Enhancing Security of Transmitted Data by Improved Steganography Method

Abdullah M Basahel
Department of MIS
Faculty of Economics and Administration
King Abdulaziz University
Jeddah, Saudi Arabia

Mohammad Yamin
Department of MIS
Faculty of Economics and Administration
King Abdulaziz University
Jeddah, Saudi Arabia

Adnan Ahmed Abi Sen
College of Computer and
Information Technology
King Abdulaziz University
Jeddah, Saudi Arabia

Summary
The great developments in the world of communications and the advancement of the associated technologies, such as the Internet of Things (IoT) with web-based and mobile applications, have changed our way of life. This has created a kind of linkage between virtual and real worlds, rendering applications and services to be ubiquitous. We are also witnessing a phenomenon in which the electronic devices that connect to the Internet and are widespread making use of technology and providing a better level of service to users. However, sending and receiving information over the Internet generates many issues and problems. The most serious of them is the security and protection of transmitted information. This issue has become one of the most important things which is a matter of concern to researchers as well as the users themselves. Ensuring privacy and security of the transmitted data is a matter of urgency and cannot be neglected while dealing with the transmission of data using the services and tools in the IoT. In this article, we provide an improved algorithm to increase the protection level of transmitted information by means of cryptographic encryption so that this information cannot be seen by others or disclosed to anybody. This algorithm has been evolved as an application that works on mobile phones so that any user can benefit from it when exchanging sensitive and confidential information such as account numbers and passwords with other users.

Key words:
Steganography, DES, LSB, Security, Privacy

1. Introduction

The aim of this research paper is to announce and present an improved algorithm to increase the protection level of transmitted information by means of encryption. With the help of this algorithm, the transmitted information cannot be breached. Moreover, no sense can be gathered from the transmitted information in case it was disclosed to others. We have formulated this algorithm as an application for mobile phones so that any user can benefit from it when exchanging sensitive and confidential information such as account numbers and passwords to other users.

The issues surrounding information security are not new. These issues have persisted in all times and have engaged scientists and researchers in the quest of protecting the privacy and security of information regardless of its form. These issues will continue to remain and are expected to persist over the years as the tendency to protect confidential information and privacy are inherent for everyone [1-2]. With the development of computer science and the complexity of the underlying fields and invasion of information in all areas of life, researchers had to work in tandem with the development of this science to this era, when it has become the need to ensure security and confidentiality. The integration of information has led to the disclosure of secrets causing damage and heavy losses to individuals and companies [3-4]. This is where cryptography has stepped in and has become one of the most important branches for dealing with information security. This helps in communicating the required confidential and sensitive information, without raising any kind of doubts. The user of this type of science can send digital files (text, audio or visual ...) [5-7] on to the other parties without giving a clue to others that it contains very personal, secrete and sensitive information. Thus, the science of steganography has provided a wonderful solution based on circumventing some of the senses of the human being to send what they would want in a gentle, smooth and isolated manner. In addition, the coding techniques and skills are adequate to prevent attacks even if attackers acquire transmitted communication or information in the form of a picture by discovering or having direct access to this information [8-9].

Manuscript received April 5, 2019
Manuscript revised April 20, 2019

1.1 Background

Use of cryptography to protect privacy and security of information dates back centuries. The Arabs, Greeks, Persians and Romans have used this science in the implementation of their military plans. This science was further developed and exploited during the Second World War in communicating the so-called open encoded messages. Figure 1 shows the basic steps of the traditional process of concealment or retrieval [10-11].

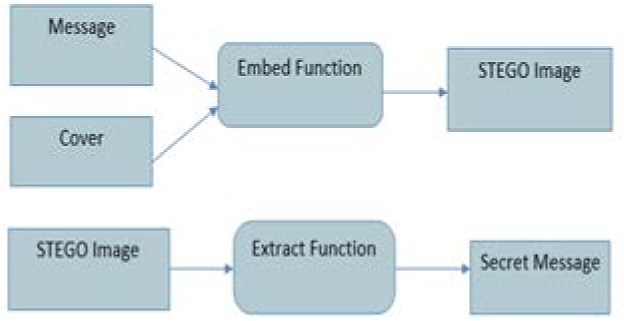


Fig. 1 Main phases of Steganography

With the passage of time, attackers developed tools to decrypt steganography messages and hence the protection of sensitive information once again emerged problematic. More on this science and surrounding issues can be learned from [12-14]. Some of these issues are listed below.

