https://dx.doi.org/10.4314/dujopas.v8i3b.1
ISSN (Print): 2476-8316
ISSN (Online): 2635-3490
Dutse Journal of Pure and Applied Sciences (DUJOPAS), *Vol. 8 No. 3b September 2022*

Secure Document and Image Transmission Through an Encrypted Network System

Mansur Aliyu, Onyia Franklin Nonso, Anas Abdullahi, Umar Sani, Zahriya L. Hassan
Department of Computer Science,
Sokoto State University,
Sokoto, Nigeria.

Department of Computer Science,
National Open University of Nigeria

Email: mansur.aliyu@ssu.edu.ng

Abstract
Data communication and networks as a field gives high priority to data and network security. Presently, internet security issues have become very critical in sharing information. Perhaps, there is need for robust techniques for the protection of data shared via unsecured network channels. Since cryptography is a technique for securing plain text messages such as encrypted key exchange and authentication but reveals when and where communication is taking place, while steganography hides the existence of data to be transmitted. Thus, there is need for a tool that combines these two techniques in a single data transmission. As such, this paper intends to develop an application that combines both features of cryptography and steganography techniques for secure communication. The application is a cross-platform tool that can effectively hide information in many different carrier file formats such as image, audio or digital video file. The study adopt the requirements of Advanced Encryption Standard (AES) and Least Significant Bit (*LSB) algorithm in order to come up with best technique that is more robust in securing confidential documents and images. The developed App accepts different file formats when hiding plaintext, messages, and images. The App is recommended to government security agencies, financial institutions, e-commerce websites/app, educational bodies, and individuals in sending personal data online.*

Keywords: Secure Document, Image Transmission, Encryption, Network System

INTRODUCTION

The speedy growth of network technology makes the security of data and information over Internet a critical issue. Nowadays, wireless technology becomes a dominant way of communication. Sending and receiving pictures via wireless network is predominantly popular (Bansal & Badal, 2022). Despite wireless communication medium has a small bandwidth size and vulnerable to intruders. Therefore, extra level of secured data transmission is needed to ensure wireless network becomes more secured and reliable. The digitally transmitted image can be meddled with, interrupted, and damaged criminally by hackers, the images can be encrypted before transmitting them over a network so that hackers and attackers are denied access (Anas & Bagiwa, 2020).

**Author for Correspondence*

Computers and the Internet are the major media connecting different parts of this modern global virtual world (Cheltha *et al.,* 2022). Therefore, if the sensitive data regularly sent is kept confidential to the destination, people can easily exchange a lot of information from any distance within seconds. With the proliferation of attacks recorded during the exchange of electronic information, more robust methods are needed to protect data transmission (Anas *et al.,* 2022). The problem of insecure communication is exacerbated by the fact that much of the data is sent over the open Internet and can be processed by third parties such as email and instant messaging. In order to address this problem, an encryption and steganography techniques need to be developed in order to enhance security by integrating encryption and steganography into one system.

The advancement of Information Technology in the 21st century has made business customer relationships easier and friendlier. In e-commerce business, buying and selling of products or properties are mainly conducted over the Internet, which includes procurement of materials, receiving orders, processing of exchange, payment online, delivery services, authentication, inventory control, shipment services, and customer care. E-security threats, cyber-crimes, and secrecy of transactions have been major issue, which needs an everlasting solution in day-to-day businesses without loss of confidential documents during transactions. In related challenges, most internet users send documents via email in an encrypted network, but hackers or attackers still penetrate as a man-in-the-middle attack and hack the information through a different process (Anas & Bagiwa, 2020). Therefore, it is a big challenge for marketers to convince their consumers regarding their security concerns, through finding solutions to e-security threats, cyber-crimes, frauds, and thefts.

Furthermore, the cloud-based services, file storage, and archiving has become the order of the day in the information technology for storage of documents and imaging services over the Internet server managed by cloud-computing providers. Concerning this option of storage, which has increased the numbers of people exploring, and running their cloud service using products like; Google Drive, Microsoft One Drive, media fire, Dropbox, SharePoint, and iCloud. etc. A lot of risks are involved while transmitting data to the cloud base. It required data security for secure documents and images transmitting via a network.

The importance of computer networks protection has extended every day as the dimensions of information transferred over the Internet. This drives the researchers to explore many forms of studies to enhance the ability to solve network security problems. An approach to this issue is to mix the advantage of cryptography and steganography in a single scheme. Many researches devised wonderful strategies for combining cryptography with steganography techniques in a single scheme (Cheltha *et al.,* 2022). In some latest studies, many techniques had been combined in a mixture of steganography and cryptography with a comparative analysis. The comparative analysis has been applied primarily at the necessities of Internet security protection i.e. authentication, confidentiality, and robustness (Anas *et al.,* 2022).

In one of the studies, the encrypting method through combining cryptography and steganography strategies to cover the information was designed. In the cryptography process, a powerful method for data encryption was used as one's supplement approach, that's known as SCMACS (Cheltha *et al.,* 2022). It uses a symmetric key approach wherein each the sender and receiver were given an identical key for encryption and decryption. In the steganography part, the LSB approach was used and maximally preferred. Other studies developed a fairly secured steganography method through combining DNA collection with hyper-elliptic curve cryptography (Das & Baykara, 2019). This method takes control of each technique to offer an excessive and stable communication network, which uses the advantages of each DNA

cryptography and Steganography. The set of rules (in algorithm) attempts to cover a mystery photograph in some other cowl photograph through changing them into DNA sequences using the nucleotide to the binary transformation table.

