ISSN:2320-0790

COMPUSOFT
An International Journal of Advanced Computer Technology

REVIEW ARTICLE

Available online at https://ijact.in

DEVELOPMENT OF A DATA SECURITY MODEL USING STEGANOGRAPHY

Terungwa Simon Yange and Moses Agana A

Department of Mathematics/Statistics/Computer Science,
Federal University of Agriculture, Makurdi, Nigeria

Abstract: This paper studied steganography and designed a simplistic approach to a steganographic tool for hiding information in image files with the view of addressing the security challenges with data by hiding data from unauthorized users to improve its security. The Structured Systems Analysis and Design Method (SSADM) was used in this work. The system was developed using Java Development Kit (JDK) 1.7.0_10 and MySQL Server as its backend. The system was tested with some hypothetical health records which proved the possibility of protecting data from unauthorized users by making it secret so that its existence cannot be easily recognized by fraudulent users. It further strengthens the confidentiality of patient records kept by medical practitioners in the health setting. In conclusion, this work was able to produce a user friendly steganography software that is very fast to install and easy to operate to ensure privacy and secrecy of sensitive data. It also produced an exact copy of the original image and the one carrying the secret message when compared with each other.

Keywords: steganography, cryptography, encryption, decryption, secrecy

I. INTRODUCTION

Data like medical records of patients are extremely sensitive information, needing uncompromising security during both storage and transmission. Such records often have to be traceable to patient medical data such as medical diagnosis, X-ray or scan (CAT, MRI etc.) images. While numerous security tools that encrypt the information and prevent unauthorized access to the data exist, the possibility of hiding the very existence of these records, using image steganography is discussed in this research.

Data has literally become an organization’s backbone and it is essential to implement procedures in order to ensure the security of data. No technique is full-proof; hence it is necessary to understand that by implementing data protection techniques one cannot guarantee the security of data. However, the damage done can be considerably reduced [1]. Steganography is a Greek word meaning secrete writing. It is the art and science of writing hidden messages in such a way that no one apart from the sender and intended recipient even realizes there is a hidden message [1]. It is the practice of hiding messages so that the presence of the message itself is hidden, often by writing them in places where they may not be found, specifically; the use of small files in computers to communicate secret information Steganography is a technology that hides a message within an object, a text, pictures or media files. It hides the existence of a message from a third party, thereby allowing for an easy transfer of sensitive data without prying eyes being able to tell that a message is being transported [1]. Put in another way, it is an information hiding technique which allows the concealment of files and messages within other files such as media files. It is often confused with Cryptography, not by name but in appearance and usage. The easiest way to differentiate between the two is to remember that Steganography conceals not only the contents of the message but also the mere existence of the message. Cryptography is the science of writing in secret code. It is necessary when communicating over any untrusted medium, which includes just about *any* network, particularly the Internet. Within the context of any application-to-application communication, there are some specific security requirements, including:

- *Authentication:* The process of proving one's identity. The primary forms of host-to-host authentication on the Internet today are name-based or address-based, both of which are notoriously weak.
- *Privacy/confidentiality:* Ensuring that no one can read the message except the intended receiver.
- *Integrity:* Assuring the receiver that the received message has not been altered in any way from the original.
- *Non-repudiation:* A mechanism to prove that the sender really sent this message and cannot deny sending such a message.

Cryptography does not only protect data from theft or alteration, but can also be used for user authentication. Generally speaking, there are three types of cryptographic schemes typically used to accomplish these goals: secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography, and hash functions, each of which is described below. In all cases, the initial unencrypted data is referred to as *plaintext*. It is encrypted into *ciphertext*, which will in turn (usually) be decrypted into usable plaintext [2].

Communication between two parties over long distances has always been subjected to interception, this led to the development of encryption schemes [2]. Encryption scheme achieve security basically through a process of making a message unintelligible so that those who do not possess the necessary decryption keys cannot recover the message. Through encryption, we can hide the content of a message as does cryptography, the existence of an encrypted communication in progress cannot be hidden from a third party, who might be able to decipher the message. The need to avoid this led to the development of Steganography schemes which compensate encryption by hiding the existence of a secret communication. It provides good security in itself and so when combined with encryption it becomes a powerful security tool. Steganography improves encryption and security by creating a medium in which sensitive data can be passed through prying eyes via a file, without alerting anyone that the transmitted file actually contains a message. It should be implemented more in practice today as cyber-terrorism and data-theft are becoming an everyday occurrence. It is a relatively old technology, but is still very young with regards to modern usage. With the high security concerns of cooperation and individual users alike, the secure transmission of data needs to be a viable option.

