GLOBAL JOURNAL OF ADVANCED RESEARCH
(Scholarly Peer Review Publishing System)

ENHANCEMENT OF DATA SECURITY AND SHORT INFORMATION EXCHANGES BY STEGANOGRAPHY FOR ORGANISATIONS IN TANZANIA

Adum Joseph
Lecturer, Database (SQL) and Information System
consultant, Faculty of Applied Science and Technology,
Kampala International University,
#9790, Dar es Salaam,
Tanzania.
josephadum@yahoo.com

Edward Orinda Onyango
Lecturer & Senior SW Engineering Consultancy,
Faculty of Applied Science and Technology,
Kampala International University,
#9790, Dar es Salaam,
Tanzania
edwardonyango@gmail.com

ABSTRACT

The major objective of this research was to identify the challenges on how data and short message exchange can be secured and implemented using image Steganography mechanism as a safe data information exchange within organizations in Tanzania. The researcher adopted interview as the research instruments, where the research population consisted of 16 staffs that were selected as departments' directors, extensions officers and secretaries. SPSS and excel were used as data analytical tools. The researcher found out that confidential data and information are still being intercepted irrespective of data protection put in place, the network security is becoming more important as the number of data exchange on the internet increases, therefore, the confidentiality and data integrity requires protection against unauthorized access and use. Organizations having a large number of staffs have made it harder to maintain their security of exchanging data with one another while trying to accomplish their usual business. The researcher therefore recommends that, high level security and data protection mechanism be implemented and put into practice. The researcher also recommends that the organizations' management should adopt a system for compressing data that leads to an increase performance of the transfer and embedding the encrypted data in the image file in such a way that the image file pretends as normal image file which assures the security in the information transfer.

Keywords: Steganography, Security challenges, Data relay, Short information exchanges, organizations in Tanzania.

1. INTRODUCTION

The world is becoming more interconnected with the advent of the Internet and new networking technology. There is a large amount of personal, commercial, military, and government information on networking infrastructures worldwide. Network security is becoming of great importance because of intellectual property that can be easily acquired through the internet.

There are many security issues that deal with securing wireless/handheld devices, centralized sever and gateway system and more importantly securing information being communicated via wireless channels in addition to persistent applications and data security (R. Acharya et al). As many cooperate organizations and individuals are rapidly adopting the wireless technology, it will be necessary to review various security measures and techniques that could be deployed in securing data transmission and accessibility by a mobile flexible user. Therefore, in this paper, we exhaustively discussed various security measures taken in security data transmission and accessibility on wireless local Area Networking (WLAN).

Information Communication Technology (ICT) is increasingly becoming more wide spread throughout University education worldwide. This is in line with UNESCO's policy paper for Change and Development in Higher Education which urges Higher Education institutions to make greater use of the advantages offered by the advancement of communication technology to improve the provision and quality of their education. Many universities around the world are turning to the use of ICT, now generally referred to as e learning, as a complement to teacher led tuition on campus (Hazemi and Hailes, 2002).

US armed force showed hand gestures during a photo sessions to convey some military secrets. The field of Steganography is limitless and any kind of cover media can be used for carrying secret messages. Cover medias can be text, images (grey, binary, color), audio, video etc. It is also being used by terrorist for covert communication which is potential for endangering our national as well as world security. Despite the ill effect there are positive sides of Steganography. For example a photographer can store the aperture size, future references etc while taking a picture. Steganography has a wide application in medical imaging were the details of the patients are embedded within the medical image. Similarly Steganography can be used for different friendly applications. It is also used for copy right protection using it along with Watermarking (UK Essay, 2015).

Availability of system and information to the legitimate parties (UK Essay, 2015).. There are many people who are involved in world of Information Technology, they prefer to use internet through their computers to get help upon their day to day activities in their workplace either from one office to another in simplified and convenience aspect with great secret. Computers with softcopies like data have become vulnerable to the hackers and crackers which need some technique to keep them secret through their transmission media by encrypting-decrypting mechanisms such as Steganography. (Kimberly, 2010).

Recent interest in security was fueled by the crime committed by Kevin Mitnick. Kevin Mitnick committed the largest computer related crime in U.S. history. The losses were eighty million dollars in U.S. intellectual property and source code from a variety of companies. Since then, information security came into the spotlight. In the 1990s, Internet became public and the security concerns increased tremendously. Approximately 950 million people use the internet today worldwide. On any day, there are approximately 225 major incidences of a security breach. These security breaches could also result in monetary losses of a large degree. Investment in proper security should be a priority for large organizations as well as common users (Security overview, 2008).

The University of Kimathi in Kenya define Steganography "is the art and science of writing hidden messages inside innocent looking containers such as digital files, in such a way that no one apart from the sender and intended recipient realizes the existence of the hidden message". The secret message is normally embedded in a cover medium known as a stego file in a way that totally conceals the existence of any form of communication going on. Digital images are the most widely used cover files in the world of digital Steganography. The reason for this is because the human visual system can hardly pick the difference between an original image and a stego image when embedding of secret information is properly done. (Kamau, et al, Kenya (2002).

Steganography is more difficult to detect with the advancement of Robust Steganography. Tadiparthi has done significant work in the Robust Steganography by which it is very difficult to detect or even destroy the hidden information after manipulation of the carrier. The model depends more on the strength of the cryptography and error correction rather than just Steganography (Tadiparthi, G.R, 2003).

Computer-based image steganography mainly considers the requirement that the steganographic result, the so-called stego-image, be undetectable, as pointed out in (Anderson and Petitcolas, 1998). Such steganographic techniques may be used in various applications. In the application of image database retrieval, auxiliary information, like captions, time stamps, news, etc., may be embedded into images for convenience of simultaneous handling of the images and the embedded information

1.1 Purpose of Study

The main goal of this research was to set up a mechanism with a system which will be used to encrypt and decrypt data during its transmission for security, integrity and confidentiality of that data, the following research questions guided the study;

i. What are the security challenges in data security and short information exchange in the Ministry of Agriculture?

ii. What are the techniques of hiding data using encryption?