In isolation, cryptography and steganography are not sufficient be used for the transmission of information due to the fact of their independent weaknesses (Cheltha *et al.,* 2022). Therefore, this study proposed a new system whereby both techniques are used collectively to create an almost not possible manner for third-party to breach the system and get access to unauthorized information. The system used the modern two-fish algorithms for encryption whilst a brand new technique for applying the steganography was also used, that's known as the Adaptive B45 steganography method (Prateek *et al.,* 2017).

Apart from the essential factors of data security, there are gaps related to this study, which have an effect on the security of data and networks:

- High availability: used of cryptography and steganography alone cannot be the only fundamental factors of information safety. There is need for additional strategies to defend towards system threats which includes a denial of carrier or whole network breakdown.
- Encryption keys: Data encryption is absolutely a huge venture for this study. The lengthy the encryption keys, the harder it could be for IT administrator's duties to keep track of all the keys. If the encryption key is missing, its related data is also missing.
- Expense: Data encryption may be pretty steeply-priced due to the fact application that preserve encrypted information need to have the potential for performing such duties. Without successful tool decreasing information activities may be drastically compromised. Using public-key cryptography includes the establishment and upkeep of public key infrastructure requiring heavy monetary budgets.
- Unrealistic Requirements: If a company does not apprehend a number of regulations imposed via information encryption technique it is simple to set unrealistic requirements that would jeopardize information encryption security.
- Compatibility: Data encryption may be hard when layered with present programs and applications. That can adversely affect every day activities inside the system.

So far, there are two best methods in which images and documents can be transmitted through an encrypted network system (i.e. cryptography and steganography techniques). According to Rahman *et al.,* (2016) cryptography refers to secret (crypto-) and writing (-graph), while steganography dealt with hiding transmission fact of secret data inside the video, audio, and images. Thus, this study developed a tool that combined the two techniques within a cross-platform application that can effectively hide a message inside a digital video and image before transmission and revealed the message to the authorized receiver at the end of the transmission.

Moreover, the main purpose of this study is to combine Cryptography techniques with Steganography techniques to secure documents and images through an encrypted network system. The techniques will hide secret messages inside an image, audio and video file, to prevent access from a third party. It also prevents a third party to notice or detect the presence of a second secret message invaded. With cryptography techniques, the word document or plain text is compressed first, and then cryptographic algorithms implemented on the compressed message. The file will then be used as the secret message that can be hidden in the digital audio or video, the technique is called steganography. Once a video file is embedded with a secret message, it can be sent to the authorized user.

Many works have been proposed and implemented by various researchers in the areas of encryption, decryption, image security, secure transmission and networks in the past. For instance, Cheng and Li (2000) proposed new partial encryption technique that is used for encrypting the data which is compressed. Their technique was used on many image and video compression approaches. They have proved that their technique is fast, secure and maintain the performance of the compression process. Younis and Fahmy (2007). Proposed energy efficient and cluster based clustering approach which is working in hybrid manner for transmitting the data between the source and destination. Kim *et al.* (2004). Proposed energy efficient Low Energy Adaptive Clustering Hierarchy (LEACH) with transmission control protocol for performing effective data communications between the nodes in the WSNs.

Mukesh *et al.* (2008) proposed a new energy efficient secure routing protocol that uses symmetric cryptographic algorithms for providing high level security. Their protocol has been achieved the enhanced and energy efficient image compression and also improved the bandwidth utilization and the network lifetime through security. Wenjun *et al.* (2014) discussed in detail about the issues of content oriented search of image data that are archived through online during the preservation of the input data confidentially. They have used effective and secured computation methods like homomorphic encryption that able to use effectively in the applications with high time complexity and computational cost. The authors focused in their work for conducting the comparative analysis between the two major techniques.

Also, Elhoseny *et al*. (2016) proposed a new ECC and Homomorphic based encryption method for securing the data transmission in WSNs. In their method, the ECC is used for exchanging the keys such as private and public due to its ability for providing the high level security with the help of smaller size of keys. Moreover, the existing homomorphic encryption technique is used to allow cluster head for aggregating the encrypted data without decrypting them. They proved that their method that is able to work along with the various sensing environments which need to capture the text data as well as the images including medical image data. Their model achieved better performance in terms of network lifetime, throughput, energy consumption and the memory requirements. Elhoseny et al. (2017), proposed a new method for performing secure image processing and the image transmission method in WSNs by applying the standard cryptographic algorithms such as Elliptic Curve Cryptography (ECC) and the Homomorphic Encryption (HE). They have achieved better performance in terms of network security and the network lifetime than the standard encryption algorithms like Rivest–Shamir–Adleman (RSA), Data Encryption Standard (DES) and Advanced Encryption Standard (AES).

Similarly, Stallings, W. (2013) and Cui et al. (2017) developed a framework for a secure and efficient cloud based image sharing to enable the mobile devices. Here, the standard encrypted image datasets were used with privacy. Their aim is to provide a user friendly hand held device design which saves the transmission cost over the mobile nodes. Moreover, it directly utilizes the outsourced and also correlated the input image datasets for reproducing the image of interest within the cloud. In addition, they introduced an effective index design which allows the mobile node for securing the data from encrypted image datasets. They have analysed the security level of the proposed model. Moreover, they have proved that the bandwidth and energy consumptions on each mobile node that are able to achieve all the security services and guarantees. Hou et al. (2018) in their study designed a new system called switching fractional order based chaotic system which contains the fractional order of Chen system and the other two more fractional order chaotic systems. Moreover, they have applied the switching fractional order over their newly proposed chaotic system for encrypting the

image by applying the exclusive or (XOR) operation based encryption technique. The technique improves randomness and enhances the encryption speed.

