VOL. 05 NO. 9,
FEBRUARY, 2025
E-ISSN 3026-958X
P-ISSN 3027-1169

African Scholar Publications & Research International
www.africanscholarpub.com

Journal of Science Innovation & Technology Research (JSITR)

A Secured and Interactive Model for Data and Information Transfer in Higher Institutions of Learning in Adamawa State Nigeria

Mustapha Kassim
Department of Computer Science, Federal Polytechnic, Mubi.
Corresponding Author: mustaphakassim@rocketmail.com
DOI: https://doi.org/10.70382/ajsitr.v7i9.015

Abstract
Information security is one of the most challenging problems in today's technological world, with increasing number of inventions and innovations in technology which have become an integral part for humans, the urges for same amount in field of security and privacy is felt. The techniques likes cryptography, watermarking, steganography have been able to provide some relief. The level of intruder on the network and standalone system in recent times is at alarming rate. Hackers have devised several means of intruding to both private and public network as technology appears to be advancing at a very fast rate. This menace necessitates adequate security of data and information share across network. The objective of this study is to develop an interactive model capable of securing data and information in a more effectively way. To achieve this main goal, a combination of cryptography algorithm together with steganography system is proposed. In cryptography, a hybridized RSA and Twofish Algorithm will be used to encrypt the plaintext into cipher text in other to provide a robust and strong means of securing data. In a further attempt to secure the data, Least Significant Bits (LSB) is proposed to embed or hide the data behind some cover media before it is being sent to

the intended receiver. The resulting outputs of this research provide a model that can guarantee extra security level for data so as to withstand attackers.

Keywords: Twofish, Cryptography, Steganography, Watermark, Intruder, Encryption.

Introduction

In this present time, where innovation is creating at quick pace and everyday new advancements are made, security is of most extreme need. The data should be guarded thus that it might be gotten to just by the approved work force and any unapproved client can't have any entrance of that information. Information sharing is expanding as a large number of messages and information is being transmitted on web regular starting with one place then onto the next. The security of information is prime worry of the sender. The necessary is that right information ought to be sent yet furtively that lone the collector ought to have the capacity to comprehend the information. At first procedure of cryptographic was concocted to move original data across spots. In cryptographic system the message was converted to cipher in other form covered to such an extent that exclusive the sender and recipient knew the best approach to decode it (Anil, 2018). In Nigeria , Economic and financial crime commission filed charges against those who padded the federal government payroll with about 5000 ghost workers and it was stated that the nation lost about N143bn to the salary fraud (Eniola, 2017). In 2017, the official website of Nigeria National Assembly was reported to be hacked and massive database were leaked online. Exposed data include email address, password, phone numbers, job details and resident address of over 1000 Nigeria and international officials (waqas, 2017). Incident of this nature are increasingly becoming a daily occurrence and thus require urgent attention.

Even though many security devices or systems are currently in place, hackers and eavesdroppers are becoming wiser developing more techniques to overcome the security system. An example is the WhatsApp sniffer (Haroon, 2019). Therefore, there is the need for constant review of security system to beat the hackers.

Unlike the past when images were just about recollections of memories. The

image now speak more due to the invention of the area of image steganography (Cheddad, Condell, Curran and McKevitt, 2015.), which implants mystery information in pictures ill defined to the uncovered human eye (Rabah, 2009; Amirtharajan and Balaguru, 2014). From time past accentuation on new techniques for favored bits of knowledge correspondence has been given high enormity in light of the levels of mystery required.

Steganography and cryptography are widely used for security over a public network. Steganography is the art of concealing data. The objective of steganography is to conceal the data from an untouchable; however the goal of cryptography is to make data muddled by an outcast (Shola, 2019).

Cryptography is a subject in the field of mathematics that is applied in computer science to ensure the security primitives. It is used for lots of purpose like data security, authentication, and digital signatures. It includes scrambling the first data into a form called “cipher message" that is not effortlessly translated by anybody (Kumar, 2017).

Cryptography key was utilized in translate data that was aware just from the rightful people. The confinement of cryptography was that other individual came to realize that the message had a shrouded message in it thus the likelihood of message being decoded by other individual expanded.

