Vol-9, Issue-2 PP. 20-34 ISSN: 2394-5788

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

DESIGN AND IMPLEMENTATION OF SECURED ONLINE TRANSCRIPT ISSUING AND PROCESSING USING CRYPTOGRAPHY AND STEGANOGRAPHY

Faluyi Bamidele Ibitayo
Department of Computer Science,
Federal Polytechnic Ado-Ekiti,
Ekiti State,
Nigeria.
faluyi_bi@fedpolyado.edu.ng

Akin-Olayemi Titilope Helen
Department of Computer Science,
Federal Polytechnic Ado-Ekiti,
Ekiti State,
Nigeria.
Teeking2001@yahoo.com

Makinde Bukola Oyeladun
Department of Computer science,
Osun State College of Technology,
Esa-Oke Osun State,
Nigeria.
bukolamakinde22@gmail.com

ABSTRACT

Confidentiality and accuracy are two prime concerns of issuers of academic history of any tertiary institution to students, otherwise known as transcript, which in most cases are sacrificed for timeliness of its availability for the purpose of its request. Most Nigerian graduates have forfeited great opportunities that come their ways as a result of late arrival of their transcripts to the requesting agents. In this paper, we propose a processing of online request and sending of academic history to and fro requesting agents and sending institutions using Crypto-steganography which is a combination of Cryptography and Steganography methods of securing information Blowfish algorithm. was used in the Cryptography module Hash-LSB technique was adopted in the Steganography module. With this approach, confidentiality of the document is ensured while the receiving agents also receive the document in good time. Use Case Diagram was used as design tool while Python was used to implement the scheme.

Keywords: Cryptography, Steganography, Blowfish algorithm, python, encryption, decryption, transcript

1. INTRODUCTION

Transcript is documentation of a student's permanent academic record, which usually means all courses taken, all grades received, all honors received and degrees conferred to a student. In the internet age, all our daily life actions have been managed electronically using huge number of coputers connected by internet network. These electronic actions include e-commerce, online banking, online booking of air flight tickets, students registering in the tertiary institutions and online applying for visa. All these activities need to produce and manage documents digitally, an example on these documents, including university transcripts, letters and business contracts (Fischer and Herfet, 2006; Abboud, 2015; Ayodele et al, 2018). Producing digital documents electronically is more suitable and simpler than paper documents and also dealing with paperless documents is far better because of the ease of editing, searching and storing of them (Fischer et.al, 2007; Abboud, 2015; Olukemi Sadeet.al, 2018). In addition, making these documents available digitally in the computer networks permit them to be transmitted and processed electronically (Fischer and Herfet, 2006; OgunlolaOkunolaOlasunkanmiet.al, 2018). However, releasing documents in the networks exposes them to different types of attacks, hackers and threats, hence; protecting digital documents is very significant matter in the networked society (Abboud, 2015; BamideleIbitayoFaluyi et.al, 2018)

In the transcript, you can usually see:

i. The course unit code,
ii. The title of the courses,
iii. The duration of the course,

iv. The grade (your exam mark)

Steganography is a form of science that deals with cryptic information. It is the art of writing in cryptic text that is unrecognizable to a person who doesn't hold the key to decrypt it.

Steganography is not a new form of science. In fact, Steganography is derived from the Greek word "steganos", which means hidden or secret and "graphy" means writing or drawing. Thus, steganography means secret writing. In contemporary terms, steganography has evolved into a digital strategy of hiding a file in any form of multimedia such as an image, an audio file or even a video file. (Kavitha2012; Sanjay Burman, 2019).

Cryptography and steganography are well known and widely used techniques that manipulate information in order to cipher or hide their existence respectively. Cryptography scrambles a message so it cannot be understood; the steganography hides the message so it cannot be seen. Cryptography is not sufficient for secured communication. The power of steganography is in hiding a secret message by obscurity, hiding its existence in non-secret file. In that sense, steganography is different from cryptography, which involves making the content of the secret, message unreadable while preventing non-intending observers from learning about its existence (KshitizRastogi, 2018)

These two techniques have been used to protect information since ancient times, but only individuals and organizations with extraordinary need for confidentiality like the military government and institutions had bothered to exert the effort required to implement it. (Venkata2007; Maroof Ali *et.al*, 2018). However, as time passed and need for information security grew larger in everyday businesses, cryptography and steganography became the important tools for securing data from the sender to the receiver. (Ansderson2010; Ravi Kumar, Ahtisham Hashmi2019)

The basic concepts are Encryption and Decryption. In cryptography, encryption is the conversion of information in readable form (text), into an unreadable form called cipher text, which is impossible to read except by those that possess the secret key or appropriate knowledge to decipher the message and decryption is the transformation of the cipher text back to its original form. (Denning 2002; Abdel-Karim, A. T.2020). While in Steganography, Encryption is the art of embedding a message, image, or file within another message, image or file (text, audio, image, video) and Decryption is the art of extracting the embedded data from inside the cover data. (Katzenbeisser2011; Domenico, B. 2018)

Cryptography scrambles a message so it cannot be understood; the Steganography hides the message so it cannot be seen.

