

Flexible Stego-System for Hiding Text in Images of Personal Computers Based on User Security Priority

Nouf A. Al-Otaibi¹, and Adnan A. Gutub²

¹ Collage of Computer & Information Systems, Umm Al-Qura University, Makkah, Saudi Arabia
Email: noof-awad@hotmail.com

² Custodian of the Two Holy Mosques Institute of the Hajj & Omrah Research,
Umm Al-Qura University, Saudi Arabia
Email: aagutub@uqu.edu.sa

Abstract: Flexible security system suitable to hide sensitive text-data on personal computer (PC) is proposed and implemented. The system provides security information to the user to select the cover-image within the PC based on his/her security priority. The technique flexibility allows the user to test several images to hide the same text within. Then, the user chooses one image to be used as cover image based on his selection knowing the security priority needed.

The system uses normal image based steganography replacing the pixel least significant bit with text-hidden. The study explores the data dependency and its security effects by experimenting 30 different fixed size images showing interesting attractive results.

Keywords: security for personal computer, image base steganography, hiding text on PC, user security priority

1. Introduction

Securing sensitive text to be hidden within images of personal computers (PC) has advantage of the ability to utilize some of the PC available pictures to act as the cover media. Interestingly choosing among personal images can be assumed fully confidential and only known by the PC user [1]. This security action 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. pictures on the PC, is based on the fact that the PC data cannot be penetrated easily by normal means [2]. We in this paper, present a flexible security system. The system is utilizing image base steganography hiding the text in several images, showing the security affect within all, then, allowing the user to priorities among the images and select preference.

The least significant bit steganography technique is the main hiding method used to insure protection [3] of the sensitive information on 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 [4], in general, can use any cover object of media types, i.e. text, image, audio and videos, to hide the sensitive data in it. After combining the secret with the cover object (making it PC dependant), the resulted file is known as the stego-media as shown in Figure 1.

In this paper we proposed and implemented a flexible security technique to benefit from testing hiding the text on several cover-images allowing the user to select the his/her security choice dedicated for certain PC application, i.e. depending on the security results given to the user for selection of image. The steganography system is adopting the normal image based steganography hiding the encrypted data in the least significant bit (LSB) [5,6].

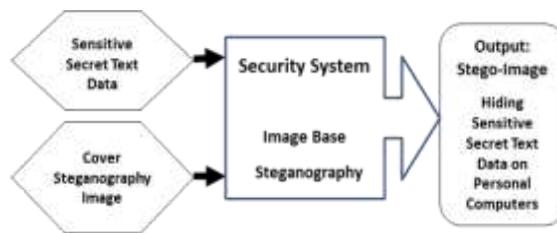


Fig. 1: Overview of normal steganography security system

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 to secure information that are found suitable for PC data hiding. Section 3 presents our proposed flexible security system design and modeling issues, followed by a brief explanation of the implementation in Section 4. Section 5 gives details of the relation of system security priority and data dependency stressing on the benefit of this work showing different images observing interesting comparison results. Section 6 summarizes the work in the conclusion giving some ideas of related possible future work.

2. Related Work

Several methods are found in the literature suitable for PC security applications. Interestingly, we are focusing on the ones utilizing steganography assumed suitable for PC security applications. For example, Vikas Tyagi in [2] is describing a method of steganography through image processing. The work shows hiding the data in the image through the least significant bit (LSB) image based steganography. The paper did not give details of the utilizing the algorithms used but showed advantage of practical implementation benefiting acceptable security. The research used random sized numbers for hiding flexible according to the size of the data. This made the third party disability to predict the size of data easily.

Mehdi Hussain presents image steganography LSB technique in [5]. 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 [7], proposed image steganography combined with 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 [7] 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 [8] proposed a technique to implement steganography but with secret keys 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 [8]. 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 [9] proposed a security method relaying somewhat on steganography 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 [10] used securing methods involving LSB steganography assuming resulting acceptable security. The image pixels are all considered in their binary form and the secret bits replace the least significant bit (LSB) within every pixel. The presented results showed comparison to other methods reporting that steganalysis does not affect the time complexity for certain security improvements.

