Data Security Using Steganography

AliyuKamalu Babando[1]Bamanga Mahmud Ahmad[2]

[1]Department of Computer Science, Taraba State Polytechnics(kab_babando@tarabapoly.edu.ng)
[2]Computer Science Department, Federal University of Lafia, Nigeria (mabamanga@gmail.com)

Abstract
Steganography is a fascinating topic that is unique from the everyday cryptography and system administration that most of us deal with. Steganography is a type of code that can be used to communicate covertly. We looked into steganography's theoretical and practical limitations. We used the LSB methodology to print out the picture steganography system enhancement to provide a secure communication method. This steganography computer software shows how to use any text format to hide any type of information. The capacity of this application to support any type of text is its crowning achievement. Since prehistoric times, man has yearned for the capacity to converse in a private manner. Steganography isn't just for military or espionage objectives, as evidenced by the recent boom in research into watermarking to safeguard intellectual property. Steganography, like cryptography, will become more important in the future for safe communication in the "digital world."
Keywords: *Encryption, Decryption, Plain Text, Cipher Text, Cryptanalysis, Steganography, Brute Force and Cryptography*

I.   Introduction

Because data transmitted across a network might be accessed by unauthorized users or hackers, network security is one of the most difficult issues facing the globe today. As a result, a method to improve network security must be devised. As a result, communications can be secretly conveyed via digital media and subsequently transported over the internet using steganography techniques. Unauthorized access can be advantageous since a large portion of the information obtained from a system is in a format that they can read and analyze. Unauthorized access can be used to reveal information to others, to falsely represent an individual or organization, or to make an attempt. One solution to this difficulty is to use steganography (Spagnoletti, 1995). Improvisation and transposition encryption are the building blocks of known cryptography techniques. A transposition cipher conceals data by rearranging message characters. In a transposition cipher, the plaintext remains unchanged, but the character layout is scrambled. A frequency study of the cipher text demonstrates that each letter is not identical in this approach. In an improvisation cipher, each character in the plaintext is improvised for another character in the encrypted text. An improvisation cipher is an encryption method that only uses improvisation changes. Dispersing and misunderstanding are two other methods for hiding the excessive in a plaintext communication that are related to exchanging and imprecision. Dispersing dissipates the plaintext's surplus by distributing it over the encrypted text. The simplest way to cause dispersal is to exchange. A misunderstanding obscured the relationship between the plaintext and the encrypted text. The simplest way to accomplish this is through improvisation. The proposed method makes use of the improvisation encryption process. An interchanging cipher changes the letter ordering, but an improvisation cipher replaces letters with other letters to render the message unintelligible. The improvisation cipher algorithm offsets the alphabet, with the key being the number of letters offset. To recover the plaintext, the receiver reverses the cipher text's improvisation. Russell (2008; Russell, 2008; Russell, 2008; Russell, 2008; Russell, 2008; Russell, 2008; Russell, 2008; Russell, 2008; Russell, 2008; Russell, 2008; Russell, 2008

Steganography is a technique for hiding data in digital media. In contrast to cryptography, the purpose is to keep individuals from discovering the hidden information, rather than from believing it exists. In the digital era, data is at the heart of computer communication and the global economy. The concept of data concealment has inspired people to devise imaginative methods to prevent data from falling into the wrong hands in order to ensure data security. Without faults or interruptions, digital data can be transmitted from one point to another via computer networks. The availability of digital media has raised concerns about material being hacked and modified by unauthorized parties over time. Digital material's quality and information can be duplicated without loss. As a result, it poses a substantial risk to data security and the intellectual property rights of copyright holders.

The Internet is used for communication as well as information dissemination to the general population. The necessity to hide hidden messages in various multimedia and communicate securely over the Internet has grown as the Internet develops around the world. Every day, the variety of strategies for concealing information grows, with a more sophisticated approach. Text, images, audio, and video are all examples of digital media that can be used for covert communication and act as excellent carriers of hidden information. As data transfer over computer networks has evolved, information security has become a critical issue. Data confidentiality and integrity are thus essential to safeguard data from illegal access and usage. Encryption and steganography are two distinct forms of data hiding techniques that provide data confidentiality and integrity. The steganography technique's purpose is to convey a message across a channel that is already carrying other data. The goal of steganography is to conceal messages within other "harmless" digital data in such a way that no one can detect their presence. Steganography's primary goal is to communicate securely in such a way that the transfer of secret data does not raise suspicion (Rajyaguru, 2012).