Furthermore, Muthurajkumar et al. (2018) built a new secured and energy efficient routing protocol which uses the intelligent agents for enhancing the data communications in mobile ad-hoc networks. Their secure routing protocol achieved better performance in terms of attack detection accuracy and network lifetime with less energy consumption. Zhang and Wang (2018) published an asymmetric image encryption method which works based on an ECC. In their work, the sender and receiver agreed over the ECC point by applying the Diffie–Hellman key exchange method which is working public in nature. First, they have reduced the encryption times by combining the groups of pixel values and also convert them into big integers. Next, the sender encrypts big integers with ECC and the chaotic system. Finally, they have obtained the original data from the available encrypted big integers. In their work, they performed the key transmission and management activities simply and securely. They tested the security and efficiency of their proposed algorithm when compared to other existing systems. Lastly, Abdel-latif et al. (2019) came up with a method for performing an effective encryption process by applying the quantum image encryption over the health data. The new method uses the gray code and a chaotic map.

RESEARCH METHODOLOGY

Research Design

The most appropriate study design and methods are needed to achieve the main objectives of this study. Cryptography and steganography are two approaches used to protect information by key-encrypting it or obfuscating it. The encryption algorithm was used in this research study. The algorithms used in these methods are Advanced Encryption Standard (AES) and Data Encryption Standard (DES). The first takes the input as a block of plain text and applies encryption. The most well-known block cipher algorithms are AES and DES. The system uses two different mathematically related keys, called the public key and the private key. Calculating a private key from a public key is not mathematically feasible and is therefore considered one of the most secure systems. The public key is freely distributed, but the private key remains private. The public key is used to encrypt plaintext, and the pair's private or private key is used to decrypt it. Next, the Stegano-Encrypt API is implied.

This Application Programming Interface (API) is responsible for using Least Significant Bit (LSB) image steganography to hide sensitive content in static, unsuspecting images (locks). It takes the content that needs to be hidden as input and outputs a stay gold image or error. When hiding an image, the algorithm first resizes the image to half the cover image, maintains the aspect ratio, and then converts (compresses) it to JPEG, MP3, or MP4 format to fit the cover image will do so. The block diagram (Figure 2.1) shows the Techniques.

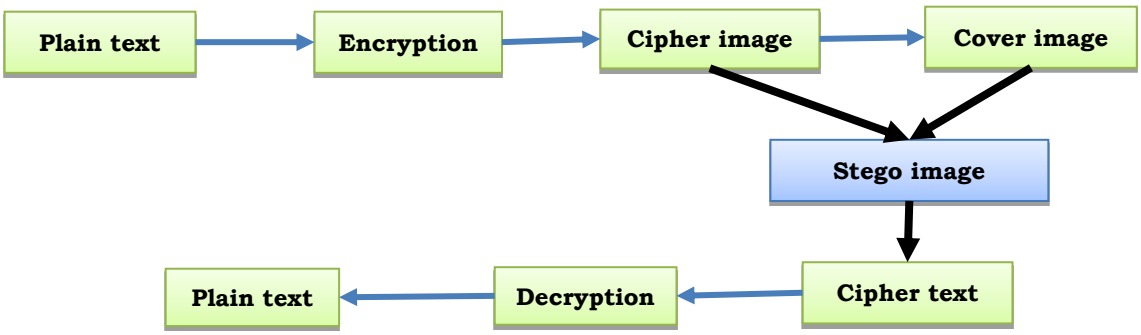

***Figure 2.1**. Proposed Research Flow*

Requirement Analysis

In this study, two types of requirement analysis was adopted (i.e. functional and non-functional requirements analysis).

Functional requirements

These requirements determined the specific functional behavior of the new system.

- ***Login:*** authenticate the username and password of the sender, otherwise deny system entry.
- ***Secret Text Message File*:** Allow user to write a secret message to be hidden, or to select any text file as a secret message.
- ***Cover Image:*** Shield Image is the image that will be used to hide a secret text message.
- ***Stego Encryption LSB:*** used the shield image to hide secret text messages by interchanging the bits of the shield image with the bits of the main message.
- ***Sender:*** send stego image file to the authorized receiver with whom the sender would like to interact.
- ***Receiver:*** receives the sent stego image and decrypt to get access to the hidden text message within shield image.

Non-functional requirements

- ***Safety Requirements*:** Both sender and receiver most make sure only them have the key to encrypt and decrypt data hidden inside the image.
- ***Security Requirements:*** Only the sender and receiver must be aware of the encrypted file. The user must not reveal the sent image signal as well as the receiver data
- ***Software Quality Attributes:*** Only the sender and the receiver can interact via image, audio, or video. No chance of understanding the hidden image.