Cryptography and Steganography both provide security, the use of only one method at a time will not be sufficient for a secured communication, however, it is a good practice to combine the two methods together for adding multiple layers of security. By combining, the data encryption can be done by a software and then embed the cipher text in an image or any other media. The combination of these two methods will enhance the security of the data embedded. (Luca 2013;S. Panwar, S. *et.al* 2018). This combined chemistry will satisfy the requirement such as confidentiality, security and robustness for secure data transmission over an open channel.

According to Markus Kahn's definitions, Steganography is the ability and knowledge of communicating in a way which hides the existence of the secret message. There are three different aspects in hiding the information techniques challenge with each other; capacity, security, and robustness. The steganography strives more for high security and capacity. The aim for high security means that focus is to secure the hidden transcript in a cover medium while capacity refers to the size of the transcript that can be hidden in a cover medium. There are four categories of cover medium digital files that can be used in steganography techniques which are text, image, audio/video, and protocol. However, the more appropriate formats to use are image and audio file formats because of their high degree of redundancy. The basic model of the steganographic process using image format in illustrated below.

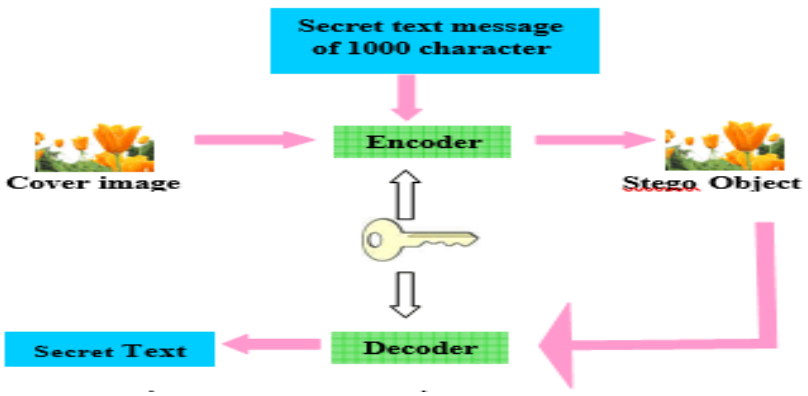


Figure 1:The basic model of steganographic process using image format, source: (Anderson 2005**)**

These techniques have become much more open and public in the last few years. (Anderson 2005; Mamoun 2018). The steganography and cryptography are better techniques for data hiding which manipulates information (data) in order to cipher or hide their existence.

The steganography technique aims to prevent a third party from realizing that any covert communication has taken place, it was believed to be first practiced during the Golden Age in Greece where messages were inscribed on the underlying wood of the wax tablet. Only persons who have knowledge of the embedded information and possess a "key" will be able to decode and view the information. This key can take many forms which can range from a passphrase for electronic steganography to an understanding of a method to decode the information. In the modern day sense of the word steganography, is usually refers to information or a file that has been concealed inside a digital picture, video or audio file and sent through the network to the recipient, where the actual message is separated from it. (Luca 2013; Olukemi Sade 2019).In the case of cryptography, it stores and transmits data in a form so that it can no more be interpreted or understood. It is a way of protecting sensitive information as it is stored on media or transmitted through network communication paths, which made government organizations, military units, and some corporate houses to adopt its use. They used cryptography to guard their secrets from others, just like steganography, the parties must possess a key to be able to get the information. Some techniques of early cryptography are the hieroglyph, Caeser Shift Cipher, Vigenere Coding used by the Egyptians, Romans and various Italian and Papal States respectively.

The hidden message is plain, but unsuspecting to the reader. Steganography's intent is to hide the existence of the message, while cryptography scrambles a message so that it cannot be **understood. (Kumar 2010; Ayodeji 2019).**

2. LITERATURE REVIEW

Transcript is documentation of a student's permanent academic record, which usually means all courses taken, all grades received, all honors received and degrees conferred to a student. In the internet age, all our daily life actions have been managed electronically using huge number of computers connected by internet network. These electronic actions include e-commerce, online banking, online booking of air flight tickets, students registering in the tertiary institutions and online applying for visa. All these activities need to produce and manage documents digitally, an example on these documents, including university transcripts, letters and business contracts (Fischer and Herfet, 2006; Abboud, 2015; Ayodele*et.al*, 2018). Producing digital documents electronically is more suitable and simpler than paper documents and also dealing with paperless documents is far better because of the ease of editing, searching and storing of them (Fischer et al, 2007; Abboud, 2015; Olukemi Sade*et.al*, 2018). In addition, making these documents available digitally in the computer networks permit them to be transmitted and processed electronically (Fischer and Herfet, 2006; Ogunlola Okunola Olasunkanmi*et.al*, 2018). However, releasing documents in the networks exposes them to different types of attacks, hackers and threats, hence; protecting digital documents is very significant matter in the networked society (Abboud, 2015; Bamidele Ibitayo Faluyi *et.al*, 2018)

Tyagi (2002) described a method for integrating cryptography and steganography together through image processing. The work started by clarifying the way for encryption of the secret text before hiding it in the image. Then, the encrypted data is to be hidden in the image through the least significant bit (LSB) image-based steganography.