2. LITERATURE REVIEW

2.1 Review of literature of the related studies

In recent decades, the information assurance and cyber infrastructure security fields have developed rapidly. There are now sophisticated techniques to address many security issues in organizations. Confidentiality and integrity can be achieved with robust encryption techniques and message-digests. The exchange of signed message-digests can be used to address potential disputes (J. Feng et al, 2010). Secure untrusted data repository (SUNDR) can be used to detect fork consistency attack and write serializability.

Preventing an adversary from sending malicious input requires tamper-proof software and defenses against Sybil attacks. Research on the design and implementation of tamper-proof secure software has a very long history in both academia and industry. Many design and development tools, techniques, and best practices have been developed to identify and remove vulnerabilities from software. However, developing complex software devoid of vulnerabilities is nearly impossible. Moreover, though security of PC-based software platforms and applications has been widely studied, mobile device and application security remains an active area of research. As a result, we assume that a determined adversary will be able to compromise mobile devices and the applications running on them. Gilbert, et al. recently proposed to use Trusted Platform Modules (TPMs) to guarantee the integrity of raw sensor data, as well as data derived from raw data (P. Gilbert et al, 2011). TPMs, however, are not universally found in mobile devices. Moreover, even in the presence of TPMs, an adversary can manipulate the sensor inputs (e.g., GPS signals).

In accordance to research made by Akhtar, N.; Johri, P.; Khan, S., in the year of 2013 implemented a variation of plain LSB (Least Significant Bit) algorithm. The stego-image quality has been improved by using bit-inversion technique. LSB method improvesthe stego-image. Through storing the bit patterns for which LSBs are inverted, image may be obtained correctly. For the improving the robustness of Steganography, algorithm had been implemented to achieve the randomization in hiding message image bits into cover image pixels instead of storing them sequentially. This method randomly disperses the bits of the message in the cover image and thus, harder for unauthorized people to extract the original message. The presented method shows good enhancement to Least Significant Bit image technique in consideration to security as well as image quality (Maganbhai et al,, 2015).
In response to this data security mechanism, most organization has established the application to strengthen the security concern on the data environment on their resources including server based network data environment.

2.2 Automation of the stego-image technique to improve decision making.

Several researches has been stipulated by different authors revealing the importance of the image Steganography " machine learning approach based on alpha-trimmed mean feature preprocessing is introduced to determine whether secret messages are hidden within JPEG images", the researcher also integrates a multi-preprocessing sequence to develop the classification system which contains features generated from an image dataset including Steganography and clean images, feature ranking and selection, feature extraction, and data standardization. Neural networks using radial basis functions train the classifier to accomplish the decision making progress (IEEE. Vol. 7, 2015).

The analyzed image is labeled as either a steganographic or a clean image. The computer simulations have shown that classification accuracy increases by 40% when using feature preprocessing within the complete detection system over a system without feature preprocessing. In addition, alpha-trimmed mean (including mean and median) statistics approach results in higher classification accuracy (IEEE. Vol. 7, 2015).

2.3 A system that meets user's requirements

Individuals or organizations may decide to place personal/private/sensitive information in Steganography carriers, the application is advantageous because it portrays cost effective development since individual and staffs users of the organization will be able to access the system via a uniform environment. There is no need to develop and test it on all possible operating system versions and configuration were it makes easier troubleshooting. Unlike the traditional system, the server will be accessible anywhere with the registered staffs known by the system, a Microsoft net framework platform that has been used by a researcher is the far best suited to satisfy the needs.

3. METHODOLOGY

The study was guided by descriptive survey research design which systematically describes the details and characteristics of a population. It describes the data security and their protection on what is being studied and exploration of the existing phenomenon. An interview guide was used as a research instrument to collect data from the respondents. The instrument was selected because it allowed the researcher to get in-depth data about the requirements specification of the Steganography system. The instrument was also selected because the target population was known.

The target population consisted of ministry department directors, Extensions Officers secretaries of Ministry of Agriculture Food Security and Cooperatives. The researcher collected data from a target population which made total of 16 targeted respondents. They were selected because they are people responsible for data transfer and receiving in the ministry.

The validity of the instrument was ensured using content and face validity methods. The content of the instrument was discussed together with experts from the ministry of Agriculture, and with the supervisor. Supervisor went through the study variables and contents of the research instrument in line with objectives to identify elements that would be corrected. This helped in eliminating those elements that were not important. The intention of the discussion was to examine the appropriateness of the different items in the instrument to measuring the research variable.

4. ANALYSIS OF FINDINGS

4.1 System Analysis

Among the known fact gathering technique that was used in gathering data was interview and observation as other additional methods. Analysis was done followed by the problem recognition and feasibility phases and this was completed prior the design phases to start.

4.2 Feasibility study

The feasibility of the research project was analyzed in the ministry and business proposal was put forth with a very general plan for the research project and some cost estimates. During system analysis the feasibility study of the proposed system was carried out. This ensured that the proposed system not a burden to the ministry and it should be done in order to create a better security of the data being exchanged within and outside the ministry base. During the data collections, workers were given interview guides by the ministry. The response and results showed that the majority wanted to get the data security mechanism and the management as well were interested and therefore needed to be trained and install the system and see how it works, use and any interaction accompanied to the safety of the message exchange, finally they were instructed on how to use the system. For feasibility analysis, some understanding of the major requirements for the system was essential.

Three key considerations involved in the feasibility analysis were;

- Economical Feasibility
- Technical Feasibility
- Social Feasibility

4.2.1 Economical Feasibility

This study was carried out to check the economic impact that the system would have on the Ministry of Agriculture Food Security and Cooperatives. The amount of fund that the company can pour into the research and development of the system is limited. The expenditures must be justified. Thus the developed system was well within the budget and this was achieved because most of the technologies used are freely available and no need to employ more staffs who would be working at the administering the system.

4.1.2 Technical Feasibility

This study was carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. This will lead to high demands on the available technical resources. This will lead to high demands being placed on the client. The developed system must have a modest requirement such as desktop computers; modem printers as well as scanner at minimal or null changes are required for implementing this system.

