International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 9 – No.4, July 2015 – www.ijais.org

Design and Implementation of a Model for Information Privacy

Akinwale O. Akinwunmi
Department of Computer Science & Information Technology
Bowen University Iwo, Nigeria

Halleluyah O. Aworinde
Department of Computer Science & Information Technology
Bowen University Iwo, Nigeria

Oliseamaka T. Olise
Department of Computer Science & Information Technology)
Bowen University Iwo, Nigeria

ABSTRACT

In the world today, privacy and security of data are requirements so difficult to meet by developers and service providers ; the privacy of users and their data are threatened more and more by government agencies looking to collect as much information as possible for various reasons including security, private companies looking to cash in on the various social connections that people have developed their social graph. A review of the existing works on still image steganography and particularly the method of least significant bit hiding was done. Algorithms for the encoding and retrieval of a message into a bitmap file were designed and an application showcasing the use of steganography coupled with cryptography was developed using Microsoft Visual C ++ . This work therefore, designed and implemented a model for information privacy. The study indicated that steganography combined with cryptography provides both security and privacy for encrypting a message.

General Terms

Information Security

Keywords

Information Privacy, Encryption, Steganography, Cryptography

1. INTRODUCTION

With the advances in Computer networks and communication and expansion in its use in different areas of life and work, the issue of information security has become increasingly important [1]. The desire to have private conversations or to be able to send a message to someone with the assurance that the contents of the message will not be viewed or tampered with by a third party has always been an issue of immense importance [2]. The advent of social networking sites made public all the activities that a user engages in, coupled with the propagation in the wake of terrorist attacks, that those who want their thoughts or messages private are hiding something, the avenues for keeping messages private and free from eavesdroppers, are getting tougher and more difficult by the day.

People have always wanted to keep their words and thoughts secret, hidden from prying eyes and as such, the options available to keep secrets safe are either dismal, or draw unwanted attention to the presence of a locked secret; hence, they introduced an approach for securing and safely hiding things in an unsuspecting manner [3].

Steganography or secret writing like cryptography is a form of preventing third parties from reading or deciphering a message that is written [4]. It is the art and science of communicating in such a way that the presence of a message cannot be detected. It is the method of embedding hidden content in unremarkable cover media so as not to arouse an eavesdropper's suspicion [5]. Steganography has been seen as a useful tool that allows the transmission of covert information over an overt communications channel and as such, the hidden data is both difficult to detect and when combined with known encryption algorithms, equally difficult to decipher [6].

This work therefore is aimed at designing a model for information privacy which addresses the problem of a third party eavesdropping on messages through the application of steganography as security measure.

2. PAST RELATED WORKS

Hiding messages by masking their existence is not a recent innovation; it has been in existence for ages and good examples of such include a Roman General that shaved the head of a slave tattooing a message on his scalp. When the slave's hair grew back, the General dispatched the slave to deliver the hidden message to its intended recipient [7]. In related manner, ancient Greeks covered tablets with wax and used them to write on. The tablets were composed of wooden slabs. A layer of melted wax was poured over the wood and allowed to harden as it dried. Hidden messages could be carved into the wood prior to covering the slab. When the melted wax was poured over the slab, the now concealed message was later revealed by the recipient when they re-melted the wax and poured it from the tablet [8].

In the 20th century, invisible inks were widely used technique for information hiding; during the Second World War, people used milk, vinegar, fruit juices and urine to write secret messages. When heated, these fluids become darker and the message could be read. Much later, the Germans developed a technique called microdots which are photographs with the size of a printed period but have the clarity of a standard type-written page; the microdots are then printed in a letter or on an envelope and being so small, they could be sent unnoticed. However, recently, The United States government claimed that Osama Bin Laden and the al-Qaeda organization use steganography to send messages through websites and newsgroups but not substantiated yet [9].

With the above given historical instances of steganography, it is evident that for a steganographic system's key to be discovered, the security of the system must be irrevocably broken [6].