System Requirements

Hardware Requirements

- Intel Core I5, 250 GHZ process speed, 4 GB RAM, and 500GB Hard drive.
- Minimum Hardware Requirement: Pentium III 256 MHz and above with 128MB RAM and 80GB Hard drive

Software Requirements

- Operating System: Windows 7, 8 and 10
- The source code; Java programming language (JDK 8)
- The service; Python 3.6 programming language
- Tool: NetBeans

SYSTEM IMPLEMENTATION

This section presents system analysis and design implementation of the steganography secured software application developed in this research. It provides how to use some type of different formats such as; jpg, mp4, and mp3 to hide any type of files inside them and transmit through an encrypted network system. The masterwork of this application is that it supports the above-listed file type without the need for conversion, and lowers the limitation on file size to hide.

System Analysis and Design

This Steganography secured device software program calls for any sort of file plaintext, data, or message that is to be hidden. It has modules encrypt and decrypt. The source code become implemented at the NetBeans Integrated Development Environment (IDE) and become

written with the Java programming language (JDK 8). Java prepares a massive quantity of tools and alternatives for programmers, which simplify programming. One correct aspect about the Java utility is that it auto-converts the extension type to the desired layout. The algorithm used for Encryption and Decryption on this application affords using numerous layers instead of the usage of only the LSB layer of the image. Writing data begins off evolved from the ultimate layer (eighth or LSB layer); due to the importance of this layer, the least and each higher layer has doubled appreciably from its layer. The encrypt module is used to cover information on the duvet page; nobody can see that information or record. This module calls for any sort of record or message and offers only one file format in a destination.

The decryption module is used to get the selected hidden information file format. Takes the selected file format as output and passes the file to the destination folder for hidden message files. Before you can encrypt the file, you need to save the name in a specific location. You can save the file name before saving the information in the LSB layer. This information is needed to retrieve the file from the encrypted file in the decrypted state.

Activity Diagram

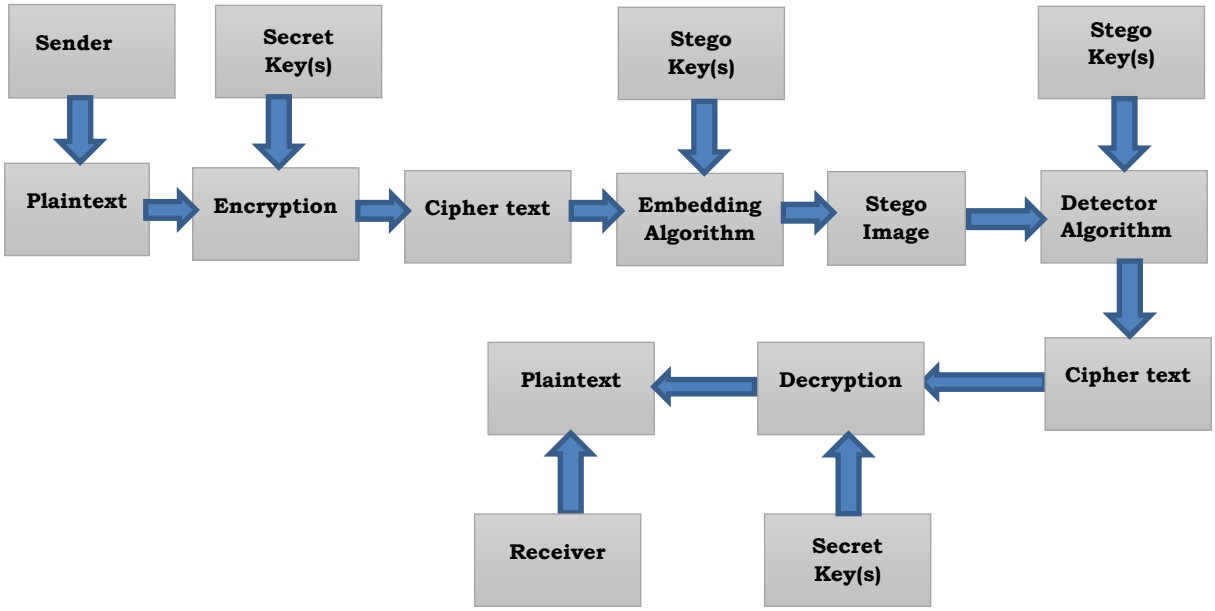

Figure 4.1*: Activity Diagram*

An activity diagram in Figure 4.1 shows that data flow in the steganography secured system. The sender sends a message, plaintext, other images, or embedded picture in a bitstream for example a copyright mark, a barcode, or a serial number that wishes to remain confidential. The file moves to the next phase which is encryption and. then a password will be generated, which is known as secret keys or stego-keys, to make sure that only authorized user with the corresponding decoding key can open/access the message embedded in the cover-object.

The encrypted file (plain text), is then converted to *ciphertext.* The encrypted file was hidden within the harmless text (Image file, audio file, or video file) using a corresponding embedding algorithm, that produces a cover object, transmitted to the intended user. The covered object with the embedded secret message is called the stego-image. Getting back the messages from a stego-image involves first the cover object and seconds a corresponding decoding key. A secret

key that was generated during the encoding process finally, the cipher text is decrypted into the original plaintext file format.

In general, the information hiding process extracts redundant bits from the cover objects. The process is: It consists of two steps. First step identifies the redundant bits of the cover object. Redundant bits are bits that can be changed without compromising the quality or integrity of the cover object. In second step the embedding process selects a subset of redundant bits and replaces them with the data in the secret message. The Stay Gold image is generated by replacing the selected redundant bits with message bits.