4.1.3 Social Feasibility.

The aspect of study was to check the level of acceptance of the system by the user especially the intended user. This included the process of training the user to use the system efficiently. The user must not feel threatened by the system, instead must accept it as a necessity. The level of acceptance by the users solely depended on the methods that were employed to educate the user about the system and to make them familiar with it. Their level of confidence was raised so they were able to make some constructive criticism, which was welcomed, as the final user of the proposed system.

4.1.4 Organizational Feasibility

The response towards the new system was positive and workers liked because the mechanism is likely to bring the communication technique at a very high safety and protected between parties to both the Ministry of Agriculture Food and Cooperatives and related staffs whom are not happy with the present unsecured data security and short text information exchange methods that resulted into data loss, isolated, disclosure and unsecured. The newly data hiding information mechanism was the best and secure data and information exchange through the use of image.

4.3 System Requirements Specification.

The section derives the functional and non functional requirements needed for effective and efficient operations of the system. In order for the system to run the following were needed to make it effective;

4.3.1 Functional requirements.

- It was preferred that we use a windows based front end.
- The user should be able to pick out the image file he wants to use in the hiding process.
- The format of the image files which can be used for the hiding process should be 24-bit bitmap.
- User should be able to enter the text message he wants to hide.
- User should be able to view the image before and after the hiding process is complete. It is preferable that a new image be created and displayed with the old image which will allow the user to compare the original image with the new one which will help him to decide whether his choice of image file was appropriate or whether he needs a new one.
- User should be able to transfer the image freely without any problems. I.e. he should be able to copy the new image file. Send or trade it with others without any special hardware requirements other than the normal communication systems available with a computer.
- There should be an encryption process to encrypt the text for better security.
- The user must be able to save the image in which the message is hidden in any desired folder.
- The user should be able to select and view the picture from which to decode.
- When the decode text is demanded the encryption key should be demanded and when entered the decrypted text displayed.
- He should be able to save the decrypted text message in a file.

4.3.2 Non functional requirements.

- The system should not lose data or corrupt files
- The system should offer plausible deniability to owners of protected directories/files, and it should minimize any processing and space overheads, to the user within a few seconds after the submission of the file to be encrypted.
- The system must exclude hidden directories and files from the central directory of the file system. Instead, the metadata of a hidden directory/file object is stored in a header within the object itself.
- The entire object, including header and data, is encrypted to make it indistinguishable from unused blocks to an observer.
- Only an authorized user with the correct access key can compute the location of the header, and ac- cuss the directory/file through the header
- The system shall be independent as it shall run in all operating systems
- The system must be expandable and maintainable to satisfy the user needs and modifiable when a new functionalities arises and able to be added within the existing one.
- It should be potable as being able to be accessed in any platform.

4.3.3 Hardware requirements

The section describes the requirements of the hardware components and software as well needed in effective and efficient running of the proposed system being implemented, for the effectiveness of the running operation the following are the requirements needed.

Table 1: Hardware requirements

Hardware	Requirement
Processor	4.0 GHZ processor speed or Higher
Memory	4.0 GB RAM or Higher, with cache above L3
Hard disk space	500GB ,databases includes
Display	800 x 600(1024 x 768 High color – 16 bit Recommended

The above table 1 shows the hardware components of the machine that allows the system function.

Table 2: Software requirements

Software	Minimum system requirements
Operating system	**Windows 7**
Database	**Ms access**
Programming	**Microsoft Visual Basic 2008,Ms Net framework 3.5 or Higher**

The above table 2 shows the software requirements recommended to enable the system run.

4.4 System design

A system design explains the logical design developed by the researcher, use case diagram data input and findings from questionnaires and interview. The design of the system was in such a way that it was able to handle the data information hiding and secure the file between the known recipients as safer as intended by the sender of the message.

The interface and screen displays showing encrypted and deception files were also produced. The system architecture design was produced. They included with networking, hardware and software specifications. Program design was shown to see how the files linked to each other.

4.4.1 Logical design.

Logical design is a blueprint or sketch of a software application that defines its entities and processes. It seeks to explain how a problem will be solved through getting solutions to design techniques. In the design, the researcher used the object oriented design technique.UML tools for object modeling.

The object modeling combines the data with processes that act on the data into a single unit, called object. An object is an item that can contain both data and procedures that read or manipulates data. The UML tools for object modeling used in this study were use case diagrams.

4.4.1.1 Use case diagram

Use case diagrams are usually referred to as behavior diagrams used to describe a set of actions (use cases) system (subject) can perform in collaboration with one or more external users of the system (actors). Each use case should provide some observable and valuable result to the actors or other stakeholders of the system.

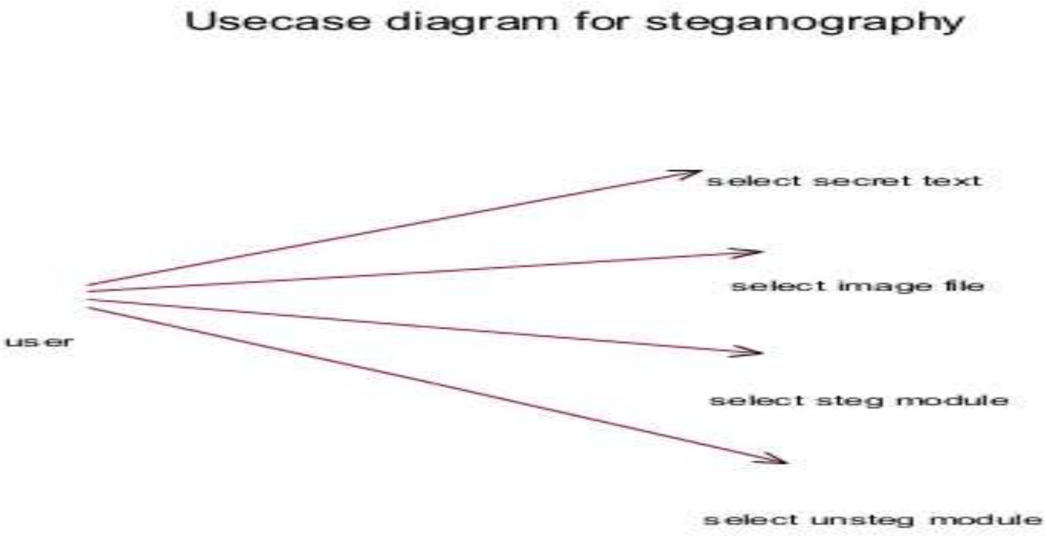


Fig 1: Use Case Diagram

Figure 1 shows how the users of the system are the actors where by a SENDER interact with the system by select an encrypted text with the file and interact with the system for compression and the system responds from another side by selecting a stego file hence decrypt the coded text message and the information delivered safely with their privileges one another.