The word steganography has a place with Greek word. In Greek the steganography signify "secured composing". The starting point of all steganography was utilized as a part of Greece. They use to enter the message on a wooden tablet and after that apply wax on it to hide the composed information. The method of steganography was obviously better than cryptography as in it the information was covered up in image or other format. The stego image or other format was then sent over web. It had advantage over cryptography as now the center individual does not come to know whether information is covered up in the image or not. The information must be unscrambled from picture by the approved individual as he most likely is aware the wonder to unravel it and had the approved key with him that was required to translate the information.

Steganography is a craft of inserting the secret data inside some other document for the most part as carrier image. Primary goal of steganography is to give a message send across among clients with the end goal that any undesirable individual can't access the data by simply looking at the cover file (Bender, Gruhl, Morimoto and Lu, 2001). This ability of conceal exchange authored as Steganography means “covered writing” in Greek. Different techniques can be

actualized to decimate the presence of the secret text. A group of systems incorporate undetectable ink, character game plan, microdots and advanced marks and spread range. Steganography basically coordinates four rule modules say, a cover document which goes about as the compartment for the secret message, a secret message that contains the characterized data, a key for encoding the mystery message and steganography for sneaking in the mystery message inside the cover image. Mix of these modules makes the stego-protest at the data securing stage. At the data recouping stage the algorithm required is executed to recuperate the principal data from the stego-object (Wang and Wang, 2014).

Steganography can be using to hides the information such that it is not noticeable to client. Steganography has separated into many types like Audio, Video, Text, and Image. If there should be an occurrence of image steganography information is taken cover behind the image Steganography is an imagination to hide the information behind an image, a sound, video or text. At the end of the day it is otherwise called the ways toward of hiding the information inside other information (Amritpal, 2020).

Statement of the problem

One of the major challenges people face when trying to pass across confidential information is how to convey the message secretly to the authorized receiver. Also, different individuals and organizations that operate over the internet need to ensure proper transmission of confidential data in order to ensure the confidentiality, integrity as well as availability of the information (Whitman & Mattord, 2011). Utilizing the procedure of Steganography, data can be covered up in various carriers, for example, image, audio documents, text records, video records and so forth.

Messages sent over the internet sometimes are prone to attacks by intruders. Access to an individual e-mail account details can be gotten by stealing or even by a random guess. Lot of ways is devised on the internet to divert mails belonging to another individual. Therefore data confidentiality, data integrity, authenticity of sender or receiver of message can easily be altered without the sender and receiver knowing it. These have posed a need to secure message needed to be kept private (Mark, 2018).

In this study, a new framework of a Video, Audio, Image and text Steganography system combined with cryptography system was needed in which the data to be

transmitted needs to be encrypted and hidden in an image or other form of steganography in order to enhance the level of security at both ends.

Aim and Objectives

The aim of this research is to develop and implement a model for securing institution's document against unauthorized access to data and information across network.

The following objectives have been formulated to achieve this:

i. To implement steganography technique in the file formats Audio, Video, Image and Text.
ii. To implement LSB steganography algorithm, with hybridized RSA and Twofish cryptography algorithms with a view to enhancing the level of security in image steganography.
iii. To develop a robust data and information security using the combination of the above (i and ii) in an interactive model.

Significance of the Study

This study is significant in several ways. To a network administrator, the study will show how data and can be secured to avoid intruders. Also, a combination of the approach proposal in this study will be useful to other researchers in the area of data and information security. Moreover, the study is beneficial to organization that seek to add impact and better improvement in information security, such as the tertiary institutions, banking sector , health, government agencies and so on.

Literature Review

Cryptography is gotten from two Greek words which mean "secret writing". Cryptography is the way toward encrypting the first content by adjusting and substituting the first content, organizing it in an apparently incomprehensible configuration for others. Cryptography is a successful approach to secure data send across the network communication paths (Bishop, 2010).