System Implementation

Figure 4.2 shows the login window as in any modern application software. This application has its default username and password, which is ***"admin"*.** It is not case-sensitive. The user has to log in with the default username and password to have access to the menu of the application where he can change its authentication.

Figure 4.2**:** Homepage

- **Minimize**- When you click on it, the application will disappear from the desktop and resides at the button, on the Windows taskbar.
- **Maximize**- It allows the user to enlarge the application to the size it contains
- **Close Button**- This allows you to close the application completely
- **Login**- After entering the required username and password. When clicked on the button it allows you to gain access to the menu of the application.

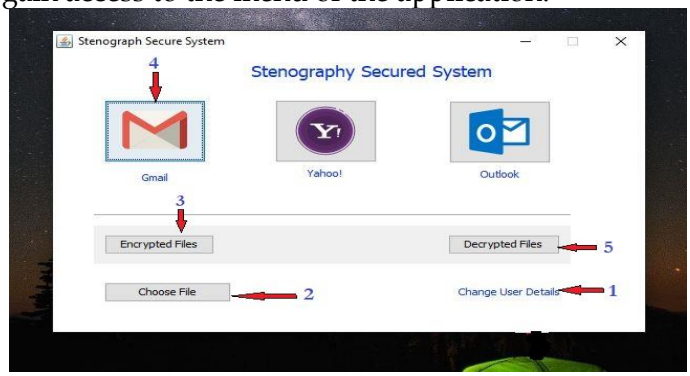

Figure 4.3**: Menu**

Figure 4.3 shows the frame of the system in which there are five options available

1. **Change User details –** This option tab will allow a user to personalize and change its login details; the username and password
2. **Chose file**- The option allows you to navigate to the document folder in the computer and selects a file you which to encrypt or decrypt.
3. **Encrypt Files-** This option allows the selected file to be encrypted.
4. **Email Services-** The frame represents Mail Services where encrypted files can be sent to the receiver by any of the listed mail providers.

5. **Decrypted Files-** This option allows the encrypted files to be decrypted to their original file format.

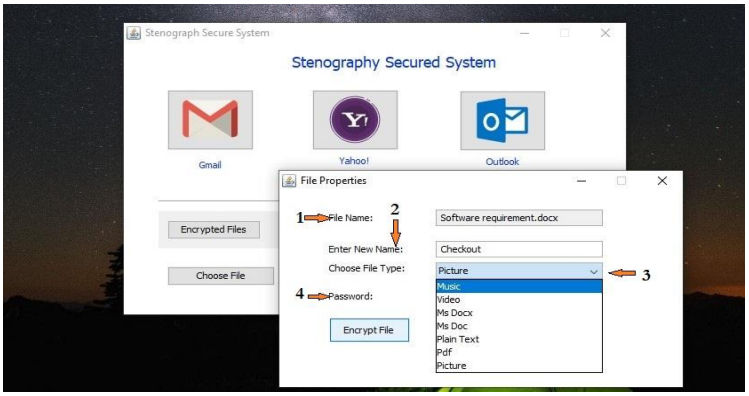

Figure 4.4**: Encoding**

The Figure 4.4 shows option tabs that are to be selected before the file will be encrypted.

1. **File Name**- The option displays the name of the selected file to be hidden.
2. **Enter New Name-** This option allows you to enter a new file name the hidden file (*Original file*) as a disguise
3. **Choose file Type-** The options tab has a drop-down box with the list of different file types. It allows you to select any file format such as pictures, music, or video as a *cover- object,* before encryption. The options tab also allows you to the select original file type when decrypting the file.
4. **Password:** The options tab is where Secret keys or Stego- keys are been generated when you click on the encrypted files button

Encryption process

1. This screen allows you to load a file that you want to encrypt, to load the file click on the button "**Choose file**". The file open dialog box, will displays as follows, select the file, which you want to hide and click on the Open button.

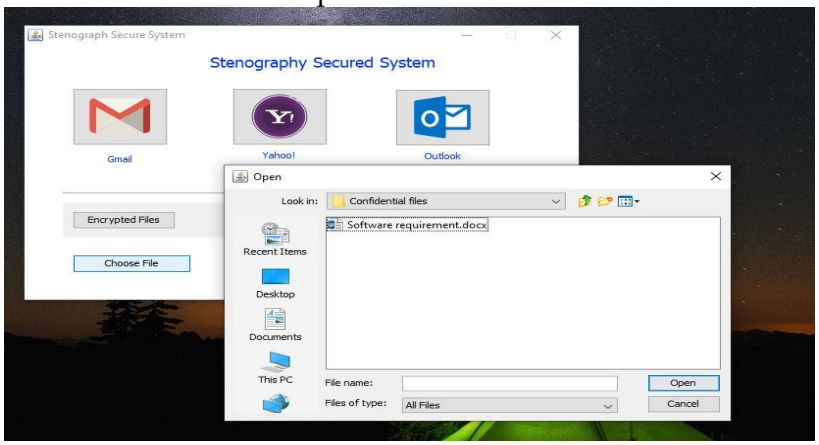

Figure 4.5**:** File Location

2. Next "***Enter New Name"*** as a disguise of the original file, then click on the dialog box on "***Choose file Type"***. Select any file type as Cover-object