Bamidele Ibitayo Faluyi *et.al*, (2018), proposed a solution for transferring academic transcript with-out any compromise in security over an in secure channel. In our proposed system, we select a true colour image of size 512 x 512 as a cover image and a secret message (transcript) which is embedded in the true colour image. The secret message (transcript) is encrypted using RSA algorithm, the encrypted (secret message - transcript) is embedded in the Least Sig-nificant Bit (LSB) of each Red, Green and Blue (RGB) pixel value of the cover image.

Bloisi and Locchi (2007), proposed image steganography and cryptography system (ISC) for securing data transfer. He used images as cover objects for steganography and secret key for the cryptography. The performance of the proposed image-based steganography and cryptography system was presented in his work. He compared his results with another algorithm in the literature known as F5 showing improved results. It was found that the comparison with F5 is replacing the least-significant bit of a DCT coefficient with message data which may be degrading and fairness of the analysis. Domenico's work makes F5 decrements its absolute value in a process called matrix encoding claiming as a theoretically unbreakable cryptographic method based on image based one-time pad steganography.,

Mohammad in (Jain *et.al*, 2012) proposed a technique to implement steganography and cryptography together to hide the data into an image by two steps. The first step, finds the shared stego-key between the two communication parties by applying Diffle Hellman Key exchange protocol. The second step makes the sender use the secret stego-key to select pixels that will be used to hide secret data. Each selected pixel will be used to hide 8 bits of data by using LSB method. Although the method showed real interesting security features, it was very complicated with high unpractical overhead. Harshitha and Vijaya (2012), proposed a security method in which the secret message is first encrypted and then hidden in a cover file with steganography. The encryption of the message is

randomly permuted using the secret key. The steganography used was based on the LSB algorithm for both embedding and extraction process. All the testing results showed interesting features generated by Matlab experimentations.

(Yang *et.al*, 2009) presented a new adaptive LSB based method for image steganography. It uses the pixel adjustment technique for better stego image quality. This adaptive LSB substitution results in high hidden capacity.

Sachdeva and Kumar (2012) used the vector quantization table to embed the secret information by which the hidden capacity and stego size is increased. A last explored method hiding encrypted secret message inside a cover file has been introduced by Nath, (2011). He proposed an algorithm for encrypting the secret message with relation to the work proposed in (Nath, 2010). The work modified the idea of play fair method into a new platform where they can encrypt or decrypt any file.Their method is dependent on the random text-key which is to be supplied by the user. They introduce a new randomization method for generating the randomized key matrix to encrypt plain text file and to decrypt cipher text file. They also introduce a new algorithm for encrypting the plain text multiple times, increasing security by increasing system complexity.

Overview of Steganography

Steganography is the ability and knowledge of communicating in a way which hides the existence of the secret message. The main goal of steganography is same to cryptography but in a different way, which is focused on securing the hidden information. The specific goal of steganography is hiding data in a digital object so that existence of the secret message cannot be detected through observation (or even complex analysis).

There are many stories about steganography. For example, ancient Greece used method for hiding messages such as hiding it in the belly of a dare (a kind of rabbits), using invisible ink and pigeons. Another ingenious method was to shave the head of the messenger and tattoo a message or an image on the messenger's head. After allowing his hair to grow, the message would be undetected until the head is shaved again, while the Egyptians used illustrations to conceal message. (Kallam *et.al*, 2010).

The goal of steganography is to hide secret information inside cover images in such a way that does not allow any "enemy" to even detect that there is a secret message present in the image. Steganography attempts to hide the presence of communication. The steganography structure is made up of three elements:

i. The cover image,
ii. The secret image,
iii. The key

The cover image can be a painting, or a digital image. It is the object that will carry the hidden message. A key is used to decode the secret message. This can be anything from a password or a pattern. Steganography is applied to images, but many other data or file types are possible.

i. Audio
ii. Video
iii. Text
iv. Executable programs.