When all said is done, cryptography is exchanging information through the origin to goal by modifying it through a private code. The cryptosystems utilizes a plaintext as information and produce a cipher text utilizing encryption algorithm taking secret key as information. The imperative components in cryptosystems are

1. Plain text (input)
2. Encryption algorithm

3. Secret key
4. Cipher text
5. Decryption algorithm

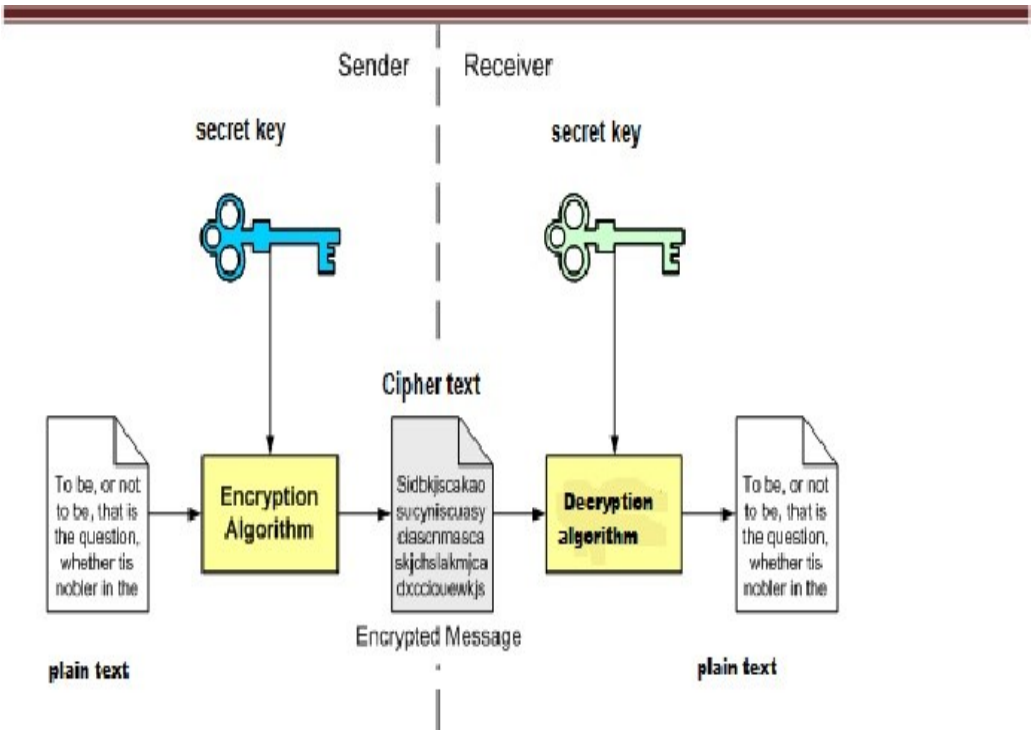


Figure 1: Model of cryptographic structure

Steganography

Steganography in Greek signifies "covered writing". Steganography is the way toward conceal data within different types of data like text, image or audio record, with the goal that cannot be noticeable in the normal perception (Morkel, 2010).

Steganography as a strategy which improves the secret information from unauthorized client. It is utilized worldwide with the aim goal of securing the information while transmission. With the expansion in numeral of clients for internet the utilization of the steganography is additionally expanded to a degree.. This method manages hiding the message presence with the goal of security (Hussain, 2018).

The basic types of steganographic techniques are:

1. Pure steganography
2. Secret key steganography
3. Public key steganography

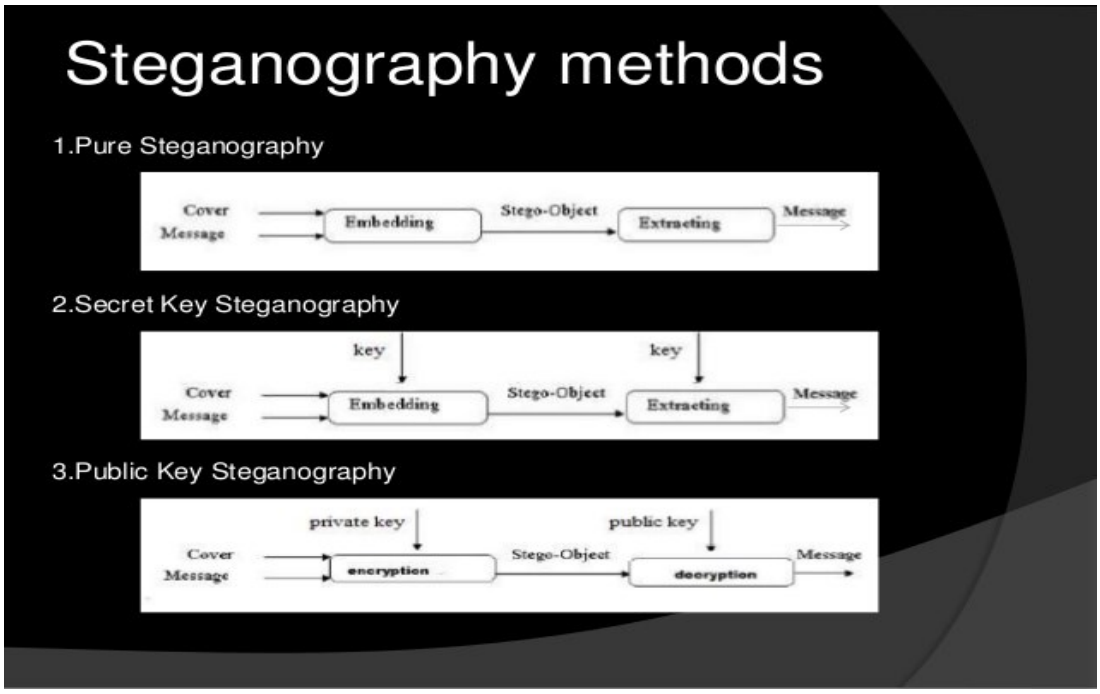


Figure 2: Steganography techniques (Zaidoon, 2015).

Combined Cryptography and Steganography

Both the procedures can be consolidated to give one more level of security. The message can be first encrypted utilizing cryptography to cipher content. This cipher message at that point can be implanted in a cover media using steganography. This consolidated approach will fulfill the three objectives of information hiding: security, limit, strength.

Materials and Methods

Research design

This explains in details how this study "A Secured and Interactive Model for Data and Information Transfer in Higher Institutions of Learning" using the combine techniques of steganography and hybrids cryptography to enhance the level of data and information security in an interactive model.

The information concealing model utilizing the steganographic method in this research can be clarified utilizing this straightforward model.

The Design Method

The methodology for this research involving the use of combine techniques of Steganographic and cryptography which can be broken into two (2) major phase

1. Data securing phase
2. Data retrieving phase

Data Securing Phase

INPUT: Either Audio, Video, Text or Image and secret message

OUTPUT: Stego document (In forms of Audio, Video, Text or Image containing encrypted message

In case of text document to be secured, the following steps will be taken.

1. Divide the secret message into two (2) equal parts
2. The first and second parts are to be encrypted using RSA and Twofish algorithms respectively
3. Merge the output of step 2.
4. Embed the merge encrypted message into the cover image using LSB steganography algorithm to get stego format.

Data Retrieving Phase

INPUT: Stego format

OUTPUT: Secret message

For the data to be retrieve, the following steps will be taken

1. Extract encrypted message from the stego format using LSB steganography algorithm
2. Divide the encrypted message into two parts
3. Decrypt the two encrypted message obtained from step 2 using RSA and Twofish algorithms respectively.
4. Combine the output of step 3 to get the secret image.