Cryptography provides privacy, while Steganography provide secrecy. Privacy is what we need when we use our credit card on the internet (i.e. we don’t want our PIN revealed to the public). For this we use cryptography and send a coded pile of gibberish that only the website can decipher. Though your code may be unbreakable, any hacker can look and see that we have sent a message. But for true secrecy [4], we don’t want anyone to know we’re sending a message at all. With Cryptography, secret messages are converted into a format that is incomprehensible and unreadable without the knowledge of secret information. While with Steganography, the secret message is concealed into a host of media such as text, image, audio or video, so that the hidden data are imperceptible from unintended observer. The security challenges with data have greatly been addressed by using cryptographic techniques to enhance its privacy. But in order to fully protect data from unauthorized users, there is need to also make it secret so that its existence will not be easily recognized by fraudsters. Hence, this research seeks to develop a system to address this issue. The research is aimed at the development of a system to enhance data security using a combination of steganography and cryptography.

II. LITERATURE REVIEW & RELATED WORK

The concept of hiding information in other content has existed for centuries “the formal study of information hiding is called steganography” [2]. Steganography comes from the Greek words “stegos”- meaning roof or covered and “graphia”-meaning writing, is the practical science of hiding information inside other media with the intention of giving the impression that no hidden data is present. While we are discussing it in terms of computer security, steganography is not a new technology, as it has been around since the times of ancient Rome and Greece, where text was traditionally written on wax that was poured on top of stone tablets. If the sender of the information wanted to obscure the message for purposes of military intelligence, for instance they would use steganography; the wax would be scrapped off and the message would be inscribed or written directly on the tablet, wax would then be poured on top of the message, thereby obscuring not just its meaning but its very existence [4].

Steganography and cryptography are closely related. Cryptography scrambles messages so that they cannot be understood. The goal is to prevent the viewing of sensitive data so that only the sender and recipient can view it. But steganography is intended to take cryptography to the next level by attempting to prevent the impression of the existence of any sensitive data. That is it hides the message (data) so that there is no knowledge of the existence of the message in the first place. Also, it is a system or technique that allows a sender to embed a hidden file or message inside a cover file. A cover file is simply that which is used to embed hidden data. This cover file may be a graphics image, an audio file (such as WAV or MP3), or even a binary executable or video file. Therefore, what steganography does is to exploit human perception, as human senses are not trained to look for files that have information hidden inside of them. Even though there are programs available that can do what is called steganalysis (detecting the use of steganography). Steganography is commonly used to hide a file inside another file and that hidden file inside a carrier file is usually encrypted with a password. For example a foreign military may have a double agent working inside the Nigerian Military, the agent steals some sensitive documents and he wants to copy them onto CD to take home and email to his superiors. He knows that if he burns the documents to the disk, there is a risk of the disk being checked. So what could he do? Simple, he hides the documents inside picture files that look nothing out of ordinary.

III. Types of Steganography

Steganography can be split into two types which are Fragile and Robust. The fragile steganography involves embedding information into a file which is destroyed if the file is modified. This method is unsuitable for recording the copyright holder of the file since it can be so easily removed, but is useful in situations where it is important to prove that the file has not been tampered with, such as using a file as evidence in a court of law since any tampering would have removed the watermark. It is quite easy to implement than the robust method. The robust steganography aims at embedding information into a file which cannot easily be destroyed. Although no mark is truly indestructible, a system can be considered robust if the amount of changes required to remove the mark would render the file useless. Therefore the mark should be hidden in a part of the file where its removal would be easily perceived. Steganography can also be classified into the following forms.

Steganography in images: When hiding information inside images the least significant byte (LSB) method is usually used. To a computer an image file is simply a file that shows different colors and intensities of light on different areas of an image. The best type of image file to hide information inside is a 24Bit BMP (bitmap) image.