(a) There is always a possibility of having attackers around. Therefore, encryption must be used for the data to be converted and transmitted digitally.

(b) There could be a distortion problem which would occur as a result of information overload on digital data

(c) The possibility of attackers being able to decrypt the message.

(d) The possibility of attackers being able to detect the hash algorithm.

(e) The size of the data that can be hidden.

2. Literature Review

2.1 Encryption and Steganography

When we think of concealing a textual document of information, the foremost thing that comes to mind is the cryptography or conversion to another format which can only be decoded by means of a code key. But that does not mean that encryption is the only way in which information can be hidden from others as we mentioned historically. In fact, "Steganography" is one of the ways of concealing information that is often used by information thieves to steal sensitive information. [15]. The word "Steganography" means the concealment of information in a place illegally or in a clandestine manner that is not completely marked for the purpose of transferring it to another place, but without anyone knowing it. While Cryptography is used to hide the contents of the message (but everyone knows about its existence), Steganography is used to hide the message originally [16]. For example, someone may use an electronic image to convey text messages (or even other hidden images) to someone else without knowing anyone. The outside observer thinks that the two people share only pictures, while those images are loaded with hidden messages that are not clear [17].

A digital image is only a set of dots (pixels), which - depending on their pattern - contains a number of unnecessary or unused binary data, or its color intensity is so weak that it is possible to change it and add information to it without noticing the change in the real picture. For example, there are 256 grayscale gradients, but the human eye does not notice more than 32 gradients, so a slight change in the pixel value within the image will result in a change in one color that is impossible for the human eye to see, especially if we imagine the size of the pixel. And that one image may contain more than one million pixels and the distribution of modified pixels in a scatter [18].

2.1 Steganography and Watermark

It should be noted that the steganography is completely different from a watermark. In steganography, the concealment is invisible for security purposes in secret or sometimes illegal while the watermark is often hidden to preserve the copyright to increase information on the host file about the rights of its owner [19].

2.2 Information Security and Steganography

There are three issues associated with the information security, namely:

(a) *Reliability:* Any person who is not trusted or authorized will not know about the sensitive information

(b) Integrity: Ensure that hidden information will not be affected along the transmission path

(c) *Effectiveness:* It is not easy to discover hidden information in a file even if we suspect it exists. It is not affected or changed by the original file. Ordinary people will not notice any change to the file in which the information was hidden [20].

There are many types for steganography as described in [21] and listed below.

2.1.1 Hide information in a text file and the most important methods and algorithms [22-23]:

- First-letter algorithm

- o Every n-th character
- o ltering the amount of whitespace
- o Using a publicly available cover

2.1.2 Hide information in an image [24]:

- o The most popular medium!
- o Least-significant bit (LSB) modifications
    - o 24-bit vs. 8-bit images
    - o Tools to implement LSB: EzStego and S-Tools
  - o Masking and Filtering
  - o Algorithms and Transformations
- o Removing all but the two least significant bits of each color component produces an almost completely black image. Making that image 85 times brighter produces the image below. The limited human eye is used to detect chromatic gradients and minor noise within the image.

2.1.3 Hide information in a video or audio file [6-7]:

- o Hiding information is better because of the limited human hearing after the limit of 20000 Hz, this method is characterized by the large amount of data that can be hidden and this method is difficult to recognize because the transfer process is sequential.
- o Another recent type is using vector images, map of image, or 3D image as a cover [25].

2.1.4 Other Applications of Steganography [26-28]:

i. Security issues and confidential information on the computer and network

ii. Espionage on the information of others (may be positive or negative)

iii. Military cases and send encrypted information, confidential and non-noticeable

iv. Medical cases and the discovery of information more than medical images

v. Legal and copyright issues include information that cannot be removed. Here we mean watermarks because one of the most important characteristic of information (digital) is that it is very easy to produce and distribute an unlimited number of copies. This may undermine the music, film, books and software industries, so it therefore brings together a variety of important problems relating to the protection of intellectual property rights and production that needs to be resolved. In fact, an unlimited number of complete text, audio, data and video can be produced and distributed illegally.