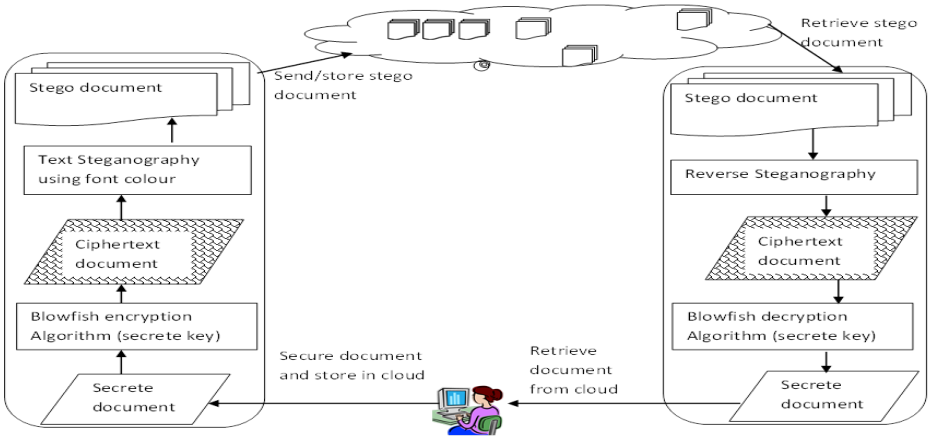


Figure 3: Architectural design of the combined system for Desktop usage

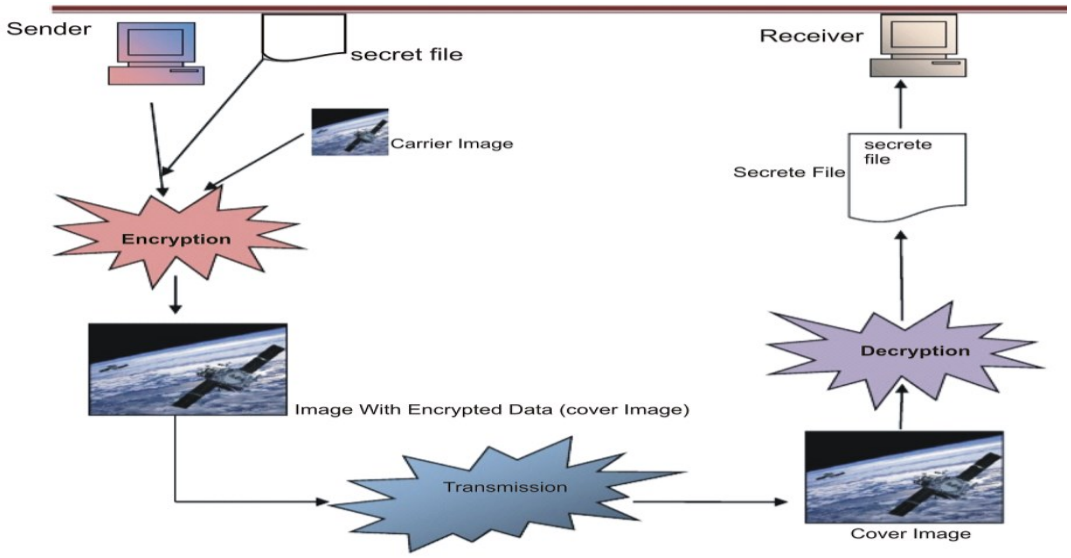


Figure 4: Architectural Diagram for an Interactive System model

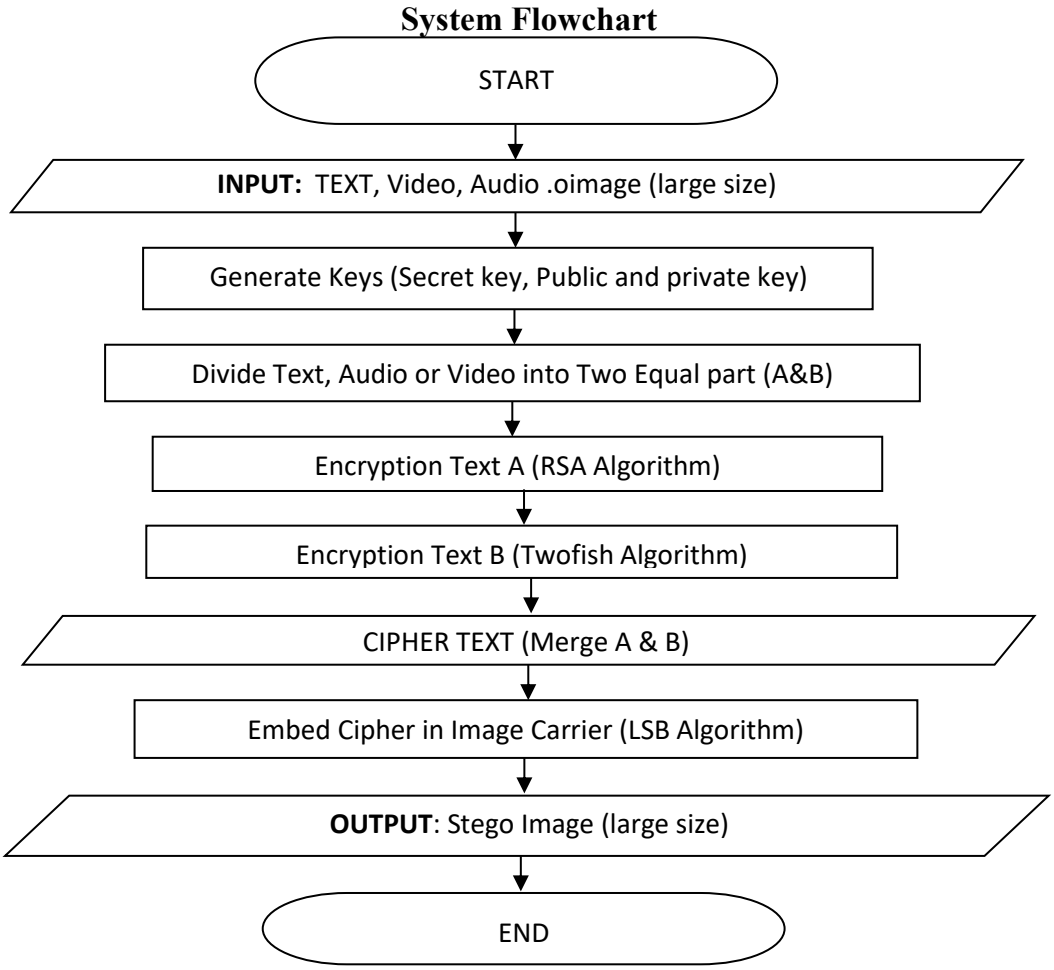


Figure 5: Flowchart for Secure Data Model

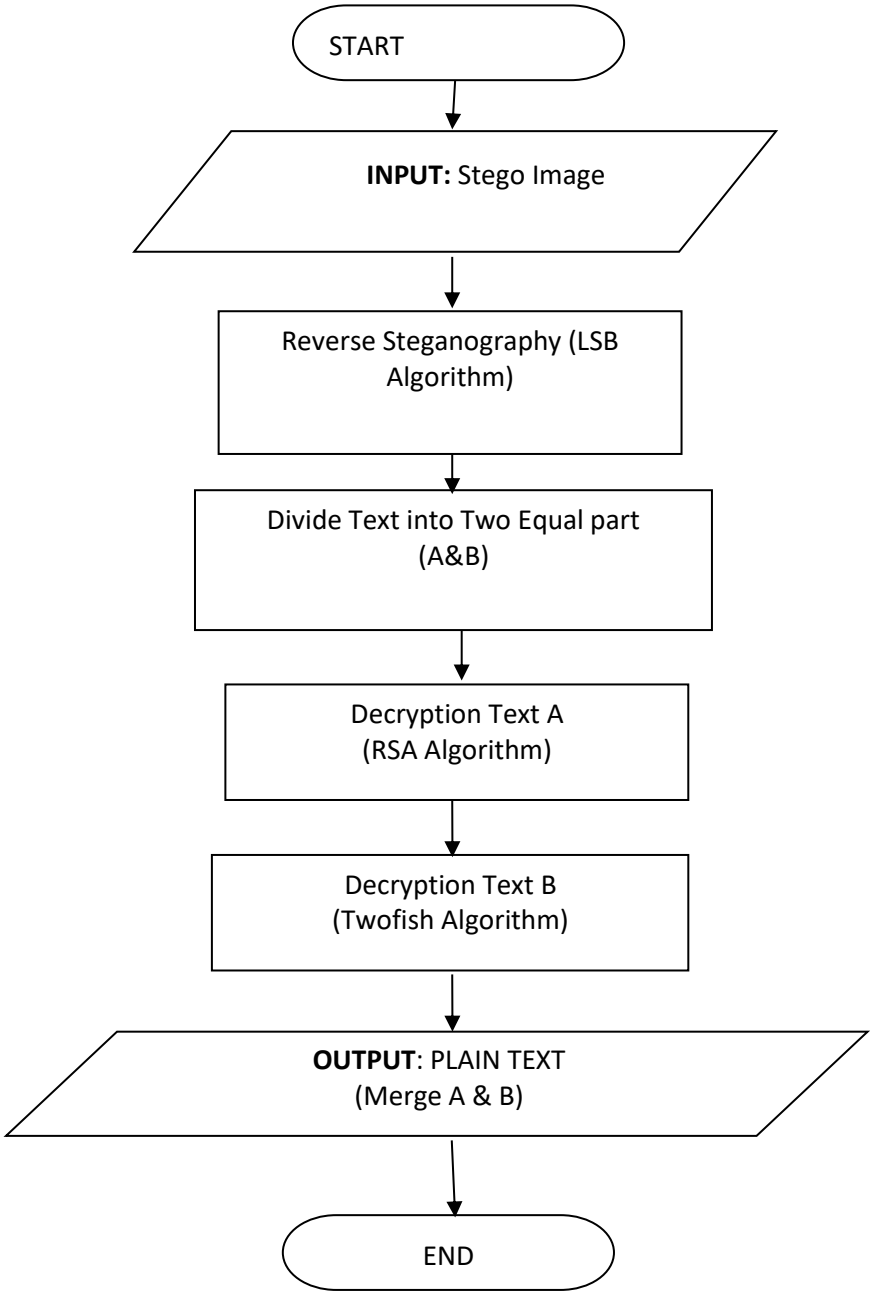


Figure 6: Flowchart for Retrieve Data Model

Results (Contribution to Knowledge)

The major contributions of this research to knowledge are:

i. Two layer security techniques i.e. cryptography and image steganograhy. for cryptography, an hybridized RSA and Twofish Algorithm is to be used to encrypt the plaintext into cipher text and

least significant bits (LSB) is to be utilized to insert or shroud information behind some cover media before it is being put away or sent to the expected receiver.

ii. Provide a strict security model to checkmate problem associated with attackers and intruders breaking into an institution's database to fetch information and use for their own benefit or for their own advantage thereby causing havoc to the institution