According to Sellars [5], “to a computer, an image is an array of numbers that represent light intensities at various points, or pixels. These pixels make up the images raster data." When dealing with digital images for use with Steganography, 8-bit and 24-bit per pixel image files are typical. Both have advantages and disadvantages, as explained below.

8-bit images are a great format to use because of their relatively small size. The drawback is that only 256 possible colors can be used which can be a potential problem during encoding. Usually a gray scale color palette is used when dealing with 8-bit images such as (.GIF) because its gradual change in color will be harder to detect after the image has been encoded with the secret message.

24-bit images offer much more flexibility when used for Steganography. The large numbers of colors (over 16 million) that can be used go well beyond the human visual system (HVS), which makes it very hard to detect once a secret message has been encoded. The other benefit is that a much larger amount of hidden data can be encoded into a 24-bit digital image as opposed to an 8-bit digital image. The one major drawback to 24-bit digital images is their large size (usually in MB) that makes them more susceptible to suspicion than the much smaller 8-bit digital images (usually in KB) when sent over an open system such as the Internet [6].

Steganography in audio: When hiding information inside audio files the technique usually used is Low Bit Encoding (LBE) which is somewhat similar to LSB that is generally used in images. The shortcoming of Low Bit Encoding is that it is usually noticeable to the human ear, so it is rather a risky method for someone to use if they are trying to mask information inside of an audio file.

Steganography in video: When information is hidden inside video, the program or person hiding the information will usually use the Discrete Cosine Transform (DCT) method. This works by slightly changing each of the images in the video only so much though, so it isn’t noticeable by the human eye. To be more precise about how DCT works, it alters values of certain parts of the images by rounding them up. For example if part of the image has a value of 6.667 say, it will round up to 7. Steganography in video, apart from the fact that information is hidden in each frame of the video is better off when only a small amount of information is hidden inside of a video as it is generally not noticeable at all. However, the more information that is hidden, the more noticeable it will become [8].

Steganography in documents/text: The use of steganography in documents works by simply adding white space and tabs to the ends of the links of a document. This form of steganography is extremely effective because the used **of** white space and tabs is not visible to the human eye at all, at least in most text/document editors. White space and tabs occur naturally in documents so there isn’t really any possible way that using this method of steganography would cause someone to be suspicious [8].

Steganography goes well beyond simply embedding text in an image. It also pertains to other media, such as voice, binary files and communication channels. Messages can be carried in TCP/IP protocol suites due to its number of weakness. Also, TV sounds can hide machine instructions, as it is reported that a firm (scientific Generics) in UK is patenting a technique which they call “infrasonic”. It was developed for hiding control signals in television broadcast sound. The technique will be used to control toys to help maintain children’s interest in the television shows.

The general model of hiding data in other data can be described as follows; the embedded data is the message that one wishes to send secretly. It is usually hidden in an innocuous message referred to as a cover-text or cover image or cover- audio as appropriate, producing the stego-text or other stego-object. The purpose of steganography is to have a covert communication between two parties whose existence is unknown to a possible attacker, as a successful attack consists in detecting the existence of the communication. The classification of steganography which involves the process of generally placing a hidden message in some transport medium, called the carrier. The secret message is embedded in the carrier to form the steganography medium [9][10]. Technical steganography uses scientific methods to hide a message, such as the use of invisible ink or microdots and other size reduction methods [11].

To start, we look at what a hypothetical perfect secret communication (Steganography) would consist of. To illustrate this concept, we will assume three hypothetical characters named Tony, Yange and Agana. Tony wants to send a secret message (M) to Yange using a random (R) harmless message to create a cover (C) which can be sent to Agana without raising suspicion. Tony then changes the cover message (C) to a stego-object (SO) by embedding the secret message (M) into the cover message (C) by using a stego-key (SK). Tony should then be able to send the stego-object (SO) to Yange without being detected by Agana. Yange will then be able to read the secret message (M) because he knows the stego-key (SK) used to embed it into the cover message (C) [6].