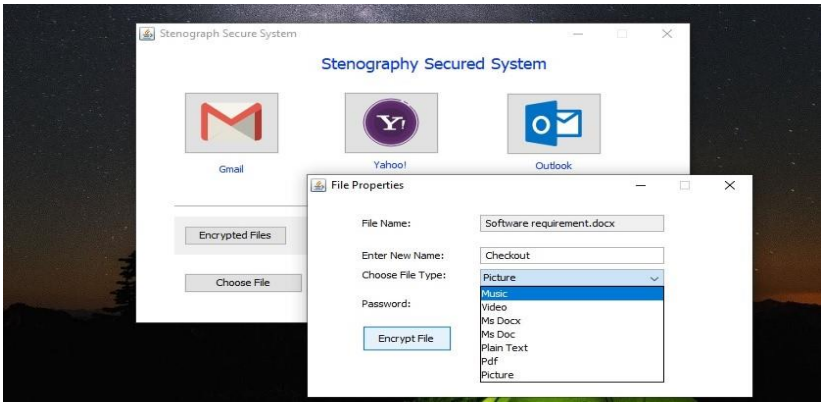

Figure 4.6: Select Cover Object

3. The next step is to encrypt the file. Now click on the "***Encrypted Files***" button, it will generate a password "Secret keys", and display "Encrypted Successful". (*The password will be shared with the receiver to use for decryption)*. The encrypted file is saved in the document inside the Steganography folder-→ encrypted folder. The next step is to click on any mail service e.g. " Gmail" to attach the encrypted file and send it to the recipient. See Figure 4.7.

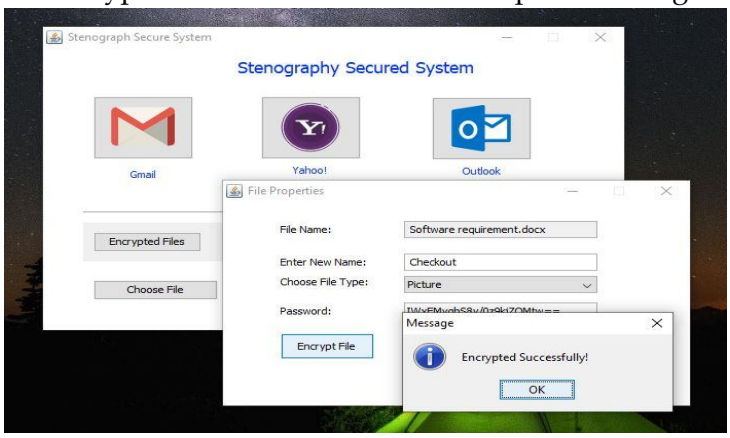

Figure 4.7: Encoded

The Figure 4.8 shows the encrypted file in a document folder → Stenography → Encrypted

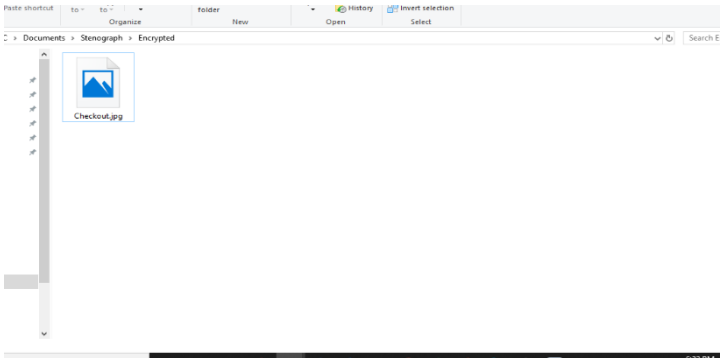

Figure 4.8: Secret Image

Decryption Process

1. Select the "***Choose Files***" tab option which opens the file dialog box, here you have to select the stego- image which has been downloaded and saved in a folder and has a hidden information file. Select the file and click on the Open button.

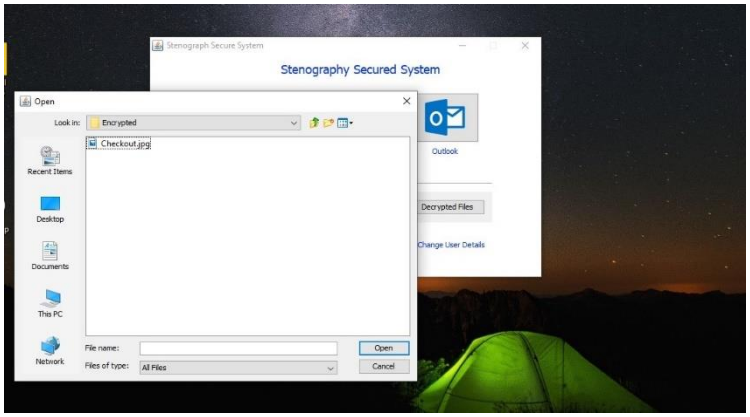

Figure 4.9**:** Location of Encrypted File

2. Next "***Enter New Name"*** the original name of the file, then click on the "***Choose file Type"***, dialogue box and select the original file type.