Steganography which was described as steganographia first appeared in a manuscript by Johannes Trithemius on cryptography; in this, he invented a steganographic cipher in which each letter was represented as a word taken from a succession of columns. The resulting series of words would then turn out to be a legitimate prayer [10].

Steganography has equally been described as the method of hiding message within an object called the cover objects. More recent cases of steganography include using special inks to write hidden messages on bank notes and also the use of digital watermarking and fingerprinting of audio and video for copyright protection [11].

In today's digital world, Steganography and Cryptography are the two major schemes by which information is made secure. Both are intended to protect information from unwanted parties and both Steganography and Cryptography are excellent means by which to accomplish this but neither technology alone is perfect and both can be broken [4]. Due to this fact, experts suggest using both steganography and cryptography to add multiple layers of security the security of classical steganography system relies on secrecy of the data encoding system [12]. Once the encoding system is known, the steganography system is defeated, when coupled together with encryption; the data hidden by steganography becomes that much more secure, guaranteeing that even if the steganographic process is cracked, the message remains secure.

[13]identified quite a number of ways in which steganography is very useful; these ranges from using it to send messages without anyone having knowledge of the existence of the communication. With this, the tendency of sending news and information without being censored and without fear of the messages being intercepted and traced back to you is made possible. Equally, with steganography, storing information on a location is possible and can as well be used to implement watermarking.

Today's steganography systems use multimedia objects like image, audio, video etc as cover media because people often transmit digital images over email or share them through other internet communication application. It is different from protecting the actual content of a message. In simple words, it is the act of hiding information into other information [14].

In implementing steganography, secrets can be hidden inside all sorts of cover information. However, [13] identified that most steganographic utilities nowadays hide information inside images due to the fact that it is easy to implement. With image steganography, an image with a secret message inside can easily be spread over the World Wide Web or in newsgroups. To hide a message inside an image without changing its visible properties, the cover source can be altered in noisy areas with many variations, so less attention will be drawn to the modifications[15]. The most common methods to make alterations involve the use of the Least Significant bit LSB for masking, filtering and transformations on the cover image [16].

Over time and from previous approaches of implementing information privacy, cryptography is used most times of which information or message is converted into cipher-text, which is unreadable except by the person in possession of the decryption key. With cryptography, an attacker or cryptanalyst might not have the decryption key but the presence of unreadable cipher-text can arouse suspicion leading to attacker attempting to decipher the message through brute-force methods or even deleting the message.

In essence, steganography is a practical technique of implementing information privacy such that messages are hidden in a way no one, apart from sender and intended recipient suspects the existence of message.

3. RESEARCH METHODOLOGY

In this work, the approaches of [11,13,16] were combined to address the problem of information privacy. The system being implemented is geared towards addressing limitations and setbacks experienced in securing message inserted into image using the Least Significant Bit insertion method. It is a model for information privacy using still image steganography that will encrypt the message before embedding it. The system will as well be able to retrieve an embedded image, decrypting it before displaying the hidden message. In essence, the model is designed to improve the security of steganographic method used through the use of classic cryptography while showcasing steganography as an ideal model for information privacy.

For the purpose of this work, waterfall model was used due to the fact that it provides a framework for the design and implementation of a model for information privacy as well as enabling the essence of this work to be achieved. Least Significant Bit LSB steganographic method which is a substitution method of embedding hidden messages reinforced with watermarking and cryptography to improve the security of message was implemented. In LSB, each last bit in a byte of image data is used to store a bit of text data making it possible to store 3 bits of text data in an image with 24 bits per pixel. In implementing the model for information privacy, bitmap images, which offers lossless compression of image data was used to include the watermark cover.

The embedding procedure of LSB based steganography is described by the following equation:

$$yi = 2\left|\frac{xi}{2}\right| + mi \qquad (1)$$

Where *mi*, *xi* and *yi* are the *i-th* message bit, and the *i-th* selected pixel value before and after embedding respectively.

Let {Pmx=0, Px=1} denote the distribution of the least significant bits of the cover image and {Pmm=0, Pm=1} denote the distribution of the secret binary message bits.