As pointed out by [7], "in a 'perfect' system, a normal cover should not be distinguishable from a stego-object, neither by a human nor by a computer looking for statistical patterns”. This is however not always the case in practice. In order to embed secret data into a cover message, the cover must contain a sufficient amount of redundant data or noise. This is because the embedding process used by steganography actually replaces this redundant data with the secret message. This limits the types of data that we can use with steganography.

In practice, there are basically three types of steganographic protocols used. They are *pure steganography*, *secret key steganography* and *public key steganography*. Pure steganography is defined as a steganographic system that does not require the exchange of a cipher such as a stego-key. This method of steganography is the least secure means by which secret communication can be achieved because the sender and receiver can rely only upon the presumption that no other parties are aware of this secret message. Using open systems such as the Internet, we know this is not the case at all. Secret key steganography is defined as a steganographic system that requires the exchange of a secret key (stego-key) prior to communication. Secret key steganography takes a cover message and embeds the secret message inside of it by using a secret key (stego-key). Only the parties who know the secret key can reverse the process and read the secret message [6].

Unlike pure steganography where a perceived invisible communication channel is present, secret key steganography exchanges a stego-key, which makes it more susceptible to interception. The benefit to secret key steganography is even if it is intercepted, only parties who know the secret key can extract the secret message. Public key steganography takes the concepts from public key cryptography as follows: Public key steganography is a steganographic system that uses a public key and a private key to secure the communication between the parties wanting to communicate secretly. The sender will use the public key during the encoding process and only the private key, which has a direct mathematical relationship with the public key, can decipher the secret message. Public key steganography provides a more robust way of implementing a steganographic system because it can utilize a much more robust and researched technology in public key cryptography. It also has multiple levels of security in that unwanted parties must first suspect the use of steganography and then they would have to find a way to crack the algorithm used by the public key system before they could intercept the secret message [6].

IV. Methodology

The main objective of this paper is to design and implement a steganography system which integrates compression and encryption to improve its capacity and security requirements. The steganographic software system designed, allows the encoding and hiding of secret messages in a cover file. The encryption and decryption algorithm implemented is one of the symmetric cryptosystem algorithms called data encryption standard (DES) using java development kit (JDK). This is because java has built in capabilities for encryption and decryption. The lossless compression was also used. Java programming language and Structured Query Language (SQL) were used in achieving the desired objectives of this study. Also, the SSADM – Structured Systems Analysis and Design Methodology was used. The Structured Systems Analysis and Design Method (SSADM) [12] is a system approach to the analysis and design of information systems. SSADM is a waterfall method by which an information System design can be arrived at. SSADM can be thought to represent a pinnacle of the rigorous document-led approach to system design, and contrasts with more contemporary Rapid Application Development methods such as Dynamic Systems Development Method (DSDM).

V. Analysis of Existing System

A multitude of methods and variations have been used in hiding information, as discussed above such as writing text on wax-covered tablets, shaving the head of a messenger and tattoo a message or image on the messenger’s head, hiding of hidden messages in elaborate book covers and paintings and a host of others. The advantages include:

i. They have ability to hide a secret message in the physical object which is being sent thereby ensuring privacy and secrecy.

ii. The cover message is merely a distraction and could be anything depending on the approach being used as long as it could hide the message without giving room to prying eyes.

iii. They are not involving much intelligence and cost when compared to the proposed system.

The secret messages were transmitted using a technique called “null ciphers” meaning that the messages were not encrypted in anyway.

VI. The proposed System

The proposed system aims to improve on the security and speed of operation of stego-system. So the system designed is a highly secured computerized steganographic tool based on three different stages which include Compression-> Encryption-> Encoding. The proposed system is designed and built with reusability and stability in mind and also features a user friendly GUI (Graphical User Interface) interface that allows the user to encode/hide information into a carrier image. With this algorithm, the security of data can be improved and ensured as it is the encrypted text and not the plain text that is embedded in the image. The phases are:

Compress ------------- Encrypt ----------------- Encode

Unlike the existing system which does not have an extra layer of security, the proposed system includes such security as compression, encryption and then encoding.