4.4.1.2 Flow chart

Flow chart is type of diagram that represents an algorithm or process, showing the steps as boxes of various kinds, and their order by connecting them with arrows. The diagrammatic representation illustrates a solution to a given problem. Process operations are represented in these boxes, and arrows, rather, they are implied by the sequencing of operations. Flowcharts are used in analyzing, designing, documenting or managing a process or program in various fields.

Below is the flowchart of data analysis informational hiding using image Steganography.

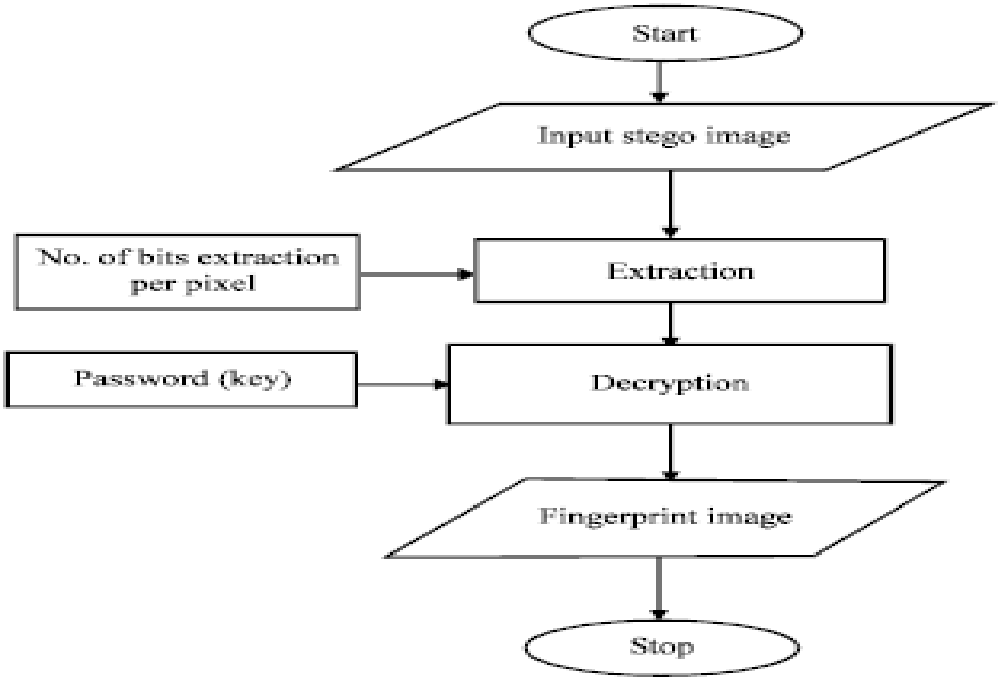


Fig 2: Flow chart diagram

The above figure 2 is the Flowchart of the data security information hiding using image Steganography mechanism. Starting by input the image and once the image extracted it loses some quality of bits per pixel and a key protection is applied to decrypt the image and the system end. Flowchart diagram it uses to show how the system flow from start to stop

Logical design includes (Entity Relationship Diagrams ER diagrams

The exits a number of frameworks for structuring, controlling and planning the development of information flow. The methodology used to develop a steganographical was enhanced a waterfall model.

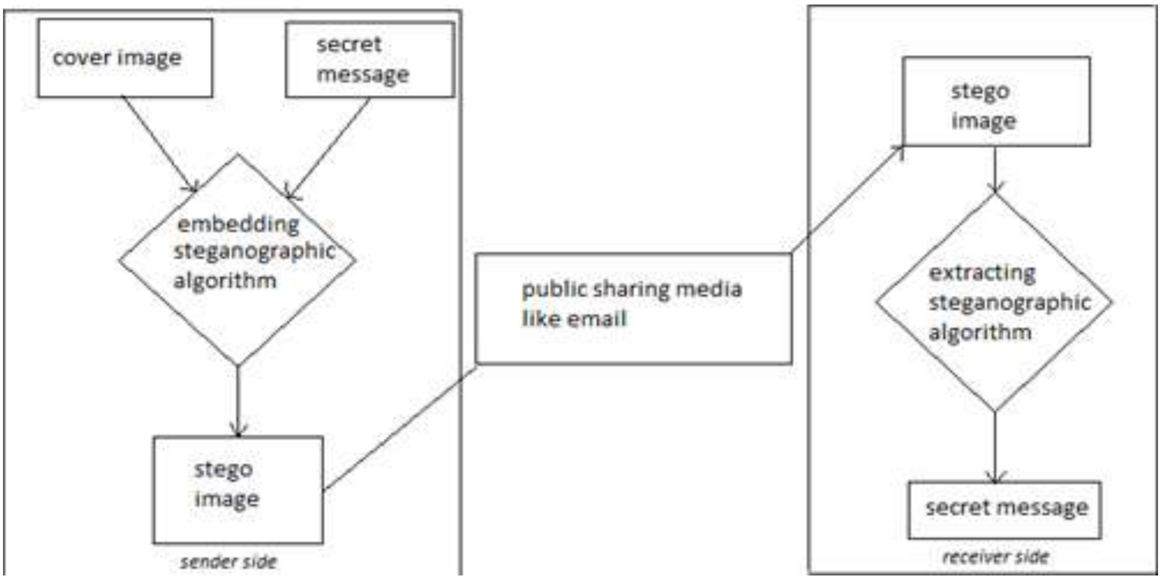

cover image
secret message
embedding steganographic algorithm
stego image
sender side
public sharing media like email
stego image
extracting steganographic algorithm
secret message
receiver side

Fig 3: Logical design

Logically the image to be covered and the file are embedded in an algorithmic mechanisms and stego or hides the file details inside the image and can be sent as a public sharing media like email to the known recepient ,the stego image has to be extracted by a receiver side and the message/file delivered logically.