It should be noted that there is a risk when using techniques of steganography illegally. If it is done so, then some spyware files would be sent to victims. One must be aware of the existence of something within the receiver file - there are a lot of algorithms and programs that provide this facility. However, from the previous discussion, the second problem is the possibility of information being hacked by these programs. This information can be extracted and decrypted.

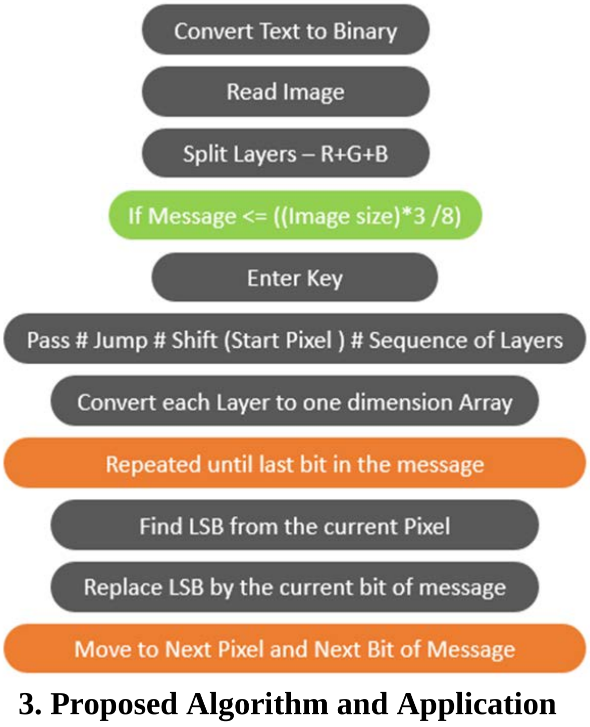

Convert Text to Binary
Read Image
Split Layers – R+G+B
If Message <= ((Image size)*3 /8)
Enter Key
Pass # Jump # Shift (Start Pixel) # Sequence of Layers
Convert each Layer to one dimension Array
Repeated until last bit in the message
Find LSB from the current Pixel
Replace LSB by the current bit of message
Move to Next Pixel and Next Bit of Message
3. Proposed Algorithm and Application

Fig. 2 Improved Algorithm of Steganography

3. Proposed Algorithm and Application

Here we outline our idea of distributing encrypted information in a way that makes it very difficult to access and decrypt it. The main proposed work is divided to two parts.

3.1 The First Part

To find a new method using Steganography which would be very difficult to break into. This is achieved by our proposed algorithm as shown in Figure 2. The main idea is to distribute the confidential message randomly in the Steganography cover each time. In the same time, enable the authenticated receiver who has the shared key of DES to know about the distribution methods automatically, by depending on this key only.

Initially, the system would separate each coloured layers Red (R), Green (G), and Blue (B) of the cover image, and convert each layer to one dimension array. Then the Key of DES would be divided into four components by "#" sign. The first component would be the small code

(Selected Password), while the second would refer to the number of pixels which we have to jump each time, the third would determine the pixel which we would start hiding from it. Finally, the last component would be a sequence of coloured layers. For example, if we suppose the key is PassKey#3#10#RRG, the hiding would start from the pixel 10, in the R layer, then in the pixel (10+3) in the R layer too, then in the pixel 10 but in the G layer. After, the previous steps would be repeated until entire message bits are hidden inside the cover image.
In this case, it is very difficult for any attacker to break the algorithm even if they collect the data from the least significant bit (LSB) in the cover image and try to decrypt them. An example for the proposed method is shown in Figure 3.

3.1 The Second Part

The second part of the system is a simple mobile application for applying the algorithm of Fig 2. This would enable users to share their secret data through a very strong protection method. The main interfaces of the proposed application are depicted in the Figure 4 and 5. In the next section we shall discuss the usefulness of our results.