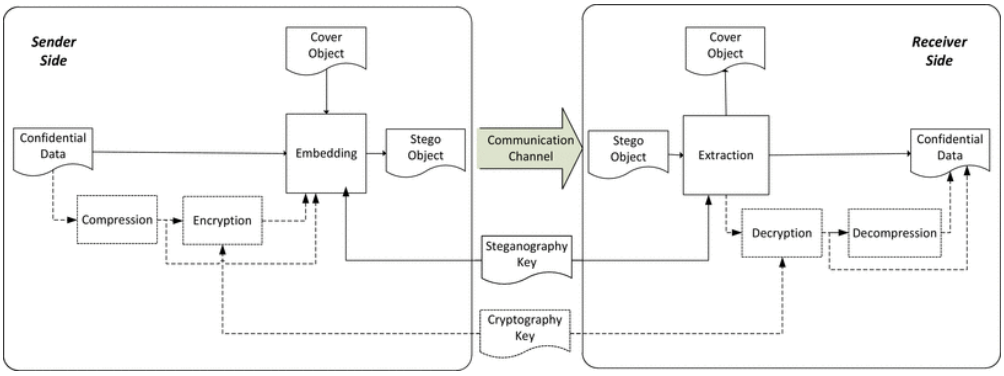


Figure 2: General Steganography Model. (Source: FridrichMchn 2013)

Image Steganographic Techniques

Image streams have high degree of spatial and temporal redundancy in representation and have pervasive applications in daily life, thus they are considered as good candidates for hiding data. Image steganography can be then employed in various useful applications. One application use image steganography for military and intelligence agencies communications. Another type of

application was demonstrated by Robbie et al, and Lie et al, where data hiding in image was used for image error correction during transmission or for transmitting additional data (e.g subtitles) without requiring larger band-width. A different application was presented by (Zhang *et.al*, 2012) where image steganography was used for hiding data in an image captured by a surveillance system. That is, in order to protect the privacy of authorized people, their images are extracted from the surveillance image and embedded in its background.

Generally speaking, image steganography is the extension of image steganography.an image file can simply be viewed as a sequence of images, yielding image data hiding similar to image data hiding. In addition to the image attacks that can be applied on the separate frames of image; there are much more attacks for images such as loss compression, change of frame rate, formats interchanging, addition or deletion of frames during image processing. Handling an image stream as multiple two-dimensional images, does not consider the dependencies that exist among pixels in their three dimensions. The hiding capacity is much higher in the case of image. Images provide new dimensions for data hiding such as hiding messages in motion components. The audio components of the image file can also be utilized for data hiding. Focusing on image steganographic techniques, we can classify them in a number of ways. One way is to categorize them according to compression, i.e. compressed image techniques and uncompressed (raw) image techniques; this classification was adopted by another classification that can be used based on the domain of embedding, i.e. spatial domain techniques and transform domain techniques.

Moreover, Shirali-Shahreza suggested categorizing image steganographic techniques according to the following criteria: considering the image as a sequence of still images or finding new dimensions in the image that help on the steganographic process or utilizing the image saving format for information hiding.

Elements of Steganography

There are two important elements in steganography; cover and data. The cover is a medium to carry hidden messages during transmission without showing the existence of the hidden message. Because of that, the appropriate cover must be chosen, as it is a large part of what determines the efficiency of the steganographic technique. Appropriate cover means that there is no suspicious look at that cover. Once the attacker suspects something to that cover, it means the hidden message will be attacked.Then, the data is the hidden message that will be hidden in the cover. The data must be serializable, so that it may be embedded bit by bit into the cover. Steganography offers high carrier capacity keeping embedded message invisible and maintaining the fidelity of the cover media. The efficiency of the steganographic method is that one shouldn't know that the media file has been altered in order for embedding. If the malicious user knows there is some alteration, the steganographic method is defeated and less efficient. The embedded message is very fragile and hence if any modification is done to the stego image the whole secret message is corrupted. The effectiveness lies on the ability to fool an unintended user. The layers of communication can be more than one layer. A secret message can be embedded within a digital image which in turn can be embedded within another digital media or image clippings.

Least Significant Bit (Lsb)

Least Significant Bit is an example of the main techniques in spatial domain image steganography. It manipulates the cover digital image pixel bit value to embed the encrypted secret message. The encrypted message bit will be embedded in the least significant bit of the image pixel. Steganography avoids introducing as much various as possible, to minimize the likelihood of detection.

The embedding process consists of choosing a subject {j1…..j1(m)} of cover elements and performing the substitution operation cji_mi on them, which exchange the LSB of cji by mi (mican either be 1 or 0). In the extraction process, the LSB of the selected cover-element is extracted and lined up to reconstruct the secret message. (Alan *et al*., 2005).