4.4.2 Physical design.

This phase, the research implemented the blueprint for the new system based on the implementation platform. The physical design is the actual input and output process of the system based on how data is input into a system, how is verified or authenticated, how is processed and how is displayed out as output.

4.5 System Testing and evaluation.

The software system was installed in a Computer with a Microsoft Windows 7- Ultimate edition, 64 bit platform environment, Microsoft Net framework v.4 , Microsoft Visual Studio 2008, with Hard disk capacity 500gb,4gb RAM, Testing was done put in place. System testing was done after implementation with an aim of finding if every component could work alone and if all components could still work after joined them with no errors.

4.5.1 Unit testing

Unit testing carried out on individual modules of the system to ensure that they are fully functional units. The researcher did this by examining each unit separately, example the data being encrypted and empted to the other message key cipher also ensured that the message sent were secured and protected. The success of each individual unit gave the researcher to go ahead carryout integration of the system testing. All identified errors were dealt with and deburg.

4.5.2 Integration path testing

The researcher testing to ensure different modules had been put together and compatible forming a complete system of operations accessing and exchange data securely.

4.5.3 Independent path testing.

Workers tested including the management, directors, and secretaries to ensure they are integrated and test the whole system, errors were eliminated and bugs corrected. Validation testing of different input and resulting outputs was performed.

4.5.4 Validating testing

Test was conducted to see if it does as designed to do does it determines the software meets all the requirements defined in the software requirements specifications, validation testing was done after all the tests and it was repeated until the system was confirmed to have met the requirements.

4.6 System implementation

4.6.1 Implementation

The system was implemented using Microsoft Visual Basic 2005 Express Edition.

4.6.2 Maintenance

The system should be maintained by doing backup of the data and always making sure that firewalls and other security measures are taken. System security is protecting information from been accessed by unauthorized users, disclosure, disruption and modification.
Information security is concerned with the confidentiality, integrity and availability of data (aurora ,2007) assets that in order to take measures to protects information and information systems, components on how information can be compromised are; confidentiality, Authentication(validating a user),integrity(information remains unmodified from source entity to destination entity, availability(accessibility and usability of information and resource to sensitive information and resources).
Failure in the above mentioned information components compromise may lead to many dangers ranging from financial losses and losses of sensitive person information and resources.

The graphical representation of this system is as follows:

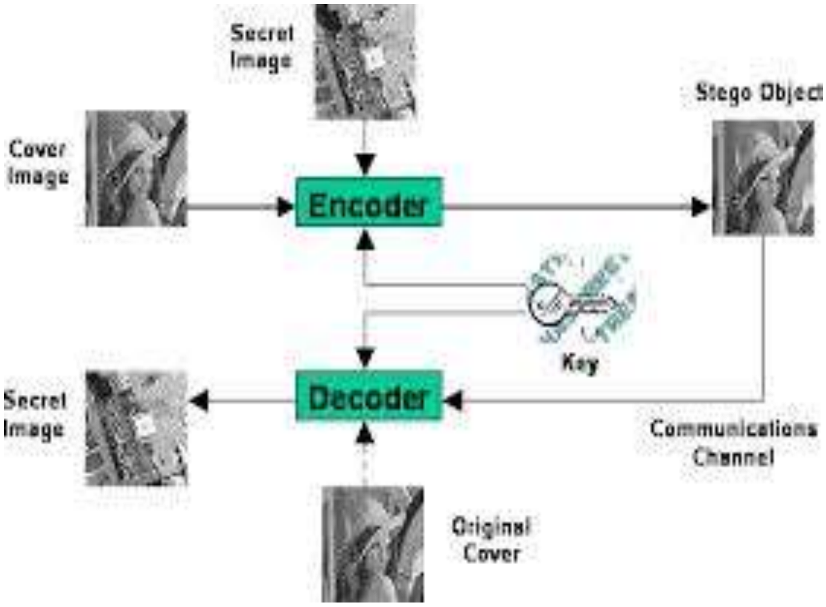


Fig 4: Technique/mechanism of stego image.

Here the cover image with secret information is passed through encoder and stego the object later the information or file with the stego image is decoded to a secret image revealed as an original cover hence the communication is established and secured through.

4.7 User Manual

This is the first screen which has two tab options – one is Encrypt Image for encryption and another is Decrypt image for decryption. In right – top panel is displays about the image to be loaded as for encryption and decryption respectively with the perfoming action button for the best processing.

