International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 4– No.11, December 2012 – www.ijais.org

Efficient Data Hiding System using Cryptography and Steganography

Abikoye Oluwakemi C.
Department of Computer Science
University of Ilorin, Ilorin

Adewole Kayode S.
Department of Computer Science
University of Ilorin, Ilorin

Oladipupo Ayotunde J.
Department of Computer Science
University of Ilorin, Ilorin

ABSTRACT
Increase in the number of attack recorded during electronic exchange of information between the source and intended destination has indeed called for a more robust method for securing data transfer. Cryptography and steganography are well known and widely used techniques that manipulate information in order to cipher or hide their existence. These two techniques share the common goals and services of protecting the confidentiality, integrity and availability of information from unauthorized access. In this paper, a data hiding system that is based on audio steganography and cryptography is proposed to secure data transfer between the source and destination. Audio medium is used for the steganography and a LSB (Least Significant Bit) algorithm is employed to encode the message inside the audio file. The proposed system was evaluated for effectiveness and the result shows that, the encryption and decryption methods used for developing the system make the security of the proposed system more efficient in securing data from unauthorized access. The system is therefore, recommended to be used by the Internet users for establishing a more secure communication.

General Terms
Information Security, Simulation and Algorithm.

Keywords
Electronic exchange, cryptography, steganography, Least Significant Bit, algorithm.

1. INTRODUCTION

Steganography is the art and science of hiding communication; a steganographic system thus embeds hidden content in unremarkable cover media so as not to arouse an eavesdropper's suspicion. In the past, people used hidden tattoos or invisible ink to convey steganographic content. Today, computer and network technologies provide easy-to-use communication channels for steganography. Essentially, the information-hiding process in a steganographic system starts by identifying a cover medium's redundant bits (those that can be modified without destroying that medium's integrity). The embedding process creates a stego medium by replacing these redundant bits with data from the hidden message [4]. Modern steganography's goal is to keep the presence of the message undetectable from an unauthorized access.

Cryptography and Steganography are well known and widely used techniques that manipulate information in order to cipher or hide their existence respectively. Cryptography scrambles a message so it cannot be understood; the Steganography hides the message so it cannot be seen. According to [1] cryptography is not sufficient for secure communication. Even though both methods provide security, a study is made to combine both Cryptography and Steganography methods into one system for better confidentiality and security [5]. Combining these two methods together for the purpose of developing a system that will improve the confidentiality and security of the message is however, the goal of this research. According to [7], the power of steganography is in hiding the secret message by obscurity, hiding its existence in a non-secret file. In that sense, steganography is different from cryptography, which involves making the content of the secret message unreadable while not preventing non-intended observers from learning about its existence. The success of steganography technique depends entirely on the ability to hide the message such that an observer would not suspect its existence, the greatest effort must go into ensuring that the message is invisible unless one knows what to look for. The way in which this is done will differ for the specific media that are used to hide the information. In each case, the value of a steganography approach can be measured by how much information can be concealed in a carrier before it becomes detectable, each technique can thus be thought of in terms of its capacity for information hiding [7].

Basically, the purpose of cryptography and steganography is to provide secret communication. Steganography can be used to cloak hidden messages in image, audio, video and even text files. According to [7], the two most common methods used for hiding information inside a picture, audio and video files are LSB (Least Significant Bit) and Injection. In this paper, an audio medium was used for the steganography and a more powerful modified LSB (Least Significant Bit) algorithm was employed for encoding the message into the audio file.