Figure 1 below shows the model of the system. In this system, the sender's end which is also the embedding side, inputs the data with the image and performs embedding which gives rise to the stego image (hidden or secured data). This stego image is now sent to the hospital server at the server end. The extraction process is now conducted at the receiver's end known as extraction side by extracting the stego image from the server, the extraction process now separates the data from the image

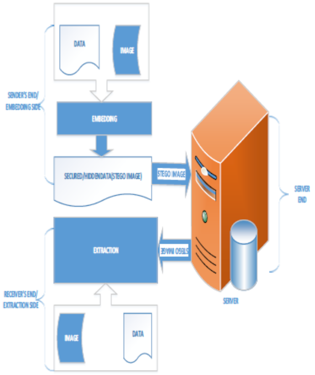


Figure 1: The Proposed Stego Model

The key concept of steganography is the ability to hide and communicate information without the potential risk of detection of the communication. The key concept of steganography is the ability to hide and communicate information without the potential risk of detection of the communication. It is the dark cousin of cryptography, because they both use codes. While cryptography provides privacy, steganography is intended to provide secrecy. Information theory tells us through Kerckhoffs' principle of cryptography [12] that the security of the system should rely only on the secret key material. And this should be the case in any steganography system. This applies to the proposed system also. Simple steganographic techniques have been in use for hundreds of years, but with the increasing use of files in an electronic format, new techniques for information hiding have become possible.

The lossless compression was applied in our stego-software tool, it maintains the original image data exactly; hence it is preferred when the original information must remain intact. Thus, it is better used in steganographic techniques/methods, since the intended receiver needs the message exactly as it is and the carrier image still looks like the original image file. Its major limitation is that its compression rate is not as high as that of lossy compression. Lossless compression format includes BMP, GIF, and PNG [13]. The lossless compression technique/method was used in our proposed system so that the exact message is what the receiver will extract on decompression.

Figure 2 illustrates how the sender who wants to communicate a secret message to a receiver (recipient) first compresses the message and then encrypts it, after which it is then encoded using the LSB technique before it is secretly hidden in a cover medium. The medium which is an image must have sufficient amount of redundant bits, which can be replaced to conceal a secret message. Next, a key called stego-key (a kind of password) is generated. This stego-key is used to randomly select and replace the redundant bits from the cover media in order to hide secret messages.

Redundant bits are defined as those bits in the cover media which if changed will not change the cover media to a great extent. The embedding process hides the secret message using the stego-key. After embedding in finished, the cover media can be transmitted to the receiver. At the receiving end, the receiver, having the proper stego-key or decryption key, can extract the secret message from the cover media.

In this design, a static stego-key is generated and it is not shared between the sender and receiver in the sense that even if the message embedded in the software encoding algorithm of the carrier image is intercepted and the encryption/decryption password is known, it is only with this our software tool which has such encoding algorithm and stego-key that the intruder can use to read/open /extract the original message from the carrier image. So if the intruder tries to open it using other software he/she will not be able to extract the message since he does know the stego key used in the encoding algorithm.

VII. RESULT AND DISCUSSIONS

The system begins with a system loading module also called the splash screen which loads all the software utilities required for the software to work in the computer system the very first time the software is executed. The main menu comprises of different modules and sub modules which were all used together to make the system achieve its goals. The details of each of the modules are shown below: The steganographic software produced has been tested and found to achieve the following:

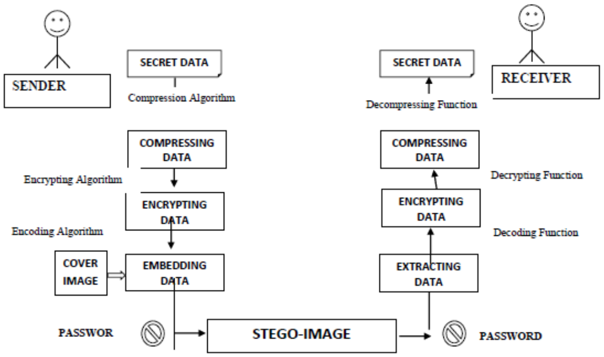


Fig 2: Overall structure of the system design

Confidentiality: the software helps to protect a user's identity or data from being read as such information hidden in the carrier file is hardly noticeable.
Data integrity: This steganography being combined with cryptography helps to protect the hidden data or information from being altered. Example; if a carrier bitmap image is later discovered to be carrying information in it and the information decoded, a decryption key/password will be required to decrypt it to get the information in plain English.