Palette-Based Image

There are two ways to encode information in a palette-based image; either the palette or the image data can be manipulated. The LSB of the colour vectors could be used for information transfer, just like the substitution methods presented, alternatively, since the palette does not need to be sorted in any way, information can be encoded in the way the colours are stored in the palette. For N colours since there are different ways to sort the palette, there is enough capacity to encode a small message. However, all methods which use the order of a palette to store information are not robust, since an attacker can simply sort the entries in a different way and destroy the secret message. (Alan *et.al*, 2005)

Transform Domain Techniques

Transformation domain methods hide message in a significant area of the cover image which makes them more robust to attack, such as adding noise, compression, some image processing. However, cropping whereas they are more robust to various kinds of signal processing, they remain imperceptible to the human sensor system. Many transform domain variations exist. One method is to use the Discrete Cosine. Katzembeisser (2011)

Spread Spectrum (Ss) Techniques

Spread spectrum techniques are defined as "means of transmission which the signal 30 occupies a bandwidth in excess of the minimum necessary to send the information". The .band spread is accomplished by means of a code which is independent of the data, and a synchronized reception with the code at the receiver is used for dispreading and subsequent data recovery. Katzembeisser (2011)

Cover Generation Techniques

In contrast to all embedding methods presented above, when secret information is added to a specific cover by applying an embedding algorithm, some steganographic applications generate a digital object only for the purpose of being a cover for secret communication. Katzembeisser (2011).

CRYPTOGRAPHY

History of Cryptography

The art of cryptography is considered to be born along with the art of writing. As civilization evolved, human beings got organized in tribes, groups, and kingdoms. This led to the emergence of ideas such as power, battles, supremacy, and politics. These ideas further fueled the natural need of people to communicate secretly with selective recipient which in turn ensured the continuous evolution of cryptography as well. Singh (2009). The roots of cryptography are found in Roman and Egyptian civilizations.

The oldest cryptographic technique, the first known evidence of cryptography can be traced to the use of 'hieroglyph'. Some 4000 years ago, the Egyptians used to communicate by messages written in hieroglyph. This code was the secret known only to the scribes who used to transmit messages on behalf of the kings. Ellis (2015).

Later, the scholars moved on to using simple mono-alphabetic substitution ciphers during 500 to 600 BC. This involved replacing alphabets with some secret rule. This rule became a key to retrieve the message back from the garbled message. The earlier Roman method of cryptography, popularly known as the Caeser Shift Cipher, relies on shifting the letters of a message by an agreed number (three was a common choice), the recipient of this message would the shift the letters back by the same number and obtain the original message. Gardner (2012)

Concept Used In Cryptography

i. **Plain Text:** It is the information present in its original format.
ii. **Cipher Text:** Conversion of plain text to non-readable format.
iii. **Encryption:** Transformation from plain text to cipher text. Encryption algorithm and a key are important in encryption.
iv. **Decryption:** Transformation of cipher text to plain text. Decryption algorithm and key is needed.
v. **Key:** Combination of numeric or alpha-numeric text or special symbol.

There are two types of encryption methods in cryptography as follows:

i. Symmetric Encryption
ii. Asymmetric Encryption

In Symmetric Encryption one key is shared between transmitter and receiver. For conversion of plain text into cipher text at sender or transmitter used to improve security level to protect the secure information use one key that same key is used at receiver side to convert cipher text to plain text.

In Asymmetric Encryption system was developed by Diffie and Helman in 1976 it's also called as Public Key Cryptography. It is the process where conversion of plaintext to cipher text from the sender with different key will be used to retrieve the secured data from cipher text to plaintext. Public key is used by the sender for encryption and at the receiver side, a different key is used for decryption.

Context of Cryptography

Cryptology, the study of cryptosystems can be subdivided into two branches:

i. Cryptography
ii. Cryptanalysis

Cryptography is the art and science of making cryptosystem that is capable of providing information security. Cryptography deals with the actual securing of digital data. It refers to the design of mechanisms based on mathematical algorithms that provide

fundamental information security services. Fiestel (2013). You can think of cryptography as the establishment of a large toolkit containing different techniques in security applications. (Menezes *et.al*, 2014)

What Is Cryptanalysis?

The art and science of breaking the cipher text is known as cryptanalysis. Cryptanalysis is the sister branch of cryptography and they both co-exist. The cryptographic process results in the cipher text for transmission or storage. Biham and Shamir (2018). It involves the study of cryptographic mechanism with the intention to break them. Cryptanalysis is also used during the design of the new cryptographic techniques to test their security strengths. Diffie and Hielman (2018).

3. SYSTEM DESIGN

System analysis is problem solving techniques that decompose a system into its component piece for the purpose of studying well how those component parts works and interact to accomplish their purpose. Large amount of information has been achieved by research methodologies; this information is then organized and analyzed before a new design. The purpose of system analysis is to ascertain what must be carried out of the system.

The Research Methodology

The new method being proposed is a hybrid system which merges the cryptography and steganography methods and is divided into two different layers namely;

i. Crypto-layer which makes use of the Rivest, Shamir, Blowfish algorithm where the sensitive text is going through the symmetric key encryption using Blowfish algorithm. The secret key is used in encryption is also needed during the decryption process when retrieving of the data is desired. The new system AES key length is fixed to 128 bits which results in 10 rounds of crypto layer operations.

ii. Stego-layer which adopts the image based steganography as in [8] which hides the encrypted data coming out of the cryptography layer in the image.