In the process of this research work, two computers will be are label with username Secure and Retriever for testing. The secret information in form of text, video, audio and image in secure end is secured by means of the combine techniques of steganography and hybridized RSA and Twofish algorithms and also secret information at the retrieving end is retrieve using the combined techniques to provide a model that can guarantee extra security level for data and information in an interactive process so as to withstand attackers

Acknowledgements

The author is grateful to Tertiary Education Trust Fund (TETFUND) Nigeria, for the grant Institutional Base Research (IBR) awarded for this work through the Federal Polytechnic, Mubi, Adamawa State.

REFERENCES

Abari Ovye John, P.B Shola & Simon Philip (2020). *Comparative analysis of Discrete logarithm and RSA Algorithm in data Cryptography.* International Journal of computer Science and Security. *(ISSN 1947-5500 Volume 13-No.2).*

Anil, K (2018), *A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique",* IJARCSSE Volume 3, Issue 7, July 2018.

Amritpal Singh (2020), *An Improved LSB based Image Steganography Technique For RGB Images*. Electrical, Computer and Communication Technologies (ICECCT), 2020 IEEE International Conference, *2020, pp 1-4.*

Bender, W., D. Gruhl, N. Morimoto and A. Lu, (2001). *Techniques for data hiding*. IBM Syst. J., 35: 313-336.