Authentication: this ensures that the origin of a particular data or information is known to the recipient. With steganography combined with cryptography, the authentication of such information is guaranteed.

Use Case Diagram

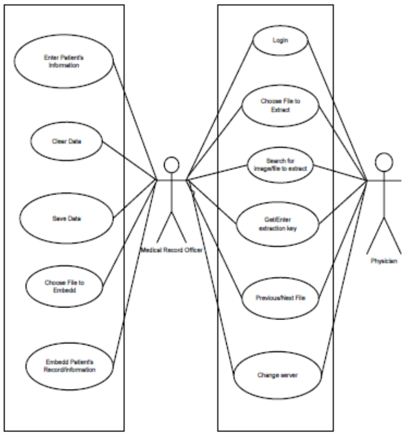


Figure 3: Use case Diagram of the system

This system provides a new approach that will improve quality security of a patient's record. Listed below are some screenshots of results from the system. Figure 6 shows the welcome page of the system when implemented, as the first page when we run the program. It displays the name of the system (embedding and extraction system for Patient's record). Below the welcome screen is a start button which lunches the program to the main menu screen as shown in figure 7. Figure 7 displays the main menu which comprises of the modules used in the application for the embedding and extraction process. The button on the screen includes; embed data, clear data, choose a file to embed, previous, next, extract data, get the key, search and change server, each with its function. In the embedding screen process, the user enters data into the fields and then clicks on the embed data button. In the extraction process, the user browse for the image by using the next or previous button, or search using the search box, then click on Get the key button. The receiver then enters the username and password. By clicking on extract data button, a dialogue box appears requesting the user to enter the key for extraction. When the appropriate key is entered, click OK and the records are extracted and displayed in the fields.

The application is standalone and when the installation process is completed, and the folder copied correctly into the hard disk, an icon is created on the desktop. Now, to start it, double click the icon on your desktop or click on it from the start menu. This will load the installed program/application into the computer's memory and run. Once the application has started running, you see the modules on the screen with the name of the software when the main menu screen appears. The user can then navigate through the menu tabs shown in the main menu. These include, "Embed data", "clear data", "choose a file to embed", "previous" "next", "extract data", "Get the key", "search" and "change server".

Algorithm for the Hiding of a Message

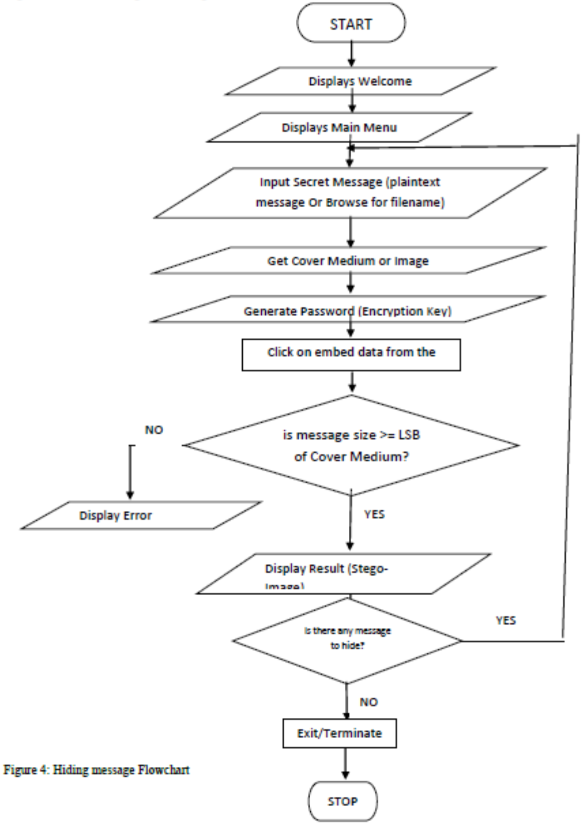

START
Displays Welcome
Displays Main Menu
Input Secret Message (plaintext message Or Browse for filename)
Get Cover Medium or Image
Generate Password (Encryption Key)
Click on embed data from the
NO
is message size >= LSB of Cover Medium?
Display Error
YES
Display Result (Stego-Image)
YES
is there any message to hide?
NO
Exit/Terminate
STOP