Through encryption, the contents of a secret communication are hidden from an unauthorized individual, but the message's substance is visible. The structure of a message is scrambled in cryptography such that it becomes meaningless and unintelligible. Cryptography, in essence, allows people to transfer information to one another in a way that prohibits a third party from accessing it (Ajit and Swati, 2013)

Steganography is becoming increasingly important as more individuals join the online revolution. Steganography is the art of hiding information so that hidden messages are not found. Stereography is a collection of covert communication techniques that prevent the message from being seen or heard. As a result of advancements in ICT, the majority of information is now kept electronically. As a result, information security has become a top priority. In addition to cryptography, steganography can be used to protect data. In cryptography, the message or encrypted message is implanted in a digital host before being transferred across the network, so the message's existence is unknown. In addition to data secrecy, this method for information hiding can be extended to copyright protection for digital assets such as audio, video, and photos. Modern communications' growing capabilities necessitate the employment of specific security measures, notably on computer networks. As the volume of data exchanged over the internet increases, network security becomes increasingly important. As a result, data security and integrity must be protected against unauthorized access and use. As a result, interest in information concealment has skyrocketed. Information hiding is a new topic of study that encompasses applications such as digital asset copyright protection (Sumedha et al, 2012).

II.   Methodology

2.1 Fact Finding Technique Used
Different methods were utilized to determine the requirements for the proposed system, but after considering some facts, the following fact was used:
1.   Observation: This is a method of data collection in which a researcher pays a visit to an event and obtains information on the procedure and outcome. As the saying goes, seeing is believing.
2.   Record inspection: This is a means of examining and dealing with the organization's publishing data as well as other documented material, searching for and gathering essential information.

2.2 Manual Process of Existing System
The advantages processes of the new system are as follow:
i.   In the organization, the new current system has been designed to provide user protection.
ii.   The interactive method can be completed by the computer in a matter of seconds.
iii.   It is possible to acquire precise security.
iv.   Access to a new system that allows you to safeguard your document by preventing it from being found.
v.   The new or existing system can provide you with quick and easy access to secure your data from any location.

Investigation of the Existing System
To encrypt and decrypt data, an encryption program employs encryption techniques. Encryption techniques generate a unique string of data for use as an encryption key, which is made up of a long string of bits or binary numbers. The more bits in the key, the more binary number combinations are conceivable, making the codes more difficult to crack. Then, in symmetric encryption, encryption algorithms scramble data by mixing bits, and the same key is used to scramble (encrypt) and unscramble (decrypt) data.

Disadvantages of the Existing System
Due to flaws in the current system, this research chapter will discuss the problem of encryption in the current system.

Password Forgotten: If you forget your password, you won't be able to decrypt or unscramble the data you've encrypted under the current system.

Lack of Backup: If you forget your password and don't have a backup copy of your data, you won't be able to access it again.

Strength of the Proposed System

Several cryptographic algorithms have been developed during the last year and are now employed in a variety of protocols and functions. Cryptography is not a static field. It has been made possible by steady developments in computing and cryptanalysis technology. Adoption of newer, more powerful algorithms as well as larger key sizes is required. To maintain backward compatibility and interoperability, older algorithms are supported in the present version. Some older algorithms and key sizes, on the other hand, no longer provide appropriate protection against new threats and should be replaced. Algorithms designated as to avoid do not provide adequate security against modern threats and should not be used to secure sensitive data.

Software Development Life Cycle Model

A software life cycle model (also known as a process model) is a visual depiction of the software development life cycle. A life cycle model depicts all of the steps that must be completed in order for a software product to progress through its life cycle phases. It also specifies the sequence in which these tasks should be completed. A life cycle model, in other words, depicts the many actions carried out on a software product from conception through retirement. The basic development activities may be mapped to phases in various ways by different life cycle models. As a result, no matter which life cycle model is used, the basic activities are included in all of them, even though the activities are carried out in various orders in each model. More than one activity can be carried out during any phase of the life cycle.

Development Process

During the development of this system, an evolutionary model was used. The evolutionary model is also known as the incremental model or successive versions model. Initially, a rudimentary functioning model is constructed. Following that, it undergoes functional upgrades, and we continue to add additional functionalities until the desired system is completed.