The message is to be compressed or encrypted before being embedded in order to protect its secrecy [17][1].

In order to improve on existing methods of LSB in the aspect of securing the message embedded into an image, Advanced Encyrption Standard AES encryption provided by the CryptoPP library written by Wei Dao[18][19] was employed; with this, the security of the message is further ensured.

Find below in section 3.1 and 3.2 the respective algorithms for encoding and decoding processes of the model

3.1 Algorithm for Encryption

Begin

Accept a message in form of text input from the user in a text area and embed it.

Encrypt the embedded text and then convert the text input to a byte array.

Open and Load a bitmap image file into a byte array.

Substitute the bits that make up the byte array of the text input for the least significant bits in the image byte array, Save the modified image byte array as a bitmap file with watermark cover.

Else, alert user of none selection of Image

Abort Operation

End

Figure 1 shows the diagrammatic representation encryption process of the model.

3.2 Algorithm for Decryption

Begin

Open and Load a bitmap image file into a byte array.

Substitute the bits that make up the byte array of the image input for the least significant bits in the text byte array,

Save the modified text array as a text file

Retrieve and decrypt the embedded text from a modified image byte array.

Display the retrieved image as message in a text area.

Alert the user of the completion of decoding process

Else, Alert the user of the occurrence of an error in decryption

End

Figure 2 shows the diagrammatic representation decryption process of the model.

