2012.

Nouf A. Al-Otaibi is currently a graduate student, pursuing Master of Sciences (MS) degree in Computer Sciences & Engineering, at Umm Al Qura University (UQU) fully sponsored by Shaqra University under the umbrella of Ministry of Higher Education. Her MS program at UQU is specialized in the information security track offered by the College of Computer and Information Systems offered at UQU-Makkah Campus, Saudi Arabia.

In 2010, Nouf completed her Bachelor of Sciences (BS) degree with honors from Taif University Saudi Arabia. Nouf followed her BS studies by pursuing a higher diploma degree in education also from Taif University completed by the end of 2011. She, then, worked as official trainers at the Saudi institute of Taif for around a year, i.e. until 2012, were she has been employed by Shaqra University as Graduate Teaching Assistant in the field of computing. At Shaqra, Nouf was assigned to teach introduction to computer science course classes as well as matlab classes based on her strong background and experience with programming languages such as matlab, java , c++ , php, and her outstanding ability to work with some databases like oracle and sql

Nouf research capability started by her BS graduation project about multimedia medical records in radiology department using techniques of expert systems. Then, in her MS studies at UQU, she worked on building a program that is reconstructing permutations from differences sequence, which was a project related to the graduate course of analysis of algorithms. She also worked as research assistant in an official project within UQU that involved different computing skills.

Nouf research interest focused lately on Computer and Information Security showing the ability to integrate cryptography, steganography, networks, artificial Intelligence, image processing, and expert systems, all from computer security point of view. She was motivated to build a high 2-level security system for hiding sensitive data in personal computers.

Prof. Adnan Abdul-Aziz Gutub is currently working as the Vice Dean of the Custodian of the Two Holy Mosques Institute of the Hajj & Omrah Research, within Umm Al Qura University (UQU), Makkah - Saudi Arabia.

Adnan is ranked as Professor in Computer Engineering specialized in Information and Computer Security within UQU. He received his Ph.D. degree (2002) in Electrical & Computer Engineering from Oregon State University, USA. He had his BS in Electrical Engineering and MS in Computer Engineering both from KFUPM, Saudi Arabia.

Adnan's research interests involved optimizing, modeling, simulating, and synthesizing VLSI hardware for crypto and security computer arithmetic operations. He worked on designing efficient integrated circuits for the Montgomery inverse computation in different finite fields. He has some work in modeling architectures for RSA and elliptic curve crypto operations. His current interest in computer security also involved steganography such as image based steganography and Arabic text steganography.

In summer 2013, Adnan has been awarded 3-month visiting scholar grant in collaboration with Purdue University, West Lafayette, Indiana, USA. Previously, Adnan have been twice awarded the UK visiting internship for 2 months of summer 2005 (at Brunel University) and summer 2008 (at University of Southampton), both sponsored by the British Council in Saudi Arabia. He had been involved in research of current studies related to Arabic Text Steganography in Data Security as well as Elliptic Curve Crypto Processor Designs.

Administratively, Adnan Gutub filled many executive and managerial academic positions at KFUPM as well as UQU. At KFUPM - Dhahran, he had the experience of chairing the Computer Engineering department (COE) for five years until moving to Makkah in 2010. Then, at UQU - Makkah, Adnan Chaired the Information Systems Department at the College of Computer & Information Systems followed by his leadership of the Center of Research Excellence in Hajj and Omrah (HajjCoRE) serving as HajjCoRE director for around 3-years until the end of 2013. Then, he was assigned his current position as the Vice Dean of HRI, i.e. the Custodian of the Two Holy Mosques Institute of the Hajj & Omrah Research.