Application

i.   Comprehensive studies in which modules for gradual implementation are readily available. When a consumer wants to start using the essential capabilities right away rather than waiting for the whole package, this is a common scenario.

ii.   Also utilized in the creation of object-oriented software because the system may be easily divided into units in terms of objects.

Advantage

i.   The user is given the opportunity to test a partially created system. Because the fundamental components are properly tested, there are fewer errors.

Disadvantage

It's tough to partition the problem into various versions that the client would accept and that can be implemented and supplied incrementally.

Evolutionary Model

It's also known as the incremental model or successive versions model. Initially, a rudimentary functioning model is constructed. Following that, it undergoes functional upgrades, and we continue to add additional functionalities until the desired system is completed.
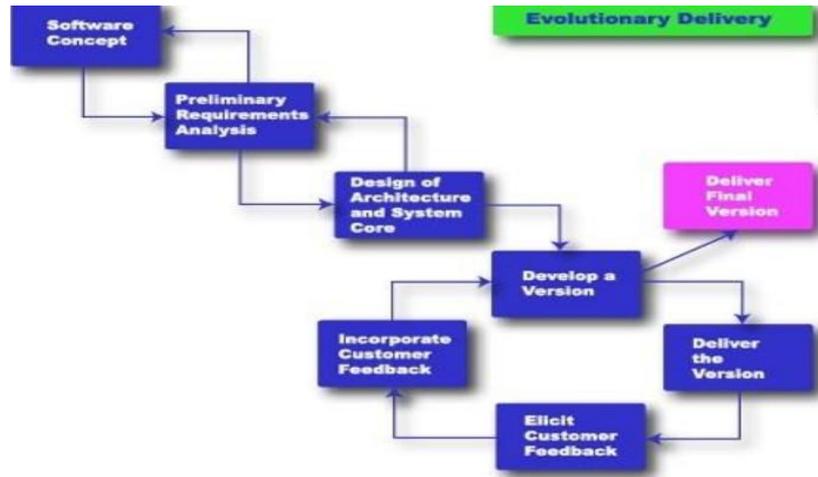
Fig1. Evolutionary Model