2.REVIEW OF EXISTING TECHNIQUES FOR INFORMATION HIDING

Several techniques have been proposed by researchers for securing electronic communication. In the research work of [9], the researchers proposed cryptography and steganography for securing data transfer using images as cover objects for steganography and key for the cryptography. The performance of the proposed ISC (Image-Based Steganography and Cryptography) system was presented and the system was compared with F5 algorithm. Also, [10] proposed method that described two steps for hiding secret information by using the public steganography based on matching method. The first step, finds the shared stego-key between the two communication parties (Alice and Bob) over the networks by applying Diffie Hellman Key exchange protocol. The second step in the proposed method is that, the sender uses the secret stego-key to select pixels that it will be used to hide. Each selected pixel is then used to hide 8 bits binary information

depending on the matching method. The proposed method is summarized in figure 1:

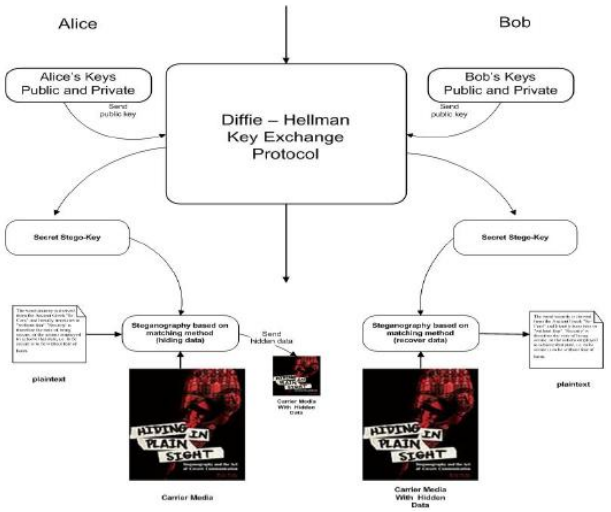

Figure 1: Proposed public key steganography protocol, adapted from [10].

[11] in their research proposed two approaches for secured image steganography using cryptographic techniques and type conversions. One of the methods shows how to secure the image by converting it into cipher text through S-DES algorithm using a secret key and conceal this text in another image using steganographic method. The second method shows a new way of hiding an image in another image by encrypting the image directly through S-DES algorithm using a key image and the data obtained is concealed in another image. The flows of the two approaches are shown in figure 2 and 3:

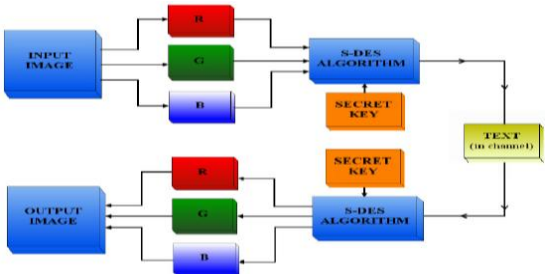

Figure 2: Flow of the first approach, adapted from [11].

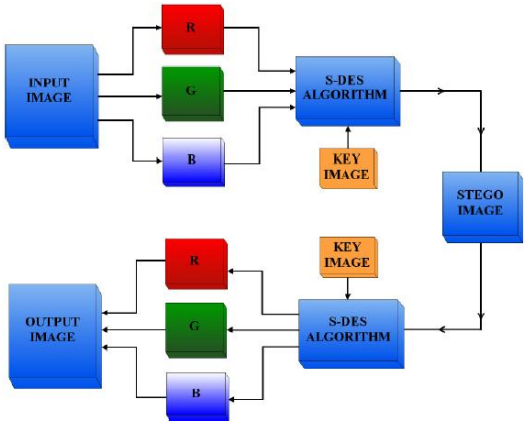

Figure 3: Flow of the second approach, adapted from [11].

3. COMBINATION OF CRYPTOGRAPHY AND STEGANOGRAPHY

Steganography must not be confused with cryptography that involves transforming the message so as to make its meaning obscure to malicious people who intercept it. In this context, the definition of breaking the system is different. In cryptography, the system is broken when the attacker can read the secret message. Breaking a steganographic system needs the attacker to detect that steganography has been used and he is able to read the embedded message. According to [8], steganography provides a means of secret communication, which cannot be removed without significantly altering the data in which it is embedded. In addition, the security of classical steganography system relies on secrecy of the data encoding system. Once the encoding system is known, the steganography system is defeated [5].