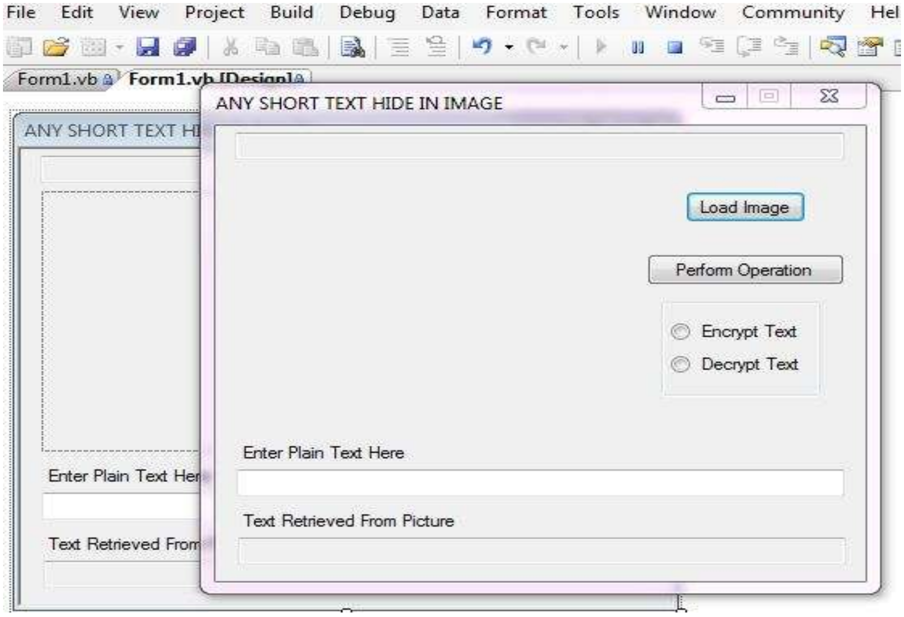
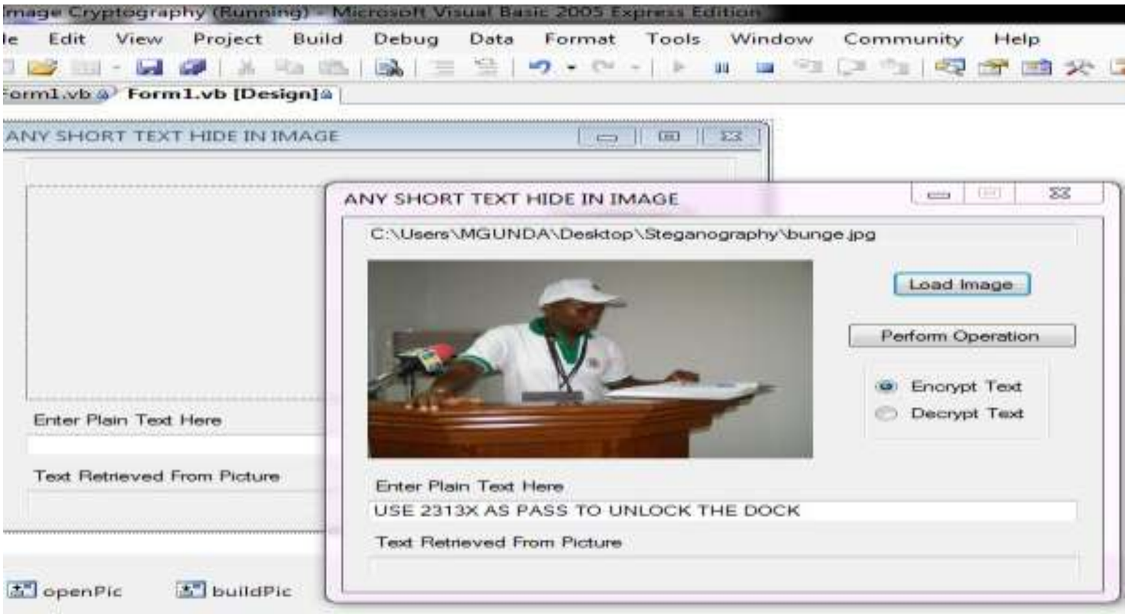


Fig 5: User screen

4.7.1 Encryption

- For Encryption select Encrypt Image tab option.
- The file open dialog box will display, select the Image file, which you want to use hide short text information and click on Open button.
- The image file will opened and is displays, next, type in the short text information on the enter dialogue box "Enter plain text message Here".
- The next step is to encrypt the file. Now select on "Encrypttext" button then click on Perform Operation , it will open the save dialog box which ask you to select the path to save and rename the New image file with the image extension like jpg etc and Save The default format of image file is BMP.


mage Cryptography (Running) - Microsoft Visual Basic 2005 Express Edition
le Edit View Project Build Debug Data Format Tools Window Community Help
orm1.vb Form1.vb [Design]
ANY SHORT TEXT HIDE IN IMAGE
Enter Plain Text Here
Text Retrieved From Picture
openPic
buildPic
ANY SHORT TEXT HIDE IN IMAGE
Load Image
Perform Operation
Enter Plain Text Here
Text Retrieved From Picture

C:\Users\MGUNDA\Desktop\Steganography\bunge.jpg

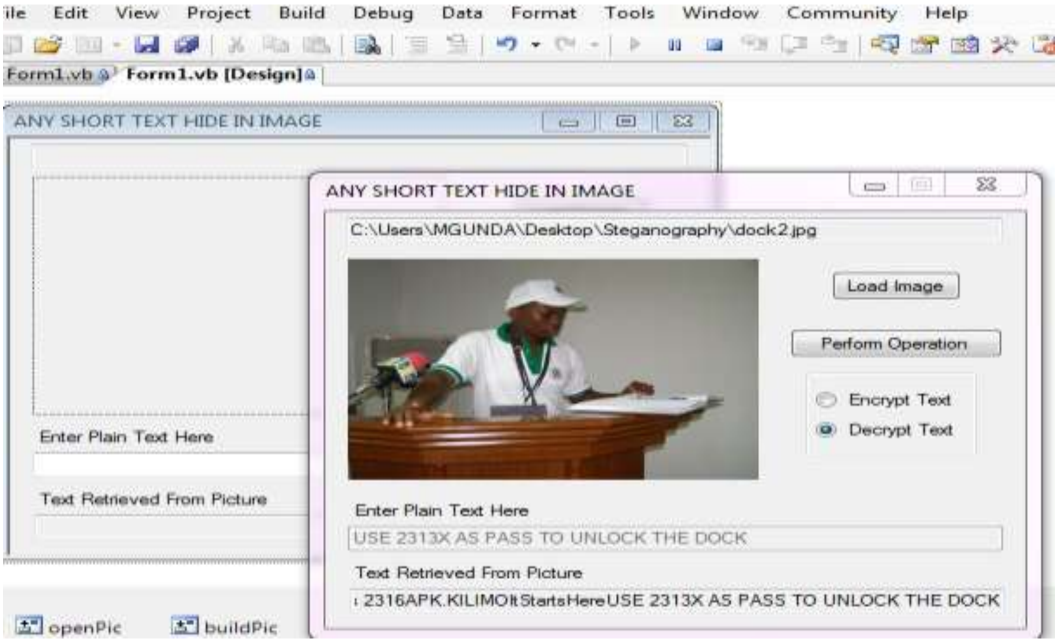
● Encrypt Text
○ Decrypt Text

Enter Plain Text Here: USE 2313X AS PASS TO UNLOCK THE DOCK

Fig 6: Encryption process

4.7.2 Decryption

- Select the Decrypt text tab option.
- Next click on the “Browse” button, which open the Open file dialog box, you have to select the image which is to be Encrypted and has hidden short text information file. Select the image file and click on Open button.
- The image file will display:
- Now click on Perform Operation button, it will decrypt the image, and the hidden short text information displayed on the Text Retrieved” from Picture dialogue box.