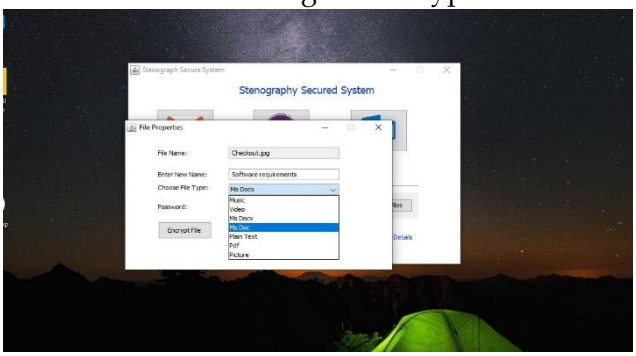

Figure 4.10**:** Selection of Original File Type

3. Next is to insert *"**Secret keys**"* in the password box *(The secret keys must be the keys that were generated during encryption)*

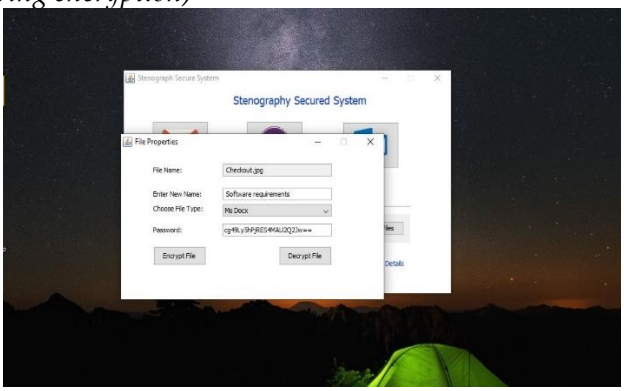

Figure 4.11**:** Enter Secret Key

4. The next step is to decrypt the file. Now click on the "***Decrypted file"*** button, and it will display a box with the message "Decrypted Successful".

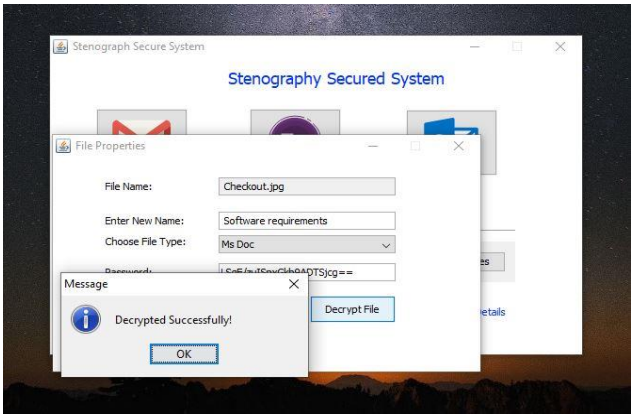

Figure 4.12: File Decryption

CONCLUSION

In this research study, the security concept of digital data communication is realized via the network. It was designed to combine elements of steganography and cryptography to improve performance. We performed a new steganography method and combined it with the AES algorithm. The executed method was implemented in a program written in Python and Java. The proposed method has succeeded in hiding various types of text in images, videos and audios in private keys, in addition to unstable displacement distances. Finally, using multiple options for the file type as a cover object is better than just using an image. The results obtained show that the proposed method is promising in terms of security and robustness. The developed system was recommended as a student management tool which includes multiple characteristics such as admission, attendance, fee collection library, examination, schedule, monitoring of transportation, student performance report, etc. The tool provides a 360-degree view of the students to handle their multiple requirements and track their instructional performance.

This study recommends the following:

- The Steganography Secured System application will aid multinational, government, and private organizations to secure and transmit their confidential documents without lapse of hacking the information.
- The application will aid in transmitting students' performance reports without having challenges in data security via the network.
- As the government moves to avert terrorism. Steganography secured system application can be used by the Military, Police, Air force and Navy to send confidential information to their counterpart team in the field.

REFERENCES

Ahmed, A. and Talal, A. (2018). Cryptography and Steganography: New Approach. *Transactions on Networks and Communications* (2nd Ed.). Melbourne, Australia: Thomson

Aiswarya, B. and Hema, K. (2017). Combined Strength of Steganography and Cryptography - A Literature Survey. *International Journal of Advanced Research in Computer Science (IJARCS), 4*(1), 97-105.

Anas, A. and Bagiwa, A. M. (2020). Survey on Passive Forgery Detection Technique. *International Journal of Science and Innovation (IJSI), 21*(4), 24-33.

Anas, A., Bagiwa, M. A., Roko A., Buda S., Zaharadden, Y. Y., Bello, A. M., Halimatu, A. A. (2022). An Inter-Frame Forgery Detection Technique for Surveillance Videos Based on

Analysis of Similarity. *Sule Lamido Journal of Science and Technology* 4(1), 15-26, doi.org/1056471/slujst.v4i.265.

Bansal, R. and Badal, N. (2022). A Novel Approach for Dual Layer Security of Message using Steganography and Cryptography. *Multimedia Tools Applet, 5*(4), 20669-20684. Doi.org/10.1007/s11042-022-12084-y.

Cheltha, J. N., Rakhra, C. M., Kumar, R. and Waliya, H. (2021). A Review on Data Hidden and Using Steganography and Cryptography. *International Conference on Reliability, Infocom Technologies and Optimization (ICRITO),* 1-4, doi; 10.1109/icrito51393.2021.9596531.

Cheng, H., & Li, X. (2000). Partial encryption of compressed images and videos. *IEEE Transactionson Signal Processing, 48*(8), 2439–2451.

Cui, H., Yuan, X., & Wang, C. (2018). Harnessing encrypted data in cloud for secure and efficient mobile image sharing. *IEEE Transactions on Mobile Computing, 16*(5), 1315–1329.