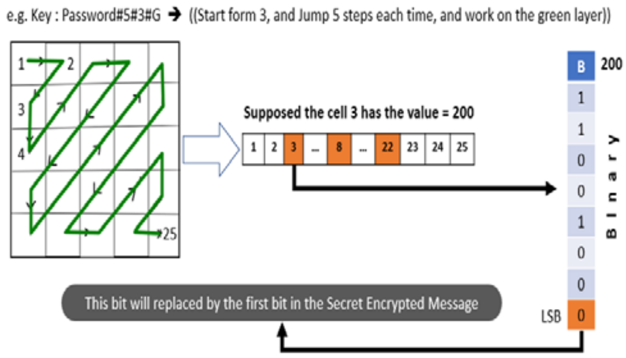
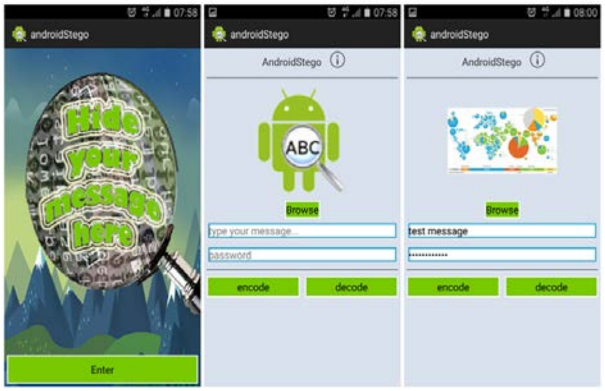

e.g. Key : Password#5#3#G ➔ ((Start form 3, and Jump 5 steps each time, and work on the green layer))
1
2
3
4
25
Supposed the cell 3 has the value = 200
1
2
3
...
8
...
22
23
24
25
B
200
1
1
0
0
1
0
0
0
Binary
LSB
This bit will replaced by the first bit in the Secret Encrypted Message

Fig. 3 Execution steps of the proposed method



test message

Fig. 4 Interface of mobile application (normal security)

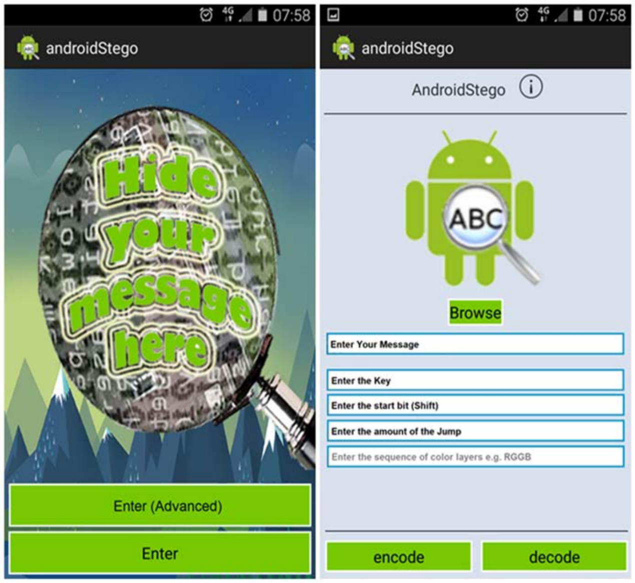


Fig. 5 Interface of mobile application (Advance security)

4. Results and Discussion

For proving the quality of the improved method, we have used metrics and have employed Correlation, Mean squared error (MSE), Peak signal-to-noise ratio (PSNR), and Bit Error Rate (BER) [29-31]. The correlation measures the similarity among the cover image and the new image after carrying the encoded the message.

$$corr = \frac{numberof\_unchangedpixels}{numberof\_all\_pixels\ in\_one\_imag}$$

MSE below calculates the mean error:

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(f_{ij} - g_{ij})^2$$

Where M, N are the number of rows and columns of the original image (cover), f ij denotes the element (Pixel) in the cover image, and gij represents the element (Pixel) of the new image after hiding message. The PSNR below measures the Peak Signal to Noise, where L is the level of peak signal that equals 255.

$$PSNRindB = 10Log_{10}\frac{L^2}{MSE}$$

Bit Error Rate measures the rate of noise after hiding the message, is given as:

$$BER = \frac{number\_of\_errors}{total\_number\_of\_bits\_send}$$

After testing the proposed method, the results are presented in Table 1.