Tools for System Analysis and Design
In order to create a system that meets the user's needs. The system design is something you'll have to give. A system is a collection of interconnected components that work together to complete a goal. A system is defined as a collection of interconnected elements that work together to achieve a common goal by receiving inputs and creating outputs in a well-organized transformation process.
Input Design: This refers to the format and types of data that will be entered by the user when the software is run. In terms of the research work's practical aspects.
The format and types of data intended as output when the program is performed are referred to as output design.
Diagrams in UML: UML allows you to create nine different sorts of diagrams to represent five different perspectives on a system. The multiple UML diagrams provide different perspectives of the software system to be produced and assist a full knowledge of the system, just as a building can be depicted from several views (or perspectives) such as ventilation, electrical, lighting, heating, and so on. Such models can be refined to obtain the system's actual implementation.
Two (2) UML diagrams were used in this suggested system:
i.   **Use Case Diagram:** Any system's use case model is made up of a set of "use cases." Use cases, on the surface, reflect the various ways in which users can interact with a system. Asking the question, "What can users do with the system?" is an easy technique to find all of a system's use cases.
ii.   **Activity Chart:** A state chart diagram is typically used to model how an object's state changes over time. State chart diagrams are useful for describing how an object's behavior changes over the course of numerous use case executions.
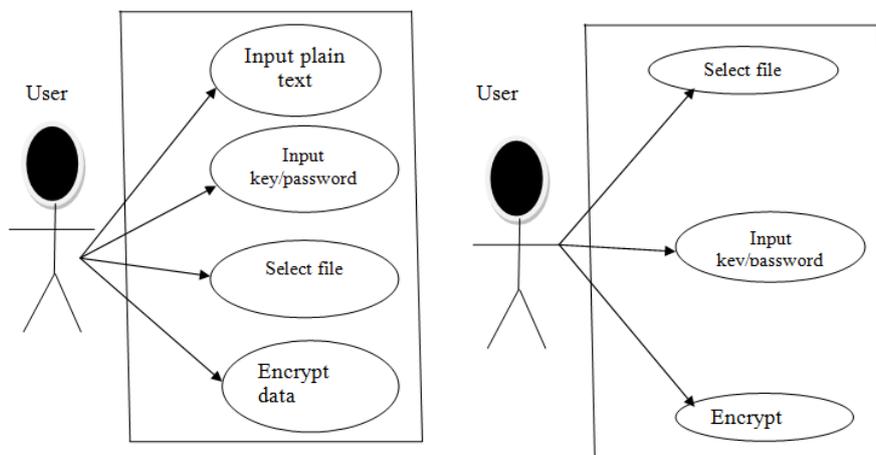
Fig. 2 Use Case UML Diagram
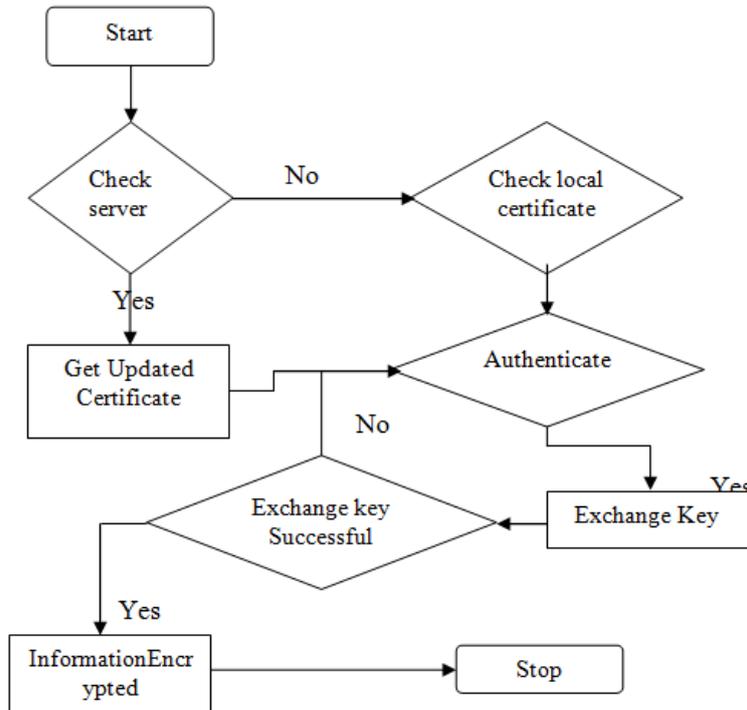
Fig. 3 State UML Diagram: Guide that monitors the action to be taken after each stage

Advantages of the new System
Based on the instructions supplied to it, a computer can make decisions on a vast number of data faster than a human can. A Computer also generates results that are reliable and efficiently complete tasks.
Large amounts of data are kept in computer memory, which allows it to do tasks at a faster rate than a human, reducing the chance of error. System Documentation: In order for the research to be user-friendly, system documentation is required. The research is straightforward and user-friendly, as well as simple to use. The importance of programmer effort in delivering a finished program cannot be overstated.

Documentation for the program: It is critical that a program be maintainable once it has completed its computation. As a result, it is critical that the program be documented, with explanations of what each component of the program performs, so that other programmers or analysts can make appropriate changes or enhancements as needed.

User Documentation: The user documentation is intended to assist the system's user in operating the system by providing the following information in the manual: The user will be able to properly use the system if they:
i.   By connecting the stabilizer plug to the wall socket
ii.   Connect the UPS plug to the stabilizer
iii.   Connect the system to the UPS
iv.   Press the ON bottom of the system whether is serial parallel.
v.   Allow the system to boot
vi.   Slot in the disk to the CD ROM
vii.   Click on start
viii.   Select program
ix.   Install the wamp server
x.   Goto the browser and type the address of the research
xi.   The research will ask to enter your account, if not then register as a new user.
xii.   When finish, simply exist the program
xiii.   Switch off the wamp server
Then shut down the system.

Software Requirement
You must meet the following software requirements in order for this program to function properly.
i.   Window operating system
ii.   Wamp server

Hardware Requirement

In addition, the following hardware requirements are required for this software to function properly.

i.   A hard disk of at least 20GB
ii.   At least 25MB of RAM
iii.   A Pentium processor (II-M)
iv.   A board with speed of not less than 960MHZ
v.   A high resolution of monitor

Implementation

A system can only be implemented when it has been thoroughly tested and determined to be satisfactory. The act of bringing a new system into a functional order or state is referred to as system implementation. In this method, a parallel changeover strategy is recommended, in which the old and new systems are operated simultaneously for a period of time. The new gradually replaces the old, but if the new fails to perform its function, the old can take its place.