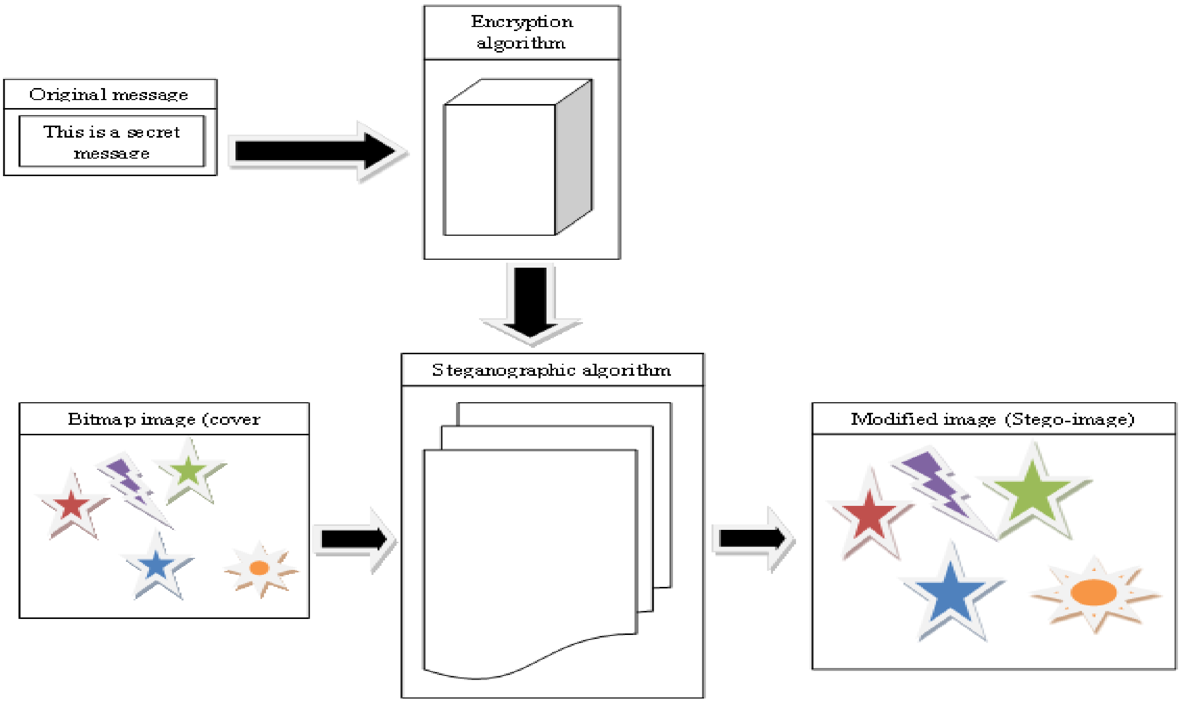


Fig 1: Encryption model of the system

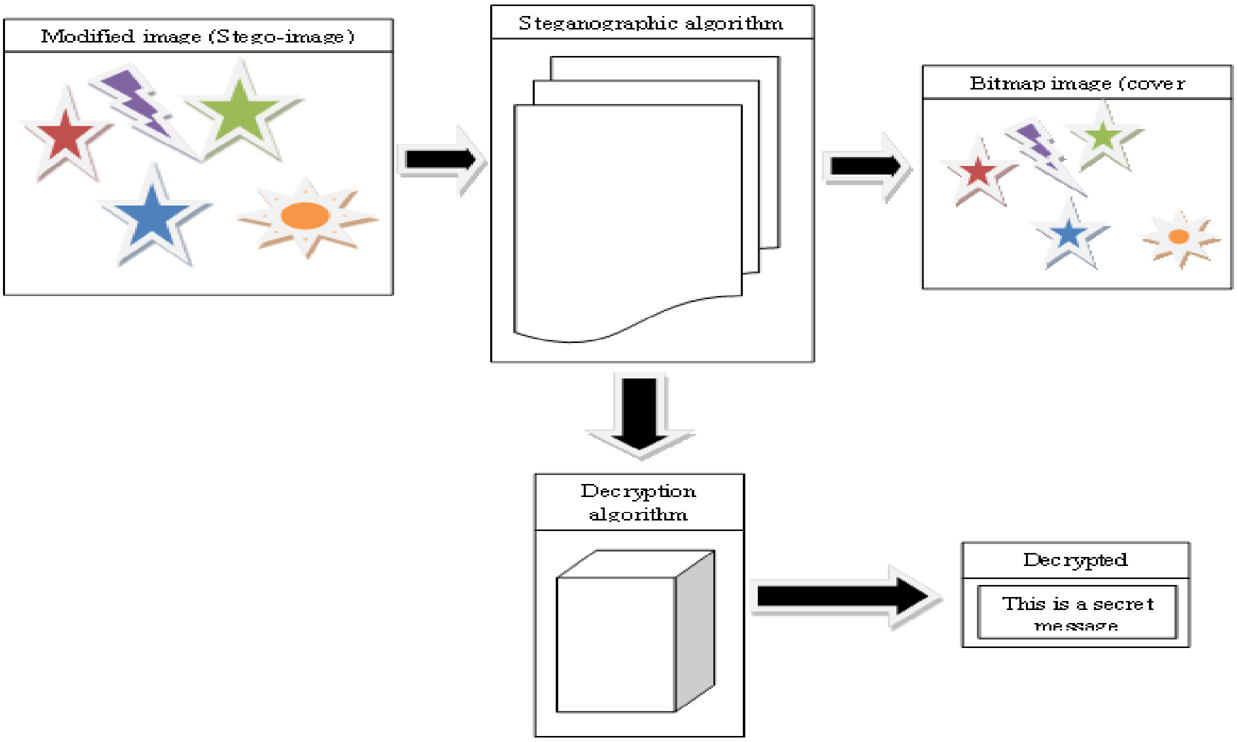


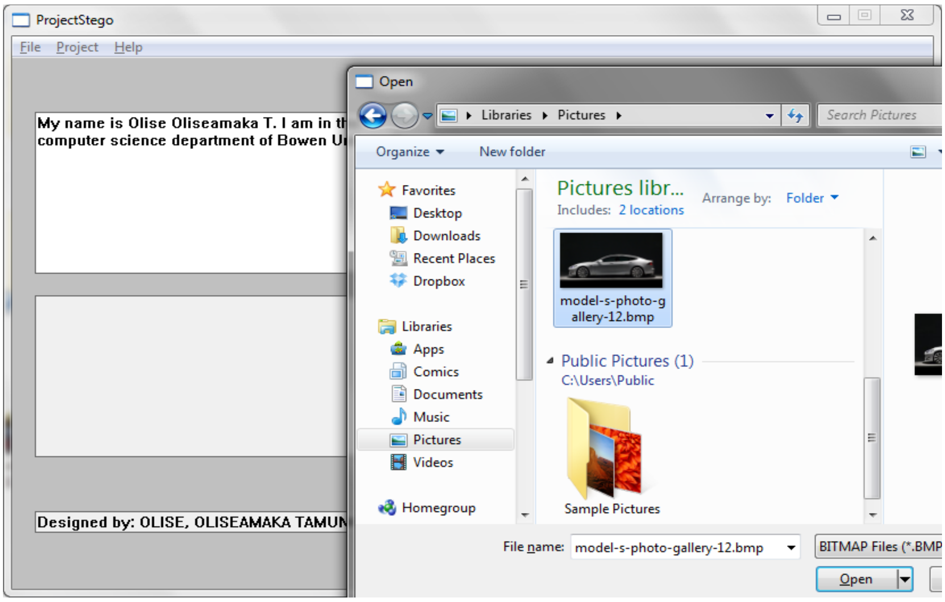
Fig 2: Decryption model of the system

4. RESULTS AND IMPLEMENTATION

This section discusses the implementation and results obtained from the designed model which was carried out LSB method to embed message secretly into bitmap image.

In this section is presented the screen shots showing the working model, its menus, the process of encoding a file and the process of decoding it. On launching the program, the startup screen shown in figure 3 below comes up. In this include a message intended to guide users on how to use the program, thereby explaining the steps to take in encoding and or decoding a message while figure 4 shows the bitmap image file titled model-s-photo-gallery-12.bmp which has been selected. The text to be encoded into this bitmap file is being displayed at the background of the file open dialog box.

Figure 5 shows a message box notifying the user of the successful encrypted of the message while figure 6 presents the selection of a stegoimage with text hidden inside it using the file open dialog box that is launched on clicking the decode button.