Table 1: Metrics Results of Proposed Method

MSE	PSNR	Correlation	BER
105.074	64.278	0.97	0.3672

From Table 1 we can note that an amount of distortion is caused by adding the secret message to the cover image. However, it is very low according to the high PSNR values. The PSNR will differ according to the size of the secret message. That reflects the positive results under the term of human eye sensitivity to the luminance. This means, the hidden message will be invisible to an attacker completely. Furthermore, a high value of correlation means that the result with an encoded secret message is very similar to the original image, unlike to bit error rate that causes a low result since the changing of the image was done in the LSB.

The new method proposed by us is very strong and resistant to attacks. However, it would cause some insensitive noise, and have high similarity between the original image and the result image. But, it is not resistant to compressing because it depends on the LSB, and that is what we shall try address in the future by enhancing other techniques for steganography as wavelet transformation.

5. Conclusion

This paper has demonstrated an improvement for the steganography technique based on LSB. It has suggested a new method of making an encryption key which has divided into four components and can be used for creating a very complex distribution of a secret message inside the cover image. This was dependent on the jumping, shifting, and changing the sequence of the color layers. Hence, no attacker can retrieve it without the shared used key. In addition, this research has proposed and implemented a mobile application for the proposed method to enable any user to share their extremely confidential and important data without being concerned about any potential attack. The testing has shown the efficiency of the proposed method. In our future research, we intend to focus on the enhancement of security more vigorously and increase the amount of data that can be shielded in the cover to provide higher resistance of the proposed algorithm against compression attacks.

References

[1] Sen, A. A. A., Eassa, F. A., Jambi, K., & Yamin, M. (2018). Preserving privacy in internet of things: a survey. International Journal of Information Technology, 10(2), 189-200.

[2] Yamin, M., Sen, A. A. A. (2018) Improving privacy and security of user data in location-based services. Int J Ambient Comput Intell (IJACI) 9(1):19–42

[3] Sen, A. A. A., Eassa, F. B., Yamin, M., & Jambi, K. (2018). Double Cache Approach with Wireless Technology for Preserving User Privacy. Wireless Communications and Mobile Computing, 2018.

[4] Kumari, T., & Singh, K. (2018). A Review on Information Hiding Methods. International Journal of Engineering Science, 17474.

[5] Sadasivam, V. R., Abishake, R., & Tamilarasan, R. (2019). Image Steganography. South Asian Journal of Engineering and Technology, 8(S 2), 140-143.

[6] Mustafa, M. F., & Beh, D. M. Y. (2018). Secure Data Transmission by Using Video Steganography. Journal of Computing Technologies and Creative Content (JTeC), 3(1), 15-21.

[7] Sinha, Nishith, Anirban Bhowmick, and B. Kishore. "Encrypted Information Hiding using Audio Steganography and Audio Cryptography. " International Journal of Computer Applications 112.5 (2015).

[8] Yahya, A. (2019). Steganography Techniques. In Steganography Techniques for Digital Images (pp. 9-42). Springer, Cham.

[9] Sellars, Duncan. "An introduction to steganography." cs. uct. ac.za/courses/CS400W/NIS/papers99/dsellars/stego. html (1999).

[10] Douglas, M., Bailey, K., Leeney, M., & Curran, K. (2018). An overview of steganography techniques applied to the protection of biometric data. Multimedia Tools and Applications, 77(13), 17333-17373.

[11] Ramesh, Vikash, Kaushik Narayanan, and Premalatha Pandian. "Steganography in Audio Signals using Variable Bit eplacement Method in DCT Domain." International Journal of Engineering Research and Technology. Vol. 3. No. 4 (April-2014). ESRSA publications.

[12] Mstafa, R. J., Elleithy, K. M., & Abdelfattah, E. (2017, May). Video steganography techniques: Taxonomy, challenges, and future directions. In 2017 IEEE Long Island Systems, Applications and Technology Conference (LISAT) (pp. 1-6). IEEE.

[13] Jain, Nitin, Sachin Meshram, and Shikha Dubey. "Image Steganography Using LSB and Edge–Detection Technique." International Journal of Soft Computing and Engineering (IJSCE) ISSN 223 (2012).