III.   Discussion

This section analyzes and summarizes the results of the encryption and decryption techniques. An oral interview was done to discuss the impact and the issue of sending messages via the internet.

This study is concerned with evaluating results with record-facts in an appropriate method to illustrate the logical structure of a message in order to better understand its purpose. This goal is to ensure that every component is evaluated critically and that fear alternatives are developed.

The research work believes the objectives to be met in a satisfactory manner.

i. Economic
ii. Specialization
iii. Simplification and standardization being practiced

IV.   Findings

The result of the researcher's analysis of the existing system is referred to as a finding. It assists the researcher in practically examining the system and proposing a better and more suitable manner of documenting the study's aim. Without studying these findings, a researcher will struggle to know what to do next. As a result of this discovery, the data was lost and a backup file was created.

The following are some of the benefits:

i.   *Speed: -* in terms of speed computer can perform in Nano second task that would take the average human being year to compute
ii.   *Accuracy: - it* maintains as very high degree of accuracy
iii.   *Reliability: -* computer are also widely used because of their reliability and dependability.
iv.   *Storage: -* the ability of the computer to store large amount of data information in a disk
v.   It is economical, it prevents loss of data, since there is security and Information record and finding become very easy.

4.1 User Authentication (Login Page)

Fig 4 shows the page that will be displayed while visiting the system. If you are a new user, you must click on register to create a new account with the system so that you can have access to the system; for example, a user can login to the system by providing a valid "Username" and "Password" before pressing the login button for the system to open for other functions; if you are a new user, you must click on register to create a new account with the system so that you can have access to the system; for example, a user can (i.e. encrypt new file, decrypt the encrypted file and logout).
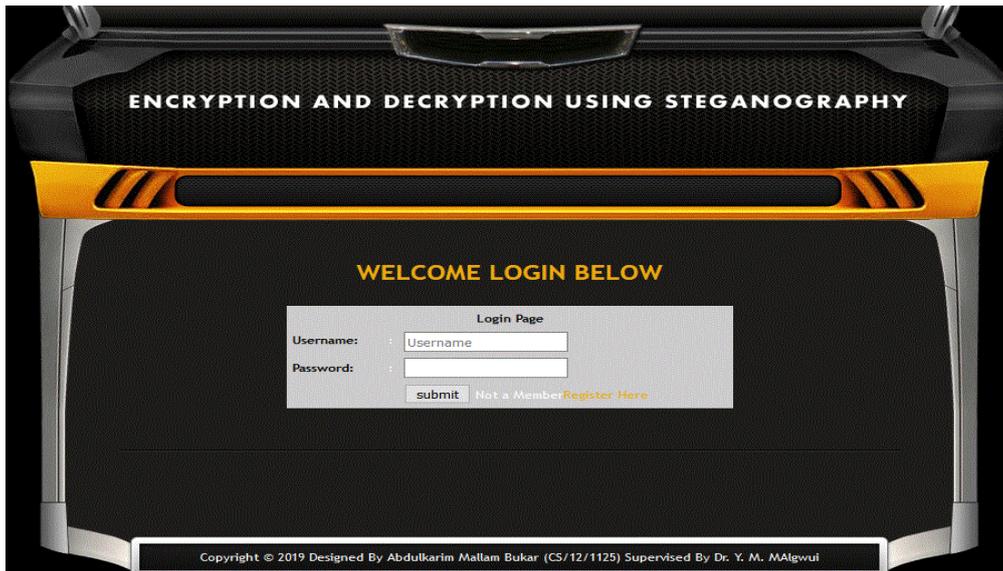
Fig.4 Login Page