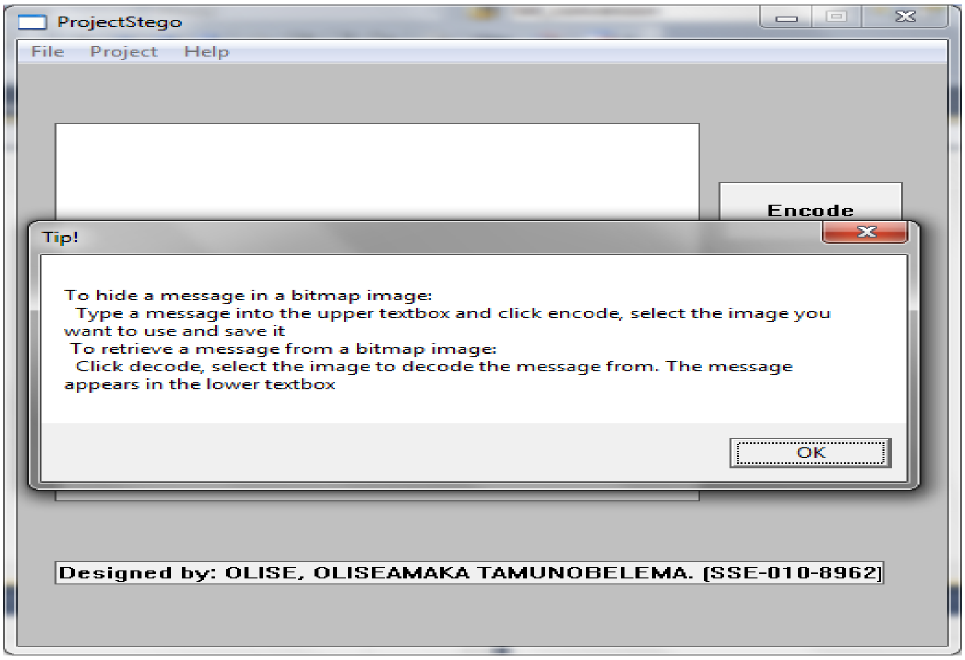


My name is Olise Oliseamaka T. I am in th
computer science department of Bowen U

Designed by: OLISE, OLISEAMAKA TAMUN

File name: model-s-photo-gallery-12.bmp

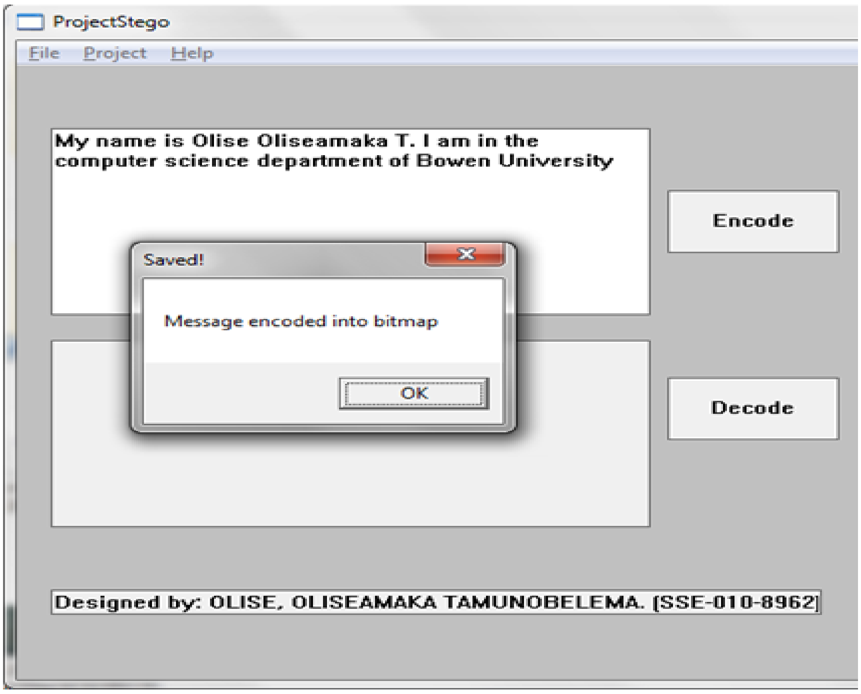
Fig 3: Program startup



To hide a message in a bitmap image:
Type a message into the upper textbox and click encode, select the image you want to use and save it
To retrieve a message from a bitmap image:
Click decode, select the image to decode the message from. The message appears in the lower textbox

Designed by: OLISE, OLISEAMAKA TAMUNOBELEMA. [SSE-010-8962]