Das, R. and Baykara, M. (2019). A Novel Approach for Steganography; Enhanced Least Significant Bit Substitution Algorithm Integrated With Self-Determining Encryption Futures. *IEEE Transact, 33*(1), doi.10.32604/csse.2019.34.023.

Dhamija, R. and Dhaka, V. A. (2015). Novel Cryptographic and Steganography Approach for Secure Cloud Data Migration, *International Conference on, "Green Computing and Internet of Things (IGCIoT)", IEEE,* 346–351.

Elhoseny, M., Elhoseny, M., Farouk, A., Farouk, A., Batle, J., Shehab, A., et al. (2017). Secure image processing and transmission schema in cluster-based wireless sensor network secure image processing and transmission schema in cluster-based wireless sensor network (2 Vols. Edition: 1022-1040, Chapter: 45). In A. E. Hassanien & T. Gaber (Eds.), *Handbook of research on machine learning innovations and trends*. Pennsylvania: IGI Global. https ://doi.org/10.4018/978-1-5225-2229-4.ch045.

Elhoseny, M., Elminir, H., Riad, A., & Yuan, X. (2016). A secure data routing schema for WSN using elliptic curve cryptography and homomorphic encryption. *Journal of King Saud University Sciences – Computer and Information, 28,* 262–275.

Geeta, D., Rote, A. and Patil, M. (2013). Steganography with Cryptography Technique for Data Hiding. *International Journal of Science and Research (IJSR), 5*(2), pp: 213-219.

Haripriya, R. and Brojo, K. M. (2017). Pros and Cons of Cryptography, Steganography and Perturbation techniques. *IOSR Journal of Electronics and Communication Engineering (IOSR-JECE),* 76-81. www.iosrjournals.org.

Hou, J., Xi, R., Liu, P., & Liu, T. (2018). The switching fractional order chaotic system and its application to image encryption. *IEEE/CAA Journal of Automatica Sinica, 4*(2), 381–388.

Karthikeyan, B. A., Kosaraju, C. and Gupta, S. (2019). Enhanced Security in Steganography using Encryption and Quick Response Code in Wireless Communications. *Signal Processing and Networking (WiSPNET), International Conference on. IEEE, 2016,* 2308–2312.

Kim, J., Jang, K. Y., Choo, H., & Kim, W. (2007). Energy efficient LEACH with TCP for wireless sensor networks. In *Computational science and its applications–ICCSA 2007,* 275–285.

Mukesh, R., Damodaram, A., & Subbiah Bharathi, V. (2008). Robust and secure image transmission in wireless sensor networks using enhanced compression and encryption. In *ACST'08 proceedings of the 4th IASTED international conference on advances in computer science and technology* (pp. 174–178).

Muthurajkumar, S., Ganapathy, S., Vijayalakshmi, M., & Kannan, A. (2019). An intelligent secured and energy efficient routing algorithm for MANETs. *Wireless Personal Communications, 96*(2), 1753–1769.

Pillai, B. M., Mounika, P. J. and Rao, P. S. (2026). Image Steganography Method Using K-Means Clustering And Encryption Techniques. *Advances in Computing,*

Communications, and Informatics (ICACCI), 2016. International Conference on. IEEE, 2016, 1206–1211.

Pooja, C. and Dinesh, C. J. (2013). Secure Image Data Transmission and Hiding Technique: A Survey. *ACCENTS Transactions on Image Processing and Computer Vision, 2*(2) ISSN (Online): 2455-4707, http://dx.doi.org/10.19101/TIPCV.2016.22001

Prateek, K., Singh, P., Tripathi, R., Kumar, R. and Deepak, K. (2017). Secure Data Transmission. *International Research Journal of Engineering and Technology (IRJET).* www.irjet.net.

Rahman, M. M., Akter, T. and Rahman, A. (2016). Development of Cryptography-Based Secure Messaging System. *Journal of Telecommunications System & Management (JTSM),* doi: 10.4172/2167-0919.1000142)

Ross, A., Fabien, A. P. and Petitcolas, R. (1998). The Limits of Steganography. *IEEE Journal on Selected Areas in Communications 16*(4), 474-481.

Salah, A. A., Dena, S. A., and Abdullah, M. A. (2018). Secure Image Transmission Over Wireless Networks. *International Journal of Engineering & Technology, 7*(4), 2758-2764.

Sophie, E. (2019). Current State of Steganography: Uses, Limits & Implications. *University of California, Davis College of Engineering Department of Computer Science* http://www.cs.ucdavis.edu/

Stallings, W. (2013). *Cryptography and network security: Principles and practice*. London: Pearson Education.

Tibabu, B. (2018). Secure Mobile Banking Framework by Using Cryptography and Steganography Methods. *Global Scientific Journals 6*(8), 23-27.

Vijayakumar, P., Vijayalakshmi, V. and G. Zayaraz, G. (*2016*). An Improved Level of Security for DNA Steganography Using Hyperelliptic Curve Cryptography. *Wireless Personal Communications, 1–22.*

Wenjun, L., Varna, A. L., & Min, W. (2014). Confidentiality-preserving image search: A comparative study between homomorphic encryption and distance-preserving randomization. *IEEE Access, 2,* 125–141.

Younis, O., & Fahmy, S. (2004). HEED: A hybrid, energy-efficient, distributed clustering approach for adhoc sensor networks. *IEEE Transactions on Mobile Computing, 3*(4), 366–379.