4.2   Registration Process
          Simply click the register button on the Home page to register as a new user, and the registration form opens, as illustrated in Fig. 4.2. The user is expected to fill out all of the essential information in the registration page, enter your data, and click on the submit button before clicking on the Home page icon on the left side of the page. A user must input his username and password before clicking the login button to gain access to the system.
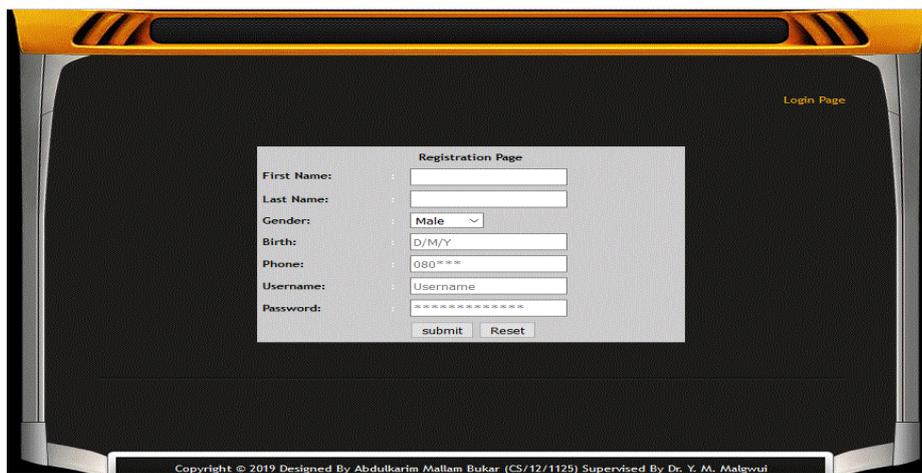
Fig. 5 Registration Form

4.3   Home Page
          After entering your username and password, the system will direct you to this page (Home Page), from which you can navigate to any location inside the system, as illustrated on the page "Home, How It Works, Encrypted File, Contact Us, and Encrypt New File."
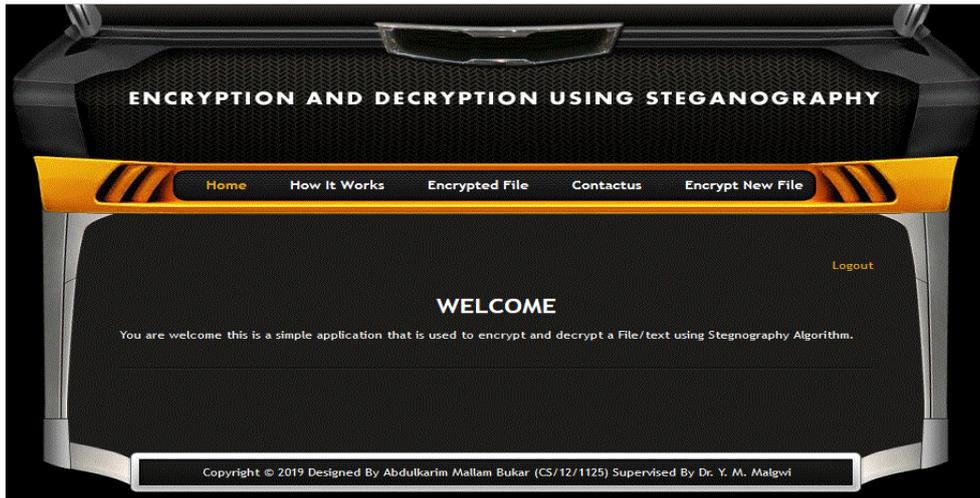
Fig. 6 Home Page