System Architecture

The two-layer system comprises of two modules namely; hiding the data and retrieving the data. In the hiding module, the crypto-layer hides the data using the blowfish algorithm. The data is further hidden in the stego-layer which uses the Least Significant Bits of pixel value. The secret key used in encryption process is needed as in the decryption process when retrieving the data is desired.

The system will hide encrypted text into an image file. The system first makes an image file as carrier file and accepts any secret text to hide into it. It uses blowfish algorithm to encrypt secret text before hiding it into the image.

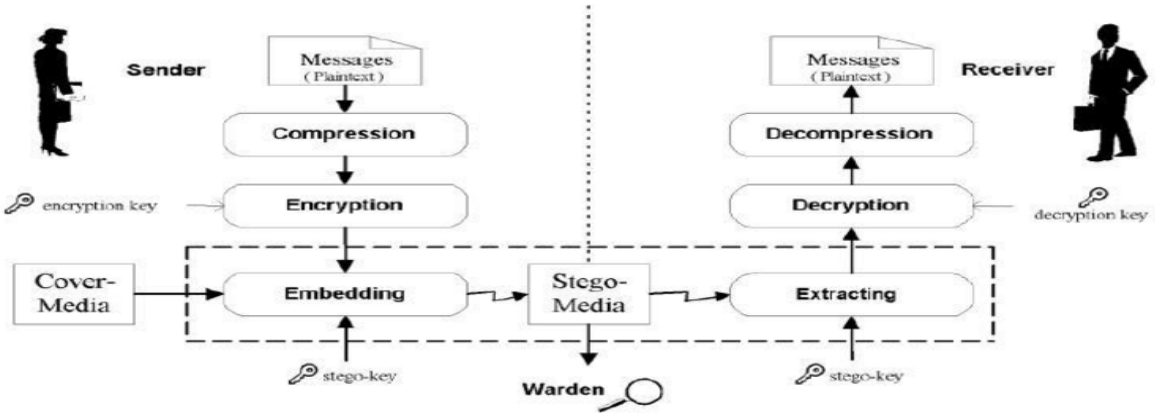


Figure 3: Combination of Cryptography and Steganography, source: (Black, et al, 2010***).***

The retrieving module involves extracting the LSBs from the stego-image to reveal the cipher text and then the generated key is checked to see if it is correct before decrypting the key to reveal the plain text. The architecture of the system can be represented in a flow diagram shown below:

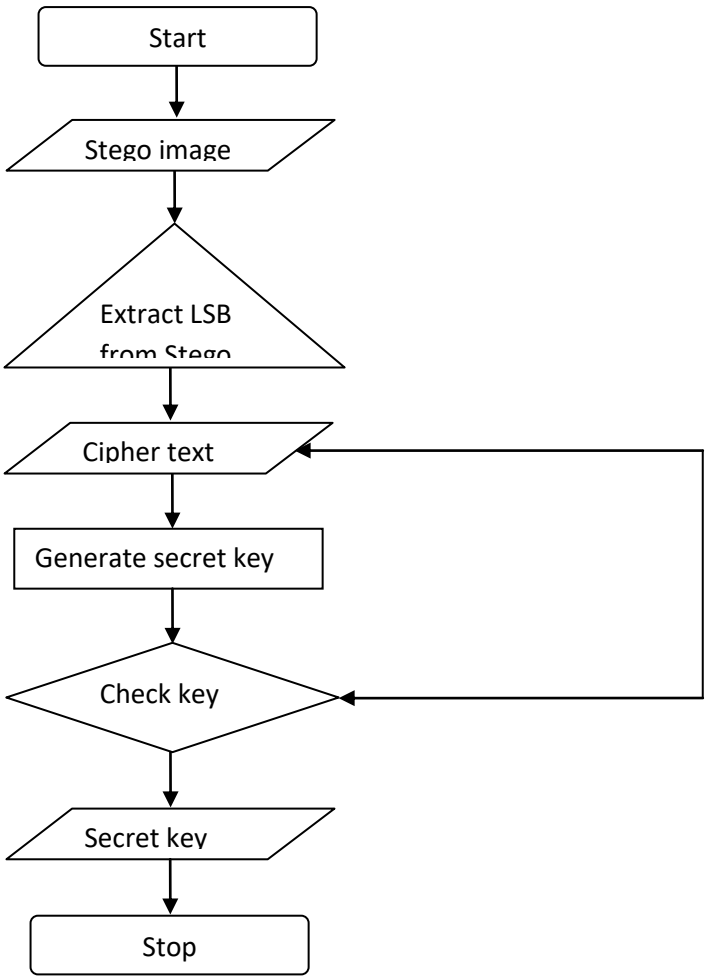


Figure 4: Flowchart for retrieving the integrated data

Analysis Of The Proposed System

The proposed system uses blowfish algorithm to encrypt the transcript before hiding it into an image. The secret transcript has a zero percent chance of been detected. It is more user-friendly and less rigid, contains a self-help page for users who are new to it.