Fig 4: Embedding a message

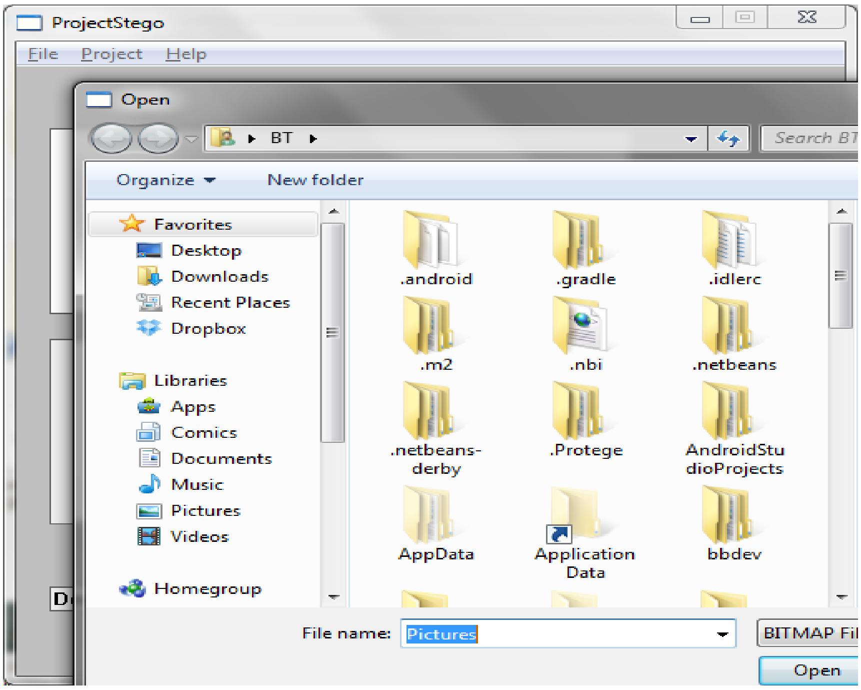


My name is Olise Oliseamaka T. I am in the computer science department of Bowen University

Message encoded into bitmap

Designed by: OLISE, OLISEAMAKA TAMUNOBELEMA. [SSE-010-8962]

Fig 5: Encrypted Message



File name: Pictures

Fig 6: Decrypting Process

5. COMPARATIVE ANALYSIS

Previously, encryption of information is mainly given concern which does not prevent noticing the presence of the content. The designed model brings up an approach whereby still image steganography is utilized to encrypt the message before embedding it using Least Significant Bit LSB and classic cryptography. With cryptography alone, information is covered into cipher-text which is unreadable except by the possession of the decryption key but the message passing is easily known. But the designed model addressed the limitation of previous approach in terms of security of the message embedded into an image using the LSB insertion method and which as a result prevent easy access and damage to the contents of the message. For cryptography, detection is easy but extraction is complex while in steganography, both detection and extraction is complex. In standard LSB steganography, once the presence of a message is suspected by an eavesdropper, it is relatively easy to detect and extract the message. Combining the cryptography and steganography together strengthened the security and privacy of information in passage. Implementing steganography only for information privacy occupies a whole lot of space and size. In order to improve on existing methods of LSB in the aspect of securing the message embedded into an image, Advanced Encryption Standard AES encryption was employed in order to further ensure the security of message and as well overshadow the weakness associated with LSB. With AES, there execution time is faster and less memory is utilized. Using either Cryptography or steganography alone for information privacy makes securing data vulnerable and can easily be broken. Combining Cryptography and Steganography together creates a platform for multi-layer security which enhances the designed model. The image cover alteration in the designed model was achieved with watermark. The security of a watermark provides resistance to hostile attacks. Table 1 gives a summary of the comparative analysis of the previous approach and the designed model.

Table 1: Comparative Analysis of Previous Approach & the Designed Model

Model	Image Cover alteration	Encryption	Decryption	Detection	Extraction	Speed of Execution	Memory Required	Multi-Layer Security	Attack
Existing approach	Involves masking, ,filtering, and transformations	Still image steganography is utilized to encrypt the message before embedding it using LSB	Still image steganography is utilized to decrypt the message after embedding it using LSB	Easy	Complex	Slow	Large	No	Susceptible
Designed approach	Involves masking,, filtering, transformations, and watermarking	Still image steganography is utilized to encrypt the message before embedding it using LSB with Advanced Encryption Standard AES encryption and classic cryptography	Still image steganography is utilized to decrypt the message after embedding it using LSB with Advanced Encryption Standard AES encryption and classic cryptography	Complex	Complex	Fast	Less	Yes	Resistant

6. CONCLUSION

The objective of this project was to design and implement a model for information privacy that can hide and recover text inside an image and as a result, steganography combined with cryptography was used as the means by which the model was implemented in order to further strengthen the security of the model.

Steganography was chosen as the primary method of information privacy while cryptography was used to first encrypt the typed text before embedding it within a bitmap image using steganographic method of LSB.

With this, a working program that models perfectly information privacy was achieved as the application is able to hide a text message into an input area inside a bitmap image as well as retrieve messages encoded into a bitmap image. In essence, a multi-layer security combining both cryptography and steganography from this work is therefore seen as a viable means of ensuring information privacy.