A last explored method for hiding secret data inside a cover file has been introduced by Joyshree Nath in [11]. He proposed an algorithm used for the secret text in relation to the work proposed in [12]. The work modified the idea of play fair method into a new platform where it 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. They also introduced securing the text multiple times by increasing the system complexity.

Several different other research papers, i.e. [13], [14], [15], [16], and [17] have also been thought-out with the methods discussed above to gather required knowledge to propose our flexible security system for hiding sensitive text data suitable for personal computers relaying on the user to select the cover-image within PC based on his/her security priority. The user chooses one image to be used as cover image based on his selection after testing several images knowing the security priority needed. The study investigated the data dependency and its security effects on 30 different fixed size images showing interesting attractive results making the method suitable to be generalized. Next sections will describe the design and implementation of our system and its comparisons in more depth.

3. Flexible System Modeling and Security Priority

To insure high security suitable for PC applications, benefiting from the several methods introduced in Section 2 above, our proposed system utilizes steganography but allowing the user to be of full control.

The system can be observed as image based steganography as in [2] hiding the data but trying to give the user more choice based on security priority that is fully subjective to the data available [1]. 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:	00101101	00011101	11011100
Pixel 2:	10100110	11000101	00001101
Pixel 3:	11010010	10101100	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 resulting in security improvement, which is considered tangible in the security priority given to the user. In fact, the bits changed are the ones degrading the security of the system, i.e. if the number of bits changed are found more, the security is degraded more, which is completely dependent on the images pixels as well as the secret data to be hidden. This flexibility feature is giving the user the security priority to choose the appropriate image as stego-image.

4. The Security System Implementation

The flexible 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 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 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 cover image, which is representing starting the operation of the steganography security system. It asks for the RGB image as cover media, such that its pixels are also converted into binary form. This method is preparing the image as binary bits and start hiding the data. 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 system hides 3 bits in each pixel.

The implementation interface of the flexible security system presented is shown in Figure 2 as an example. The picture used as cover image has 332x332 pixels as its size. The implementation example [7] assumes the sensitive secret text data as the poem “The cat and the moon” for William B Yeats (1865-1939). The algorithm

sensitive text data (the poem) is embedded in the cover-image using LSB image based steganography. 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 system is imbedded into the cover stego image resulting the number of bits different, which is the number of LSB changed due to the hiding process. This number is provided testing 30 different figures (Figure 3) showing each picture with the number of bits changed due to hiding the text, as listed in Table 1.



Fig. 2: The system interface showing bits statistics as well as the process of hiding sensitive text by the image based steganography.

The user then chooses which cover image to hide in based on his selection as of the security priority needed. The hiding process output stego-image can be saved within the PC by clicking the button “save stego image”.

TABLE I: The number of bits from different testing’s hiding sensitive text in the 30 fixed size images

pic	Number of Bits Different	pic	Number of Bits Different
1	29815	16	7749
2	26533	17	26096
3	33489	18	9222
4	17086	19	27502
5	21409	20	27149
6	25637	21	27656
7	27421	22	29447
8	22656	23	23343
9	13747	24	39382
10	41327	25	29820
11	30186	26	11169
12	22396	27	28081
13	57930	28	12339
14	33535	29	89512
15	37988	30	26230

5. User Security Priority and Data Dependency Analysis

The same secret sensitive text message, i.e. the poem “The cat and the moon”, is used to be hidden within the 30 different pictures, as introduced in the section before. We selected 30 different PC images (Figure 3) all within same size of 332x332 pixels assuming them all to be used as possible cover images, but with different security priorities.

The security testing study of fixing the sensitive text to be hidden in the pictures cover image resulted in the number of bits changed (listed above in Table 1) involved in the computation of percentage of security per image as the formula:

Percentage of security per stego-image = $(100 \times \text{Number of pixels} \times 3 - \text{number of bits changed}) / (\text{Number of pixels} \times 3)$

Note that the number of pixels is multiplied by 3 (in the formula above) due to the possibility of hiding sensitive data bits within the LSB of all 3-channels of the RGB pixels as clarified in Section 3 before.