Advantages

i. Ease of use and user friendly
ii. Not only embeds but encrypts data
iii. No change in size of cover data
iv. Absence of data loss
v. No detection of the presence of secret message
vi. Protects embedded message from being extracted by outsiders with the help of encryption key.

Modules of The Proposed System

There are total of two modules in the proposed system which is explained below:

i. **Encryption and Embedding Module:** This is the part of the system that performs the embedding and encryption process. It allows users to create an encryption key, encrypt data with the help of blowfish algorithm and then embed the data cover in the cover medium.
ii. **Decryption and Extraction Module:** This part of the system performs the decryption, and also extracts the embedded data from the cover medium. This module checks if the decryption key provided by the receiver or user correlates with the encryption key. If it doesn't, the data will not be extracted.

A comparison is made between the original file and the embedded one to indicate that less distortion is made even after changing the LSB bit of the original file.

Least-Significant Bit (Lsb) Technique

The least significant bit (in other words, the 8thbit) of some or all bytes inside an image is changed to a bit of the secret message. Digital images are mainly of two types:

i. 24-bit images and
ii. 8-bit images

In 24-bit images we can embed three bits of information in each pixel, one in each LSB position of the three 8-bit values. Increasing or decreasing the value by changing the LSB does not change the appearance of the image; much so the resultant stego image looks almost same as the cover image. In 8-bit images, one bit of information can be hidden.

A stego-image is obtained by applying LSB algorithm on both the cover and hidden images. The hidden image is extracted from the stego-image by applying the reverse process. If the LSB of the pixel value of cover image C(ij) is equal to the message bit m of secret message to be embedded, C(ij) remain unchanged; if not, set the LSB of C(i,j) to m. the message embedding procedure is given below:

S(ij) = C(ij) – 1, if LSB(C(I,j)) = 1 and m = 0
S(ij) = C(ij), if LSB(C(ij)) = m
S(ij) = C)ij) + 1, if LSB(C(ij)) = 0 and m = 139

Where LSB(C(i.j)) stands for the LSB of cover image C(ij) and m is the next message bit to be embedded. S(ij) is the stego-image. As we already know each pixel is made up of three bytes consisting of either a 1 or a 0.
For example, suppose one can hide a message in three pixels of an image (24-bit colors).
Suppose the original 3 pixels are:
(111010101110100011001011)
(011001101100101011101000)
(110010010010010011101001)

In this case, only four bits needed to be changes to insert the character successfully. The resulting changes that are made to the least significant bits are too small to be recognized by the human eye, so the message is effectively hidden. The advantage of LSB embedding is its simplicity and many techniques use these methods.
The following figure shows the mechanism of LSB technique:

LSB Insertion Mechanism

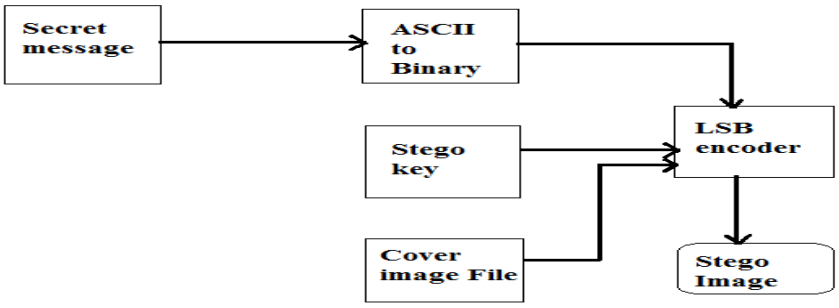


Figure 5: LSB insertion mechanism, source: (P.Malathi 2016)

LSB Extraction Mechanism

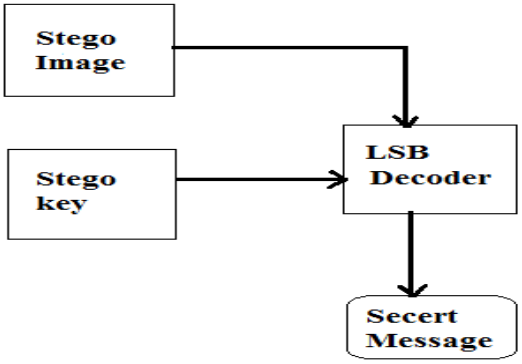


Figure 6: LSB Extraction Mechanism, source: (Darshana Patil 2017)

Data Embedding

The embedding process is as follows.
Input: Cover image, stego-key and the text file
Output: Stego-image

Procedure For Data Embedding

Step 1: Extract the pixels of the cover image.
Step 2: Extract the characters of the text file.
Step 3: Extract the characters from the stego-key.
Step 4: Choose first pixel and pick characters of the stego-key and place it in the first component of the pixel.
Step 5: place some terminating symbol to indicate end of the key. 0 has been used as a terminating symbol in this algorithm.
Step 6: Insert characters of text file in each first component of next pixels by replacing it.
Step 7: Repeat step 6 till all the characters has been embedded.
Step 8: Again place some terminating symbol to indicate end of data.
Step 9: Obtain the stego-image.