However, it is always a good practice to use Cryptography and Steganography together for adding multiple layers of security. By combining, the data encryption can be done by a software and then embed the cipher text in an audio or any other media with the help of stego key. The combination of these two methods will enhance the security of the data embedded. This combined chemistry will satisfy the requirements such as capacity, security and robustness for secure data transmission over an open channel [5]. The figure below depicts the combination of cryptography and steganography:

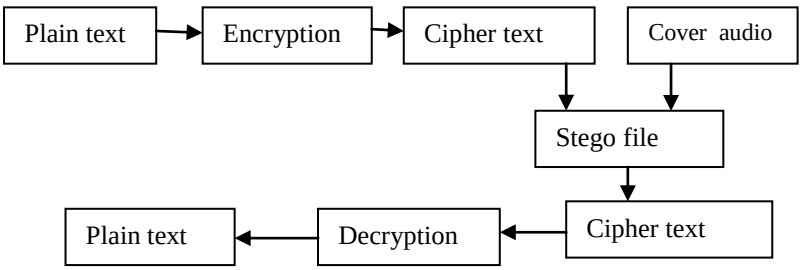

Figure 4: Combination of cryptography and steganography

4. METHODOLOGY

4.1 Least Significant Bit (LSB)

A very popular methodology is the LSB (Least Significant Bit) algorithm, which replaces the least significant bit in some bytes of the cover file to hide a sequence of bytes containing the hidden data [2]. LSB coding is the simplest way to embed information in a digital audio file by substituting the least significant bit of each sampling points with a binary message. In computing, the least significant bit (LSB) is the bit position in a binary integer giving the units value, that is, determining whether the number is even or odd. The LSB is sometimes referred to as the right-most bit, due to the convention in positional notation of writing less significant digit further to the right. It is analogous to the least significant digit of a decimal integer, which is the digit in the right-most position. In referencing specific bits within a binary number, it is common to assign each bit a bit number, ranging from zero upwards to one less than the number of bits in the number. The least significant bits have the useful property of changing rapidly if the number changes even slightly. For example, if 1 (binary 00000001) is added to 3 (binary 00000011), the result will be 4 (binary 00000100) and three of the least significant bits will change (011 to 100). By contrast, the three most significant bits stay unchanged (000 to 000). Least significant bits are frequently employed in pseudorandom number generators checksums. The figure below illustrates how the message "HEY" is encoded in a 16-bit CD quality sample using the LSB method.

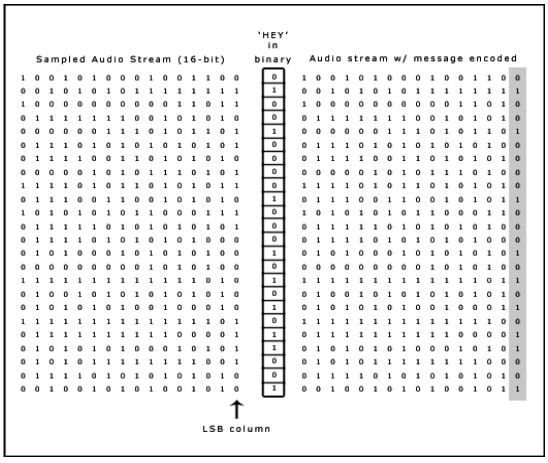

Figure 5: Illustration of how the message "HEY" is encoded using LSB method, adapted from [2].

In this figure, the secret information is 'HEY' and the cover file is audio file. HEY is to be embedded inside the audio file. First the secret information 'HEY' and the audio file are converted into bit stream. The least significant column of the audio file is replaced by the bit stream of secret information 'HEY'. The resulting file after embedding secret information 'HEY' is called Stego-file. In this paper, LSB method was employed during the encoding stage to encode the message inside an audio file.

4.2 Encoding

LSB method allows large amount of secret information to be encoded in an audio file. Audio file contains set of bytes which can be used for encoding. Some audio files may contain several bytes depending on their sizes. The following steps were used during the encoding stage:

- Encrypt the message using public key
- Convert the audio file into bit stream
- Convert each character in the message into bit stream
- Replace the LSB bit of the audio file with the LSB bit of character in the message to hide

4.3 Decoding

In this stage, the encoded file is decoded to get the hidden message. The message is decoded first and then decrypted by the public key that is known only by the authorized receivers or users of the proposed system.