[14] Gupta, Shilpa, Geeta Gujral, and Neha Aggarwal. "Enhanced Least Significant Bit algorithm For Image Steganography." IJCEM International Journal of Computational Engineering & Management 15.4 (2012): 40- 42.

[15] Purcell, O., Wang, J., Siuti, P., & Lu, T. K. (2018). Encryption and steganography of synthetic gene circuits. Nature communications, 9(1), 4942.

[16] Purcell, O., Wang, J., Siuti, P., & Lu, T. K. (2019). Publisher Correction: Encryption and steganography of synthetic gene circuits. Nature communications, 10(1), 154.

[17] Gutub, Adnan, et al. "Pixel indicator high capacity technique for RGB image based Steganography. " WoSPA 2008–5th IEEE International Workshop on Signal Processing and its Applications. 2008.

[18] Bloisi, Domenico Daniele, and Luca Iocchi. "Image based steganography and cryptography." VISAPP (1). 2007.

[19] Al-Mualla, Mohammed, and Hussain Al-Ahmad. "Information hiding: steganography and watermarking." Proceedings of the IEEE (2008).

[20] Al-Rahal, M. S., ABI SEN, A. D. N. A. N., & Basuhil, A. A. (2016). HIGH LEVEL SECURITY BASED STEGANORAPHY IN IMAGE AND AUDIO FILES. Journal of Theoretical & Applied Information Technology, 87(1).

[21] Nissar, Arooj, and A. H. Mir. "Classification of steganalysis techniques: A study. " Digital Signal Processing 20.6 (2010): 1758-1770.

[22] Bhattacharyya, Souvik, Indradip Banerjee, and Gautam Sanyal. "A novel approach of secure text based steganography model using word mapping method (WMM). " International Journal of Computer and Information Engineering 4.2 (2010): 96-103.

[23] Chen, Po-Yueh, and Hung-Ju Lin. "A DWT based approach for image steganography." International Journal of Applied Science and Engineering4.3 (2006): 275-290.

[24] Kumar, Samir, B. Barnali, and G. Banik. "LSB modification and phase encoding technique of audio steganography revisited." International Journal of Advanced Research in Computer and Communication Engineering 1.4 (2012): 1-4.

[25] Banerjee, Indradip. "Text Steganography using Article Mapping Technique (AMT) and SSCE." Journal of Global Research in Computer Science 2.4 (2011).

[26] Liao, X., Yin, J., Guo, S., Li, X., & Sangaiah, A. K. (2018). Medical JPEG image steganography based on preserving inter-block dependencies. Computers & Electrical Engineering, 67, 320-329.

[27] Elshare, S., & El-Emam, N. N. (2018). Modified Multi-Level Steganography to Enhance Data Security. International Journal of Communication Networks and Information Security, 10(3), 509.

[28] Jia-jia, J., Xian-quan, W., Fa-jie, D., Xiao, F., Han, Y., & Bo, H. (2018). Bio-Inspired Steganography for Secure Underwater Acoustic Communications. IEEE Communications Magazine, 56(10), 156-162.

[29] Jacobs, David. "Correlation and Convolution." Class Notes for CMSC 426 (2005).

[30] Hore, Alain, and Djemel Ziou. "Image quality metrics: PSNR vs. SSIM."Pattern Recognition (ICPR), 2010 20th International Conference on. IEEE, 2010.

[31] Kurniawan, Budi. Java: A Beginner's Tutorial. Brainy Software Inc, 2015.

Abdullah M. Basahel He is an Associate Professor of MIS in the faculty of Economics and Administration, King Abdulaziz University, Jeddah, Saudi Arabia.

Professor Mohammad Yamin (ANU) He is a Professor of MIS in the Faculty of Economics and Administration, KAU, King Abdulaziz University, Jeddah, Saudi Arabia. He obtained his PhD from the Australian National University (ANU) in 1983. Professor Yamin also holds an Adjunct position at the ANU.

Adnan Ahmed Abi Sen He has obtained his PhD from the King Abdulaziz University and now works for the Islamic University, Madinah, Saudi Arabia.