Figure 4: Hiding message Flowchart

Algorithm for the Extraction of a Message

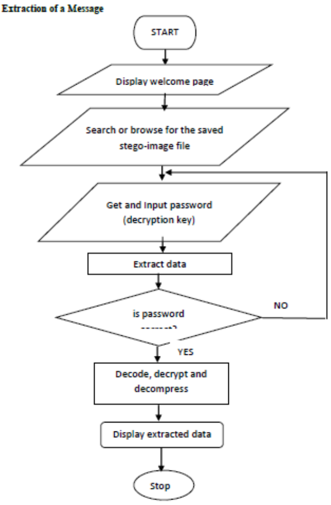
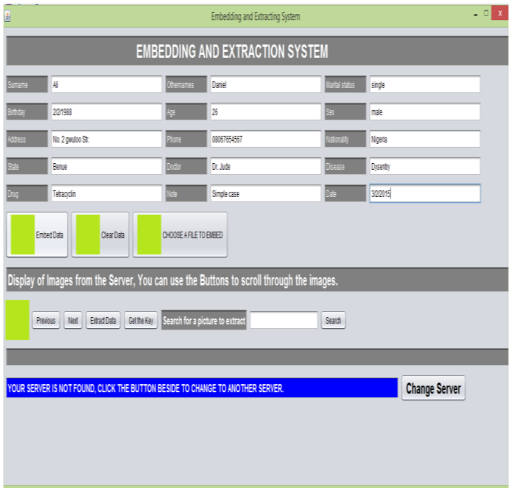

START
Display welcome page
Search or browse for the saved stego-image file
Get and Input password (decryption key)
Extract data
is password correct?
NO
YES
Decode, decrypt and decompress
Display extracted data
Stop

Figure 5: Extracting Message Flow chart

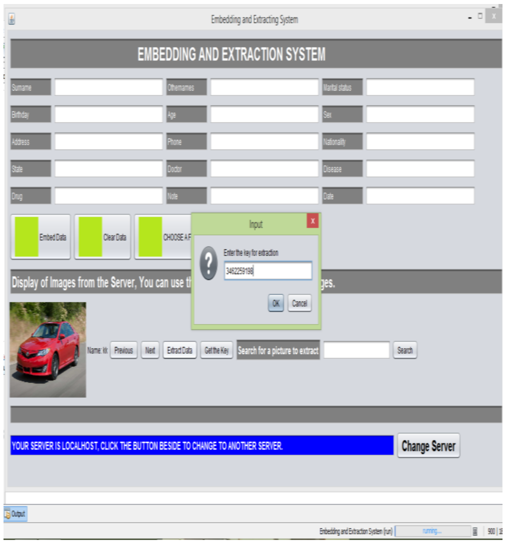


Surname	Ali	Othernames	Daniel	Marital status	single
Birthday	2/2/1988	Age	26	Sex	male
Address	No. 2 gwuloo Str.	Phone	08067654567	Nationality	Nigeria
State	Benue	Doctor	Dr. Jude	Disease	Dysentry
Drug	Tetracyclin	Note	Simple case	Date	3/2/2015

Display of Images from the Server, You can use the Buttons to scroll through the images.

YOUR SERVER IS NOT FOUND, CLICK THE BUTTON BESIDE TO CHANGE TO ANOTHER SERVER.

Figure 6: Showing data embedding process



Display of Images from the Server, You can use th ges.

Enter the key for extraction

3462259198

YOUR SERVER IS LOCALHOST, CLICK THE BUTTON BESIDE TO CHANGE TO ANOTHER SERVER.

Figure 7: Showing data extraction process

To hide a patient's record therefore, the user clicks on the "embed data" button after entering all fields in the patient's record. The other buttons are located next to it by the right of the screen. These buttons can be clicked one after the other. The first button is "embed data", this allows one to hide the record into the existing image files. The next button which is "clear data" is thereby clicked to clear fields, so as to enter the next record, followed by the secret message which can as well be selected from the existing files. This is followed by the choose file to encode button which prompts the user to select the file that he/she wants to hide with the selected image and then it is encrypted with a key and saved in the database server. After this comes the encoded/stego image which is then saved for future use.