4.4 Encryption

During encryption, the user is allowed to enter a password/key in any combination of numbers, symbols and characters. The key contains set of characters, which are used to encrypt the message before encoding.

4.5 Decryption

The user's password/key is supplied to decrypt the encrypted message in order to get the original message. The processes of encryption and decryption are handled by DES (Data Encryption Standard) algorithm.

4.6 Use Case Diagram

Use case diagram represents the functionality of the system from the user's point of view. In Unified Modeling Language, use case diagrams are used to show the functionality that the system will provide and to show which users will communicate with the system in some way to use that functionality [6]. The use case diagrams for the encoding and decoding processes of the proposed system are shown below:

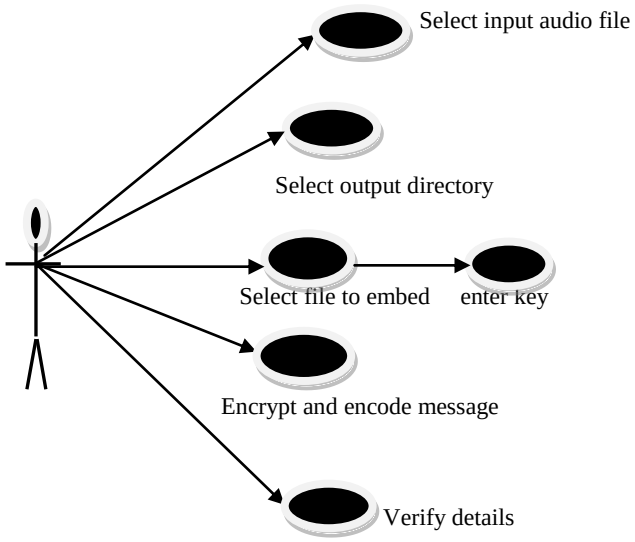

Figure 6: Use case diagram for embedding/encoding

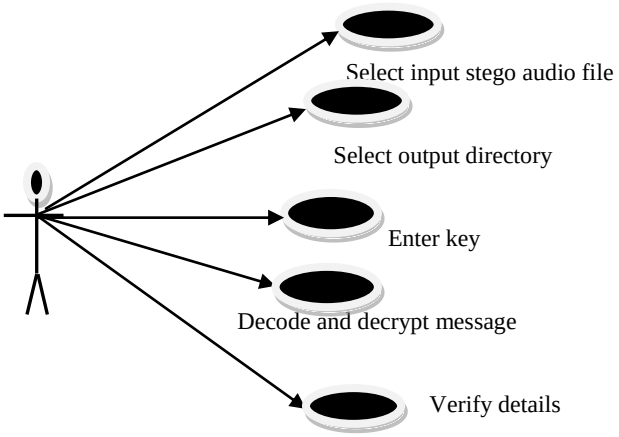

Figure 7: Use case diagram for extraction/decoding

5. RESULTS AND DISCUSSION

5.1 Main Class

The proposed system was developed using Java programming language. During execution, the main class displays the following GUI which contains options for selecting either embedding/encoding action for a new file or message, or extracting/decoding action for already embedded file. The interface also allows the user to exit the application.

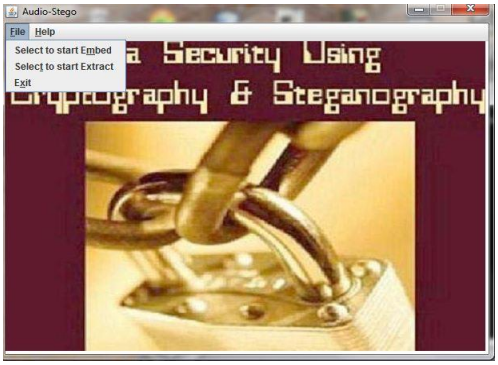

Figure 8: Interface after execution of main class

5.2 Embedding/Encoding Process

Figure 9 shows the embed wizard which is displayed after choosing the embedding action "Select to start embed" from the menu in figure 8. In this wizard, the current step is boldly highl0ighted on the left-hand side of the screen.