V.   Encrypted File

When you click on encrypted file, you'll see that all of the files were encrypted, including the date, username, and subject, to remember you what was encrypted. When you click on read file, a dialogue box will emerge, asking for your password to decode the encrypted file.
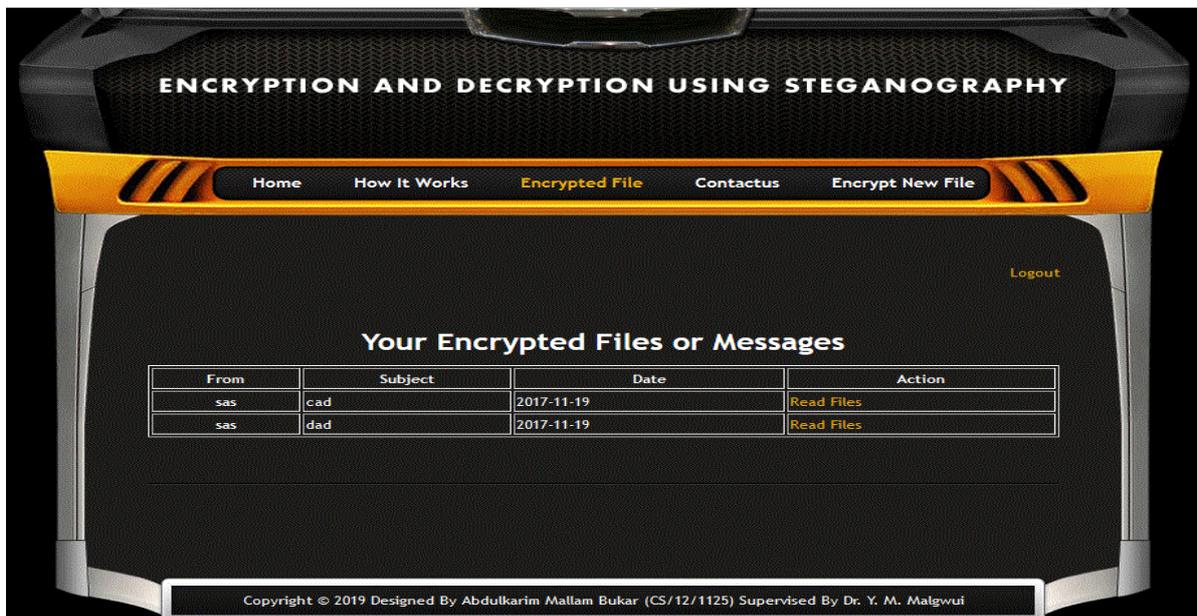
Fig. 7 Encrypted File Page

VI.   Encrypt New File

When a user wants to encrypt a new file, he should click on it. A dialogue box will appear, prompting you to fill out all of the required information, including the username and password, before clicking the submit button.
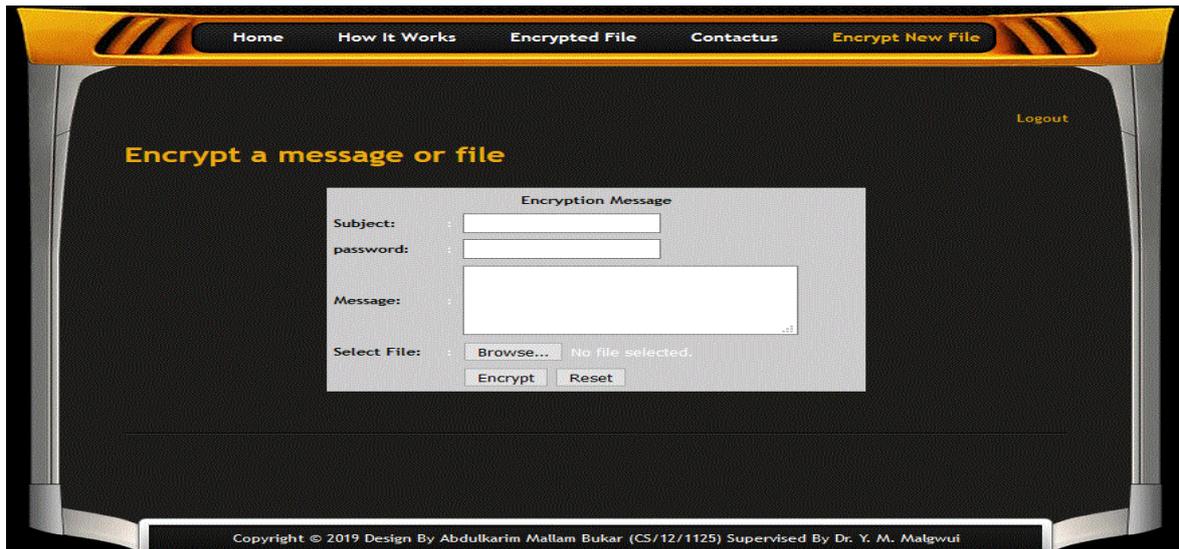
Fig. 8 Encrypt New File Page

VII.   Conclusion

Steganography is a fascinating topic that lies outside of the usual realms of cryptography and system administration that most of us deal with on a daily basis. Steganography can be used to communicate invisibly. We've looked at the theoretical and practical constraints of steganography. To provide a means of secure communication, we printed out the enhancement of the picture steganography system utilizing the LSB approach.

This steganography software is designed to show you how to use any type of text format to hide any type of information within it. This application's masterwork is its ability to support any sort of text.