In our study, the total number of pixels is fixed in all images as $332 \times 332 = 110224$; resulting the maximum possible number of bits that can be hidden as $332 \times 332 \times 3 = 110224 \times 3 = 330672$. Based on the bits changed after hiding the sensitive data, the formalization of the security difference percentage within every possible stego-image resulted in the values shown in Figure 4.

It is to be noted from Figure 4, that the real indication of the security of the system is completely dependent on the data and images available within the PC and cannot be expected nor predicted. These results (Figure 4) are based on the real security percentage computed and not subject to personal observations. Observe that Pictures: 29, 13, 10, 24 are giving the low security percentage. However, several pictures are giving acceptable percentages of security as in order (starting from the highest): 16, 18, 26, 28, 9.

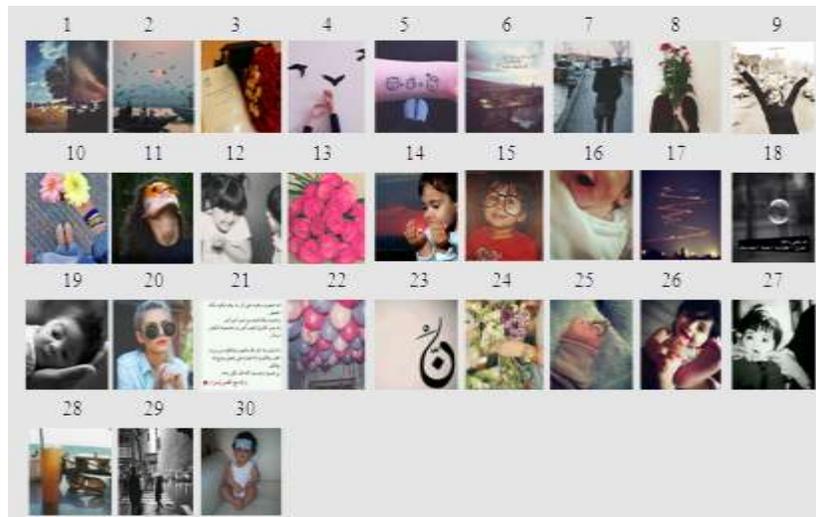


Fig. 3: The fixed size 30 images used to study the system security in relation to data dependency within the LSB image based steganography.

In other words, some pictures may be giving higher security when compared to others, which insists on our idea of allowing the user to benefit from this flexibility and run the hiding process on different pictures, giving the user full control to be choosing the appropriate suitable option.

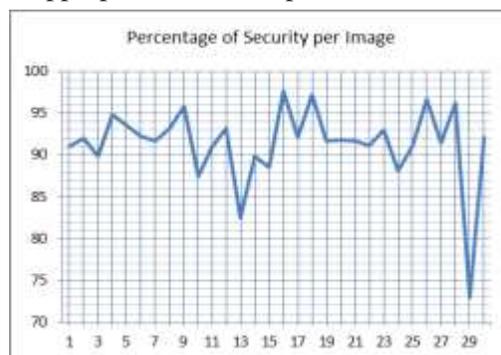


Fig. 4: Percentage of security based on the number of bits changed within the 30 fixed size pictures used in the tests due to hiding the same exact sensitive text.

6. Conclusion

In this work we have shown how to design flexible security system for hiding sensitive text data on personal computers with user security priority. We used image based steganography that is fully dependant on the PC data available to insure full control of the security of the system to be given to the user.

The flexible security system is implemented on visual basic platform showing interesting results. The system steganography embedded the same data in different images stressing on the flexibility given to the PC user to choose his prioritized security. The real benefit from this work is in allowing the user to be given the chance to observe the security degradation level of his sensitive data when embedded on different images. The system implementation explored 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 flexible security system by studying different other advanced ways to improve the hiding techniques within 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. Also, we want to try the same flexibility assuming different other cover media for steganography. We plan to look into hiding different data types in different cover media types, i.e. Audio, Video and Text, with the same features of giving the user opportunity for choosing among security priority.