Figure 9: Embed wizard

The input audio file is selected using the Jfilechooser class by clicking on the select file button. This action displays the figure below.

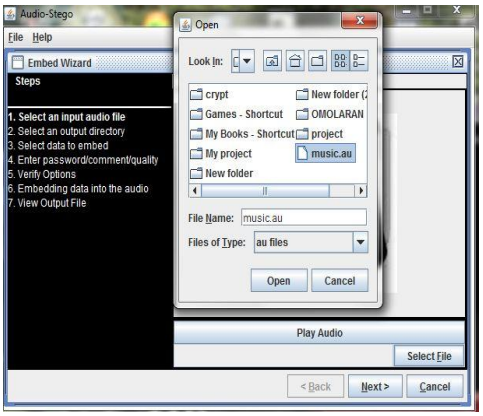

Figure 10: Select audio file

After selecting the audio file that to embed/encode, the next step is to proceed with the output directory selection. This is the directory where the output stego audio file will be saved.

After the output directory has been selected, the user selects the text file or text message to embed using the figure below:

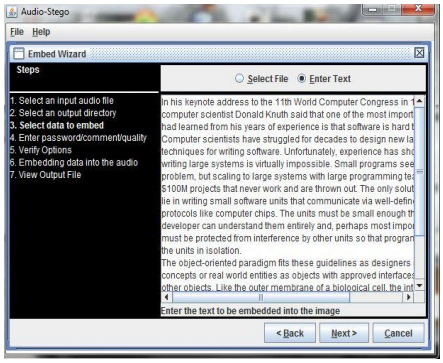

Figure 11: Message to embed

The next step is to provide password to complete the embedding process. After completing the process, figure 12 displays the details of the input and output file as well as the directory of the stego audio file.

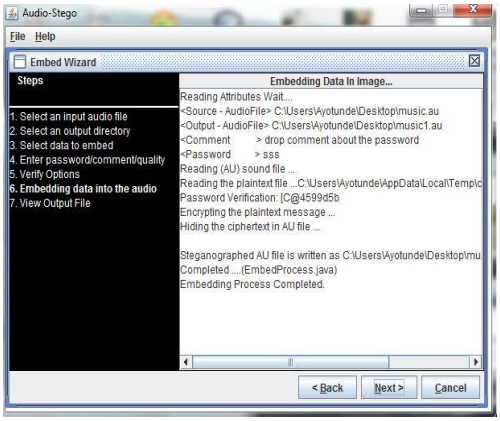

Figure 12: Details of embedded/encoded message

5.3 Extracting/Decoding Process

The extract wizard shown in figure 13 is displayed after clicking on "Select to start extract" option from the main menu in figure 8.

Figure 13: Extraction wizard

The stego audio file is selected for extraction by clicking on "Select File" button. This action therefore, displayed a dialog box for selecting the stego audio file as shown in figure 14.

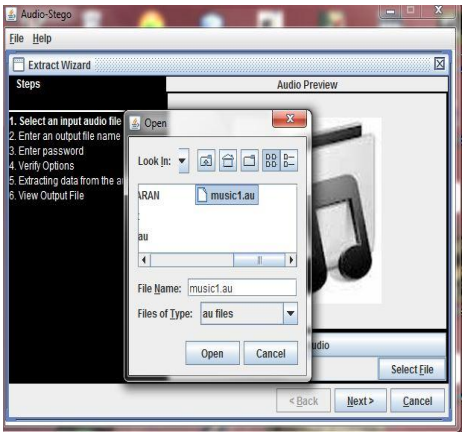

Figure 14: Stego audio file selection

After clicking on "Next" button, the system prompted for output directory and key for the decryption process. If the key is correct, then the message is decoded and decrypted from the audio file. The output of this action will display the decrypted message embedded in the audio file as shown in figure 15, this message is saved in the selected output directory.