The ability to communicate discreetly has piqued man's interest since the dawn of time. Steganography isn't simply for military or espionage purposes, as evidenced by the current growth of research in watermarking to protect intellectual property. Steganography, like encryption, will play a larger role in secure communication in the "digital world" in the future.

Comparing the projected outcome with the result produced from the developed system, as well as the benefits of the new system vs the manual system. It can be inferred that the research's goals and objectives have been met.

References

[1].   Ajit, S. and Malik, S (2013) "*Securing Data by Using Cryptography withSteganography*", International Journal of Advanced Research in Computer Science andSoftware Engineering Volume 3, Issue 5.

[2].   Bairai, A. K., (2011) "*ASCII based Even-Odd Cryptography with Gray code and Image Steganography*": A dimension in Data Security, Vol.01, No.2, pp 37-41.

[3].   Bolton, R. (2002). Statistical Fraud Detection: *Review, Statistical Science*, 17 (3), pp. 235-255.

[4].   Barthe, E. (2006) "*encryption and watermarking Publicity Campaigns* "Department of Justice, p.9

[5].   Clark, R.V. (1997). "*Situational crime and steganography technique".* 2nd edition, New York: harrow and Heston, pp2

[6].   Hart G.W, (1994.) "*To Decode Short Cryptograms*" Communications of the ACM, Vol. 37, No. 9, pp. 102108,

[7].   Kharrazi M, Sencar H. T. and Memon N, (2006) "*Performancestudy of common image steganography and steganalysis techniques*", Journal of Electronic Imaging, SPIE Proceedings Vol. 5681.15(4), 041104 (Oct–Dec 2006). SPIE and IS&T

[8].   Kaur M., S., Gupta, Sandhu P. S. and Kaur, J. (2010) "A Dynamic RGB Intensity Based Steganography Scheme", World Academy of Science, Engineering and Technology 67, pp 833 836.

[9].   Monisha, A. F. (2010) "*A Novel Steganography-Cryptography System*", Proceedings of the World Congress on Engineering and Computer Science, USA, Vol. I, October, 2010, ISSN: 2078-0966.

[10].   Sumedha K. and Singhal, A. (2012) "*Network Security Using Cryptographic Techniques*", International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 12

[11].   Ravi, and Knight K, S. (2009) "*Attacking Letter Substitution Ciphers with IntegerProgramming*", Taylor & Francis, Cryptologia, Vol.33, No.4, pp.321-334

[12].   Li X. and Wang J, (2007) "*A steganographic method based upon JPEG and particle swarm optimization algorithm*", Information Sciences 177 (15) 3099–31091.

[13].   Russell, K. M. and Ahmed, H. D. (2008) "*An Implementation of the Blowfish Cryptosystem*", IEEE conference.

[14].   Rajyaguru, M. H. (2012) Combination of Cryptography and Steganography with Rapidly Changing Keys, "*International Journal of Emerging Technology and Advanced Engineering*", Vol.2, No.10, pp 329-332.

[15].   Pia S. and Prof. Karamjeet S. (2013) *"Image Encryption and Decryption using Blowfish Algorithm in Mat lab"*, International Journal of Scientific & Engineering Research, Volume 4, Issue 7.

[16].   Sharma, M., Gaonkar, C. S., Kamar and Gupta, A. (2012) "*A Novel Approach of Image Encryption and Decryption by using partition and Scanning Pattern*", International Journal of Engineering Research & Technology (IJERT), Vol. 1, Issue 7

[17]. Spagnoletti, P. (1995) "*situational encryption and decryption and Cyber-Crime Investigation",* the online pedo-pornography case study, eurocon.

[18]. Ulutas, G. M. and Nabiyev V. (2011) "*Distortion free geometry based secret massage sharing*", Elsevier Inc, Procedia Computer Science, Vol.3, pp.721–726.

[19]. Watson A. B, (1994) "*Image Compression Using the Discrete Cosine Transform*", Mathematical Journal, 4(1), pp. 81-88.

[20]. Willson, R. (2006). "*System design and implementation of Employee Computer Crime in the Organizational Context*". information and organization, vol. 16, p304-324

[21]. Zaidan, A., Zaidan, A. K., Al-Frajat and Jalab, H. A. (2010) "*On the Differences between Hiding Information and Cryptography Techniques: An Overview*", Journal of Applied Sciences, Vol.10, No.15, pp.1650-165