Bishop, M. (2015).*Introduction to computer security.1st ed. Pearson publications.*

Cheddad, A., J. Condell, K. Curran and P. McKevitt (2015). *Digital image Steganography:* Survey and analysis of current methods. Signal Process. 90: 727-752.

Kumar Saurabh & Er.Ravinder Singh Mann (2017). *A comparative Evaluation of Cryptography Algorithms,* Intl. J. Computer Technology and Application Vol. 3(5), 1653-1657, ISSN: 2229-6093, Sept-Oct 2017.

Hussain, M & Hussain M (2018*), "A Survey of Image Steganography Techniques*", International Journal of Advanced Science and Technology Vol. 54, May, 2018, pp 113-124

Mark R. (2018). *The Complete Reference: Information Security* (2nd edition). New York. *McGraw-Hill companies.*

Morkel (2010). *An Overview of image steganography.* Information security South Africa conference (ISSA) research group. *vol.1, no .1.*

Rabah, K. (2009). *Steganography-the art of hiding data,* Inform. Technol. J., 3: 245-269.

Whitman, M.E. & Mattord, H.J. (2016).*Principles of information security.* Thomson course technology.

Zaidoon Kh, A. Zaidan, A.A. Zaidan, B.B & Alanazi. H.O (2015) *Overview: main fundamentals for steganography.* Journal of Computing, 2(3), pp. 40-43.