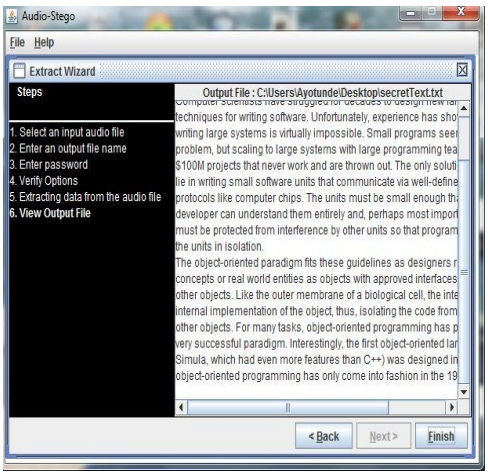

Figure 15: Embedded message after extraction

6. CONCLUSION AND RECOMMENDATION

In this paper, a system that combined the techniques of cryptography and steganography to provide efficient method of hiding data from any unauthorized users was presented. An audio medium was used for the steganography and the Least Significant Bit algorithm was employed to encode the message inside the audio file. This proposed system does not tamper with the original size of the file even after encoding and also suitable for any type of audio file format. The encryption and decryption techniques used with this system make its security more robust. The system is therefore, recommended to used by Internet users for establishing a more secured communication.

7. REFERENCES

[1] Dipti, K. S. and Neha, B. 2010. Proposed System for Data Hiding Using Cryptography and Steganography. *International Journal of Computer Applications.* 8(9), pp. 7-10. Retrieved 14th August, 2012 from http://www.ijcaonline.org/volume8/number9/pxc3871714.pdf.

[2] Jayaram, P., Ranganatha, H. R. and Anupama, H. S. 2011. Information Hiding Using Audio Steganography – A Survey. *International Journal of Multimedia and Its Application*, 3(3), pp. 86-96.

[3] Mark D. G. 2003. Chameleon Image Steganography-Technical Paper. Retrieved 14th July, 2012 from http://faculty.ksu.edu.sa/ghazy/Steg/References/ref13.pdf.

[4] Niels, P. and Peter, H 2003. Hide and Seek: An Introduction to Steganography. *IEEE Computer Society*. IEEE Security and Privacy, pp. 32-44.

[5] Raphael, A. J., and Sundaram, V. 2011. Cryptography and Steganography - A Survey. *International Journal of Computer Technology Application*, 2(3), ISSN: 2229-6093, pp. 626-630.

[6] Simon, B., Steve M., and Ray, F. 2005. Object-Oriented Systems Analysis and Design Using UML, (3rd ed.), McGraw Hill.

[7] Sridevi, R., Damodaram, A., and Narasimham, S. 2009. Efficient Method of Audio Steganography By Modified LSB Algorithm and Strong Encryption Key with Enhanced Security. *Journal of Theoretical and Applied Information Technology*, pp. 768-771. Retrieved 21st August, 2012 from http://www.jatit.org.

[8] Vivek, J., Lokesh, K., Madhur, M. S., Mohd, S., and Kshitiz Rastogi 2012. Public-Key Steganography Based on Modified LSB Method. *Journal of Global Research in Computer Science*, 3(4). ISSN: 2229-371X, pp. 26-29.

[9] Domenico, B. and Luca, L. year. Image Based Steganography and Cryptography.

[10] Mohammad, A. A., and Abdelfatah, A. Y. 2010. Public-Key Steganography Based on Matching Method. *European Journal of Scientific Research*, 40(2). ISSN: 1450-216X. EuroJournals Publishing, Inc., pp. 223-231. Retrieved 21st August, 2012 from http://www.eurojournals.com/ejsr.htm.

[11] Sujay, N. and Gaurav, P. 2010. Two New Approaches for Secured Image Steganography Using Cryptographic Techniques and Type Conversions. *Signal & Image Processing: An International Journal (SIPIJ)*, 1(2), pp 60-73.