The next step is to extract the hidden information from the carrier image. To start the extraction/ retrieval process, the user searches for the image file to extract by entering the name of the image, and then clicks on search button, otherwise he clicks on the previous or next button to fetch the particular image, then clicks on *get the key* button so as to get the key. Finally the user clicks on the extract data button and pastes the key gotten in the dialogue box given, and the message is now extracted from where it was embedded.

Our model is very robust since it combines the strengths of both steganography and cryptography. The combination of Cryptography and Steganography for secure communication is a tool that combines both Cryptography methods and Steganography techniques for secure communication. The application is a cross-platform tool that can effectively hide a message inside a digital image file. In the field of data communication, security is a top priority.

VIII. CONCLUSION

In this research, a window-based application was developed and implemented on java development kit 1.7.0_10 platform that allows a user to encrypt a secret message and hide its content into a cover image file as well as extract and retrieve the original data. Also, cryptography (encryption), compression and steganography techniques were combined and successfully implemented in order to secure a successful steganographic system with different levels of security. This work, satisfies the aim that says steganography is an effective way to obscure data and hide sensitive information. This allows an individual to hide data inside other data with the hope that the transfer medium will be so obscure that no one would ever think to examine the contents of the file. In other words, this work has successfully demonstrated that steganography is effective at securely concealing secret, vital or sensitive messages or information in media files (image file) without altering the cover file noticeably. The outcome of this study is also significant in cyber security as users of the cyberspace can use this application to secure their information from hackers and related cyber criminals. As a final thought, we see vast possibilities for the use of steganography in industrial espionage in the act of getting information out of an organization without anyone being aware. This however, is yet to be seen or reported.

REFERENCES

[1] Alain, C.B. (2001). A study of steganography and Ther Art of Hiding Information. East Carolina University. Retrieved on Feb 15th, 2009 from http://www.stegDTEC682.pdf

[2] Acken, J. (1998). How Watermarking adds Value to Digital content. Communications of the ACM, 41(7), 75-77.

[3] Bender, W. (1996). Techniques for Data Hiding", IBM Systems Journal, 35 (3), 313-336.

[4] Krinn, J. (2000). Introduction to Steganography. Journal of Military Science, in French URL: http://rr.sans.org/convertchannels/steganography.php

[5] Sellars, D. (2010), An Introduction to Steganography, URL: http://www.cs.uct.ac.za/courses/CS400W/NIS/papers 99/dsellars/stego.html, retrieved on 24th June, 2015.

[6] SANS Institute (2002). A Detailed look at Steganographic Techniques and their use in an Open-Systems Environment. InfoSec Reading Room, URL: http://www.sans.org/reading-room/whitepapers/covert/, retrieved on 24th June 2015.

[7] Petitcolas, F.A.P. (2000). Information Hiding: Techniques for Steganography and Digital Watermarking, retrieved on 24th June, 2015 from http://www.petitcolas.net/fabien/steganog raphy

[8] Aelphaeis, M. (2006). Steganography FAQ. http://zone-h.org. Retrieved on Feb 16th, 2009.

[9] Arnold, M., Schnucker, M. and Wolthusen, S.D. (2003). Techniques and Applications of Digital Watermarking and C*ont*ent Protection. Artech House, Norwood, Massachusetts.

[10] Efozia, F.N. (2008). Design and Implementation of a Steganographic software. MSc research work, University of Benin.

[11] Anigbogu, S.O. (2003). Introduction to computer science and programming languages. Christon International Company ltd, Awka, Anambra state.

[12] Kerckhoffs. A. (1883). iLab Cryptographie Militaire (Military Cryptography), Sciences.

[13] Johnson, F. and Jajodia, S. (1998). Exporing Steganography: Seeing the unseen. IEEE Computer Magazine, 31(2), 26-34, February Ed. http://www.jjtc.com/pub/r2026.pdf.