ile Edit View Project Build Debug Data Format Tools Window Community Help
Form1.vb Form1.vb [Design]
ANY SHORT TEXT HIDE IN IMAGE
Enter Plain Text Here
Text Retrieved From Picture
openPic
buildPic
ANY SHORT TEXT HIDE IN IMAGE
Load Image
Perform Operation

C:\Users\MGUNDA\Desktop\Steganography\dock2.jpg

○ Encrypt Text
● Decrypt Text

Enter Plain Text Here

USE 2313X AS PASS TO UNLOCK THE DOCK

Text Retrieved From Picture

ı 2316APK.KILIMOItStartsHereUSE 2313X AS PASS TO UNLOCK THE DOCK

Fig 7: Decryption process

4.8 Data presentation and interpretation

This part shows the presentation, analysis and Interpretation of data obtained from Ministry of Agriculture Food Security and Cooperatives.

4.8.1 Demographic characteristics of the respondents

Respondents in this study were described according to age, and gender. In each case the respondents were contacted through a close interview guides to provide their prospective profile information. This was done to enable the researcher to classify compare them accordingly. Their responses were interpreted using frequencies and percentage distribution table as shown in table

Table 3: Gender Distribution

GENDER	FREQUENCY	PERCENTAGE %
MALE	7	41.5
FEMALE	9	58.5
TOTAL	**16**	**100.00**

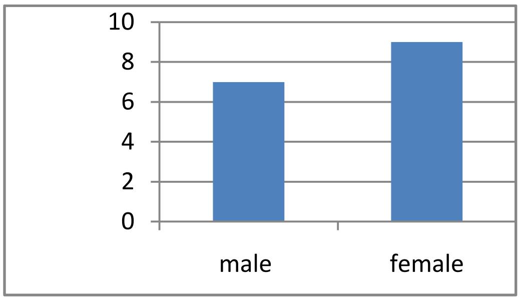


Fig 8: A column chart showing Gender of respondents

Source: (Researcher, 2016)

As indicated in table 3 and Figure 8, in terms of gender most respondents were females (58.5%) indicating that the area of the study was dominated by women as compared to men (41.5%). This means that there is gender imbalance. This might be because female were employed more than male in ministry of Agriculture and food security cooperatives.

Respondents' age distribution

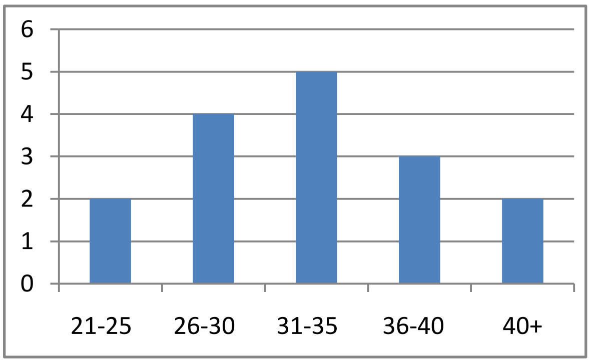


Fig 9: A column chart showing Age of respondents

Source: (Researcher, 2016)

The age distribution of respondents ranged between 21 and above 40 years of age. Majority of the respondents were between 31-35 years with 30.3% followed by those between 26-30 with 29.7%. Those between 36 - 40 were 23.3% and then above 40 were least with only 8.5% and between 21-25 with 8.5%. During the study the researcher find that, those respondent aged between 31-35 are employed in ministry and some were working for a long time in this field.

The challenges of current system

In this study the different challenges were proposed by researcher and giving those options to respondent to suggest if where the system dead ends. For independent variable all items were scaled using four points. Interpretation

Table 4: Challenges of current system

Challenges	Mean	Interpretation	Freq	%tage
Data Loss and integrity	4.23	Yes	13	81.2
Data inconsistency	1.32	Yes	1	6.3
Retention of Data	1.52	No	2	12.5
Average		**Total**	**16**	**100**

Source: (researcher, 2015)

From the table above, the respondents indicated that the major challenge affecting data and short message exchange in the ministry is data loss and integrity as shown by 81.2% as the highest response. Only 6.3% of the respondents think data inconsistency is the challenge, while 12.5% of the respondents believe that retention of data is not a challenge at all. This finding was supported by (James Black et al, 2015) who conducted research on challenges on electronic health information exchange and found out that due to this challenge, Data standards between entities, Management of data processes, and use of existing data standards when possible is totally affected during data exchange.

Data hiding technique

Table 5: Data hiding technique

Technique	Mean	Interpretation	Freq
Image encryption	3.29	Yes	14
Binary data encryption	1.30	Yes	1
Transposition encryption	1.30	No	1
Average	**3.03**	**Total**	**16**

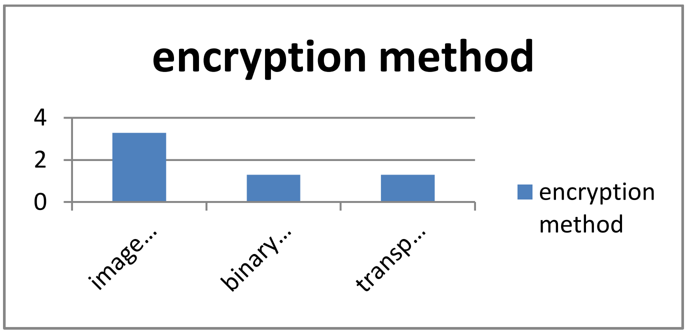


Fig 10: A column chart showing data hiding technique

Source: (Researcher, 2016)

According to table 5 and figure 10, the researcher found out that, the best proposed data hiding technique is image encryption, which many respondents have suggested with mean of 3.29. This finding also conforms to study conducted by (Chi-Kwong Chan et al, 2004) on data hiding scheme by simple LSB substitution. They found out that by applying an optimal pixel adjustment process to the stego-image obtained by the simple LSB substitution method, the image quality of the stego-image can be greatly improved with low extra computational complexity. The worst case mean-square-error between the stego-image and the cover-image is derived. In their study, they stated that experimental results show that the stego-image is visually indistinguishable from the original cover-image. The obtained results also show a significant improvement with respect to a previous work

5 RECOMMENDATION AND FURTHER RESEARCH

5.1 Recommendation

The researcher therefore recommends that, high level security of information exchange baked at client server and no unnecessary maintenance costs or backup as per the testing standards that were implemented.