7. Acknowledgments

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

8. References

- [1] N. Al-Otaibi and A. Gutub, "2-Layer Security System for Hiding Sensitive Text Data on Personal Computers", Lecture Notes on Information Theory, Engineering and Technology Publishing, vol. 2, no. 2, pp. 151-157, June 2014.
- [2] 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.
- [3] 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.
- [4] K. Patel, S. Utareja, and H. Gupta, "A Survey of Information Hiding Techniques ", IJETAE, vol. 3, no. 1, pp. 347-350, January 2013.
- [5] Mehdi Hussain and Mureed Hussain, "A Survey of Image Steganography Techniques", International Journal of Advanced Science and Technology , vol. 54, pp. 113-124, May 2013.
- [6] Mrs. Kavitha, Kavita Kadam, Ashwini Koshti, and Priya Dunghav, "Steganography Using Least Significant Bit Algorithm", International Journal of Engineering Research and Applications (IJERA), vol. 2, no. 3, pp. 338-341, May 2012.
- [7] Domenico Daniele Bloisi and Luca Iocchi, "Image based Steganography and Cryptography", Computer Vision theory and applications, vol. 1, pp. 127-134, 2007.
- [8] 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.
- [9] K. M. Harshitha and P. A. Vijaya, "Secure Data Hiding Algorithm Using Encrypted Secret message", IJSRP, vol. 2, no. 6, June 2012.
- [10] 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.
<http://dx.doi.org/10.5815/ijmecs.2012.06.04>
- [11] 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.
<http://dx.doi.org/10.14569/IJACSA.2011.020304>
- [12] A. Nath, S. Ghosh, and M.A. Mallik, "Symmetric key cryptography using random key generator", Proceedings of International conference on SAM-2010, Las Vegas (USA), vol. 2, pp. 239-244, 12-15 July 2010.

- [13] M. T. Parvez and A. Gutub, "Vibrant Color Image Steganography using Channel Differences and Secret Data Distribution", *Kuwait Journal of Science and Engineering (KJSE)*, Vol. 38, No. 1B, Pages: 127-142, June 2011.
- [14] W. Abu-Marie, A. Gutub, and H. Abu-Mansour, "Image Based Steganography Using Truth Table Based and Determinate Array on RGB Indicator", *International Journal of Signal and Image Processing (IJSIP)*, Vol. 1, No. 3, Pages: 196-204, May 2010.
- [15] A. Gutub, "Pixel Indicator Technique for RGB Image Steganography", *Journal of Emerging Technologies in Web Intelligence (JETWI)*, Vol. 2, No. 1, Pages: 56-64, February 2010.
<http://dx.doi.org/10.4304/jetwi.2.1.56-64>
- [16] A. Gutub and F. Khan, "Hybrid Crypto Hardware Utilizing Symmetric-Key & Public-Key Cryptosystems", *International Conference on Advanced Computer Science Applications and Technologies – ACSAT2012*, Palace of the Golden Horses, Kuala Lumpur, Malaysia, 26–28 November 2012.
- [17] A. Gutub, A. Al-Qahtani, and A. Tabakh, "Triple-A: Secure RGB Image Steganography Based on Randomization", *AICCSA-2009 - The 7thACS/IEEE International Conference on Computer Systems and Applications*, Pages: 400-403, Rabat, Morocco, 10-13 May 2009.

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, where 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. His experience was gained from his previous long-time work in Computer Engineering at King Fahd University of Petroleum and Minerals (KFUPM) in Dhahran, Saudi Arabia. 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. 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. Previously, Adnan have been twice awarded the UK visiting internship for 2 months of summer 2005 and summer 2008, both sponsored by the British Council in Saudi Arabia. The 2005 summer research visit was at Brunel University to collaborate with the Bio-Inspired Intelligent System (BIIS) research group in a project to speed-up a scalable modular inversion hardware architecture. The 2008 visit was at University of Southampton with the Pervasive Systems Centre (PSC) for research related to text steganography and data security.

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.