7. REFERENCES

[1] Shamim Ahmed Laskar and Kattamanchi Hemachandran 2012. High Capacity Data Hiding Using LSB Steganography and Encryption. *International Journal of Database Management Systems* pp.57-68

[2] Schneier, B. 2013. The NSA Is Breaking Most Encryption on the Internet. Resilient Systems, Inc Available at https://www.schneier.com/blog/archives/2013/09/the_nsa_is_brea.html

[3] Kirkus Reviews 2013. 301 Industry-First Reviews of fiction, nonfiction and children's & teen May 15, 2013: Volume LXXXI, No 10 Available at: http://issuu.com/kirkus-reviews/docs/kirkus_051513_issue

[4] Dunbar, B. 2002. A Detailed look at Steganographic Techniques and their use in an Open-Systems Environment. *SANS Institute InfoSec Reading Room*.

[5] Abikoye Oluwakemi C., Adewole Kayode S. and Oladipupo Ayotunde J. 2012. Efficient Data Hiding System Using Cryptography and Steganography. *International Journal of Applied Information Systems IJAIS411 pp. 6-11*

[6] Dickman S.D. 2007. An Overview of Steganography. *Department of Computer Science, James Madison University Infosec Techreport*

[7] Provos N. & Honeyman P. 2003. Hide and Seek: An Introduction to Steganography

[8] Herodotus 1996. The Histories, Pengium Classics; Reprint edition

[9] Krenn J.R. 2004. Steganography and Steganalysis

[10] Zeki, A.M., Ibrahim, A.A. and Manaf, A.A. 2012. Steganographic Software: Analysis and Implementation. *International Journal of Computers and Communications.*

[11] Cummins, J., Diskin, P., Lau, S. and Parlett, R. 2004. Steganography and Digital Watermarking. *School of Computer Science, The University of Birmingham.*

[12] Samir, B. K., Debnath, B., Debashis, G., Swamendu, M., & Poulami, D. 2008. A Tutorial Review on Steganography. *IC3*.

[13] Shashikala Channalli and Ajay Jadhav 2009. Steganography An Art of Hiding Data. *International Journal on Computer Science and Engineering*

[14] Mehdi Hussain and Mureed Hussain 2013. A Survey of Image Steganography Techniques

[15] Nameer N. El-Emam 2007. Hiding a Large Amount of Data with High Security Using Steganography Algorithm. *Journal of Computer Science 34 pp.223-232*

[16] Natarajan Meghanathan, Nabendu Chaki, Dhinaharan Nagamalai 2012. Advances in Computer Science and Information Technology. *Proceedings of the Second International Conference, CCSIT 2012 Bangalore, India pp229*

[17] Li B., He J. and Huang J. 2011. A Survey on Image Steganography and Steganalysis. *Journal of Information Hiding and Multimedia Signal Processing* pp. 142-172

[18] Bruce Schneier; John Kelsey; Doug Whiting; David Wagner; Chris Hall; Niels Ferguson; Tadayoshi Kohno et al. May 2000."The Twofish Team's Final Comments on AES Selection"

[19] Kelsey, J. Schneier, B. Wagner, D. Hall C. 1998."Cryptanalytic Attacks on Pseudorandom Number Generators". *Fast Software Encryption, 5th International Proceedings*. http://www.schneier.com/paper-prngs.pdf.

8. AUTHOR'S PROFILE

Akinwale O. Akinwunmi is a PhD holder in Computer Science and lectures at Department of Computer Science and Information Technology Bowen University Iwo Nigeria. His area of research interest among others includes Distributed Computing, Networking and Communication.

Halleluyah O. Aworinde is a MSc. holder in Computer Science from University of Ibadan. He is a staff in The Department of Computer Science & Information Technology at Bowen University, Iwo, Nigeria. His research interest includes Telemedicine, Information Security, Image Processing & Biometrics.

Oliseamaka T. Olise is a graduate from the Department of Computer Science & Information Technology, Bowen University Iwo, Nigeria.