The researcher also suggests that the size of the storage must be maintained based on the growing demand of users and capacity of the files space especially in the server side where the system needs an optimum performance based on the coming modern communication where the storage is highly needed for backup and centralized data and security software.

The ministry needs a standard file format to be implemented to a centralized server to boost the outgoing and incoming file exchange and smooth the working environment while communicating w\ithin the organization as such to the moment the system is not optimal in document or file exchange and incompatibilities.

Finally, the researcher strongly recommends the management of the ministry to adopt a system for their compressing the data that will lead to an increase the performance of the transfer and embedding the encrypted data in the image file in such a way that the image file pretends as normal image file will assure the security while the transfer takes place. That its possibly that the application should be implemented to the whole area covering the server, offices within and all related venders who communicate with the ministry preferably the divisions, headquarters and to the regional offices.

5.2 Further Research

The researcher recommends that the ministry should implement and organize a well structured ICT system to make possible identifying the user of the system for easy and access while communicating in a safe and safety in managing and control.

The researcher recommends that the ministry should implement a file standard type of Steganography where the document can be attached and be encrypted in an optional to large files attachments.

6. REFERENCES

[1] Acharya, U Rajendra, Debiprasad Acharya, P Subbanna Bhat, UC Niranjan, 2012. "IEEE Transactions on Information Technology in Biomedicine" Vol 5, Iss 4, Pg. 320-323

[2] Aurora, 2007: https://aurorasecurity.com

[3] BussinessDictionary,2015,:http://www.businessdictionary.com/definition/ciphertext.htm.

[4] Farlex2015,:http://www.thefreedictionary.com/information

[5] Farlex 2015: http://www.thefreedictionary.com/ministry.

[6] Farlex, 2015: http://www.thefreedictionary.com/data.

[7] IEEE. Vol. 7, 2015, Machine Learning and Cybernetics, 2008 International Conference (Volume:7)E-ISBN :978-1-4244-2096-4 © Copyright 2015 IEEE.

[8] International Journal of Advances in Engineering & Technology, May, 2014.©IJAET,ISSN, ,22311963.

[9] John P. Campbell and Kimberly Arnold 2002, "Course Signals: The Past, Current, and Future Kamau, et al 2002, An enhanced Least Significant Bit Steganographic Methods for Information Hiding by Gabriel Macharia Kamau, Stephen Kimani and Waweru Mwangi ,School of Computer Science and Information Technology, Kimathi University College of Technology, PO box 657-10100, Nyeri, Kenya (2002).

[10] James Black, MSCIS, Patricia A. Markus, J.D, 2015. "Ongoing challenges in electronic health information exchange" June 23, 2015.

[11] J. Feng, Y. Chen, and P. Liu, 2010. "Bridging the Missing Link of Cloud Data Storage Security in AWS," the 7th IEEE Consumer Communications and Networking Conference - Security for CE Communications (CCNC '10), Las Vegas, Nevada, USA, January 9 - 12, 2010.

[12] Kimberly E. Arnold 2010, "Signals: Applying Academic Analytics.

[13] Laurie Racine, and Phoenix Wang 2009, "Designing for Learning in the 21st Century" 2009.

[14] L.M. Cheng, Chi-Kwong Chan, 2004. "Hiding data in images by simple LSB substitution" Vol 37 Issues 3, Pg. 469-474, March 2004.

[15] Maganbhai 2015. Parmar Ajit Kumar / www.ijcsit.com (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (1) , 2015, 685- 688.

[16] MCAD/MCSD Self-Paced Training Kit: Developing Web Applications with Microsoft® Visual Basic® .NET and Microsoft Visual C#® .NET, 2nd Edition.

[17] P. Gilbert, J. Jung, K. Lee, H. Qin, D. Sharkey, A 2011. Sheth, L. P. Cox, "YouProve: Authenticity and Fidelity in mobile sending". ACM senSys 2011, seattle, WA, November, 2011

[18] QueenStreet, 2015: http://www.webopedia.com/TERM/D/decryption.html.

[19] R. Acharya, V. Vityanathan and R. Pether, 2009. "Wireless LAN Security – Challenges and Solutions", International Journal of Computer and Electrical Engineering, Vol 1, No 3., 2009.

[20] Tadiparthi, G.R. 2003. Robust steganography and analysis of information hiding techniques, Master's Thesis, New Mexico Institute of Mining and

[21] Technology, Socorro, NM, USA

[22] TechTarget2015:ttp://searchsecurity.techtarget.com/definition/Steganography

[23] "Security Overview," 2008. www.redhat.com/docs/manuals/enterprise/RHEL-4- Manual/security-guide/ch-sgs-ov.html.

[24] UK Essays 2015.A trading name of All Answers Ltd, a company registered in England, and Wales. Company Registration No:4964706.VAT Registration No.842417633. Registered Data Controller No: Z1821391. Registered office: (Copyright 2003-2015). Venture House, Cross Street, Arnold, Nottingham, Nottinghamshire, NG5 7PJ.Copyright (2003-2015).

[25] Whatis.com 2015, http://whatis.techtarget.com/definition/framework

[26] Wikipedia (2015): https://en.wikipedia.org/wiki/Data_validation.

[27] Wikipedia,2015: https://en.wikipedia.org/wiki/Encryption