Data Extraction

The extraction process is as follows:
Inputs: Stego-image file, stego-key
Output: Secret message

Procedure For Data Extraction

Step 1: Extract the pixel of the stego image.
Step 2: Now, start from first pixel and extract stego key characters from first component of the pixels. Follow Step 3 up to terminating symbol, otherwise follow step 4.
Step 4: If this extracted key matches with the key entered by the receiver, then follow Step 5, otherwise terminate the program.
Step 5: If the key is correctly, then go to next pixels and extract message characters from first component of next pixels. Follow step 5 till up to terminating symbol, otherwise follow step 6.
Step 6: Extract the secret message.

Embedding Algorithm

In this process of coding method, a random key is used to randomize the cover image and then hide the bits of a secret message into the least significant bit of the pixels within a cover image. The transmitting and receiving end share the stego-key and random-key. The random-key is usually used to seed a pseudo-random generator to select pixel locations in an image for embedding the secret message.
Inputs: Cover image, stego-key and the message
Output: Stego-image

Procedure For The Embedding Algorithm

i. Read character from text file that is to be hidden and convert the ASCII value to the character into equivalent binary value into an 8-bit integer array.
ii. Read the RGB colour image (cover image) into which the message is to be embedded
iii. Read the last bit of red pixel
iv. Initialize the random key and randomly permute the pixels pof cover image and reshape into a matrix.
v. Initialize the stego-key and XOR with text file to be hidden and give message
vi. Insert the bits of the secret message to the LSB of the Red plane's pixels
vii. Write the above pixel to stego image file

Extraction of The Hidden Message

In this process of extraction, the process first takes the key and then random-key. These keys takes out the points of the LSB where the secret message is randomly distributed. Decoding process searches the hidden bits of a secret message into the least significant bit of the pixels within a cover image using the random key. In decoding algorithm the random-key must match i.e. the random-key which was used in encoding should match because the random key sets the hiding points of the message in case of encoding. Then receiver can extract the embedded messages exactly using only the stego-key.

Message Extraction Algorithm

Inputs: Stego-image file, stego-key, random key.
Output: Secret message

Procedure for Message Extraction

i. Open the stego image file in read mode and from the Image file, read the RGB colour of each pixel
ii. Extract the red component of the host image
iii. Read the last bit of each pixel
iv. Initialize the random key that gives the position of the message bits in the red pixel that are embedded randomly
v. For decoding, select the pixels and extract the LSB value of red pixels
vi. Read each pixels then content of the array converts into decimal value that is actually ASCII value of hidden character
vii. ASCII values got from above is XOR with stego-key and gives message file, which we hide inside the cover image.

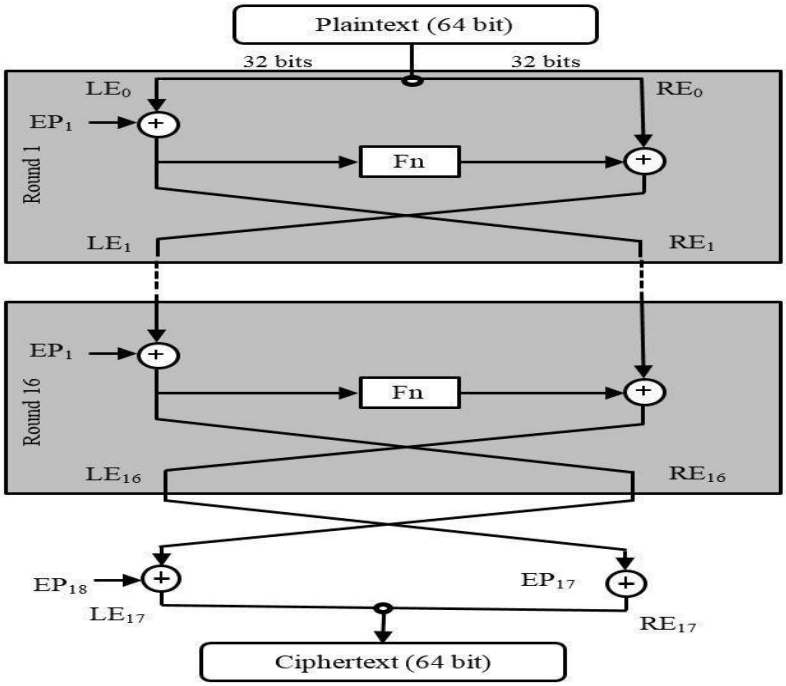


Figure 7: Blowfish Encryption Algorithm, source: (Muhammad Faheem Mushtaq et.al, 2017)

4. SYSTEM IMPLEMENTATION

Running the system implementation begins with the software asking for the secret sensitive text data message and the secret key, which is representing the starting operation of the crypto layer. Within this layer process, the program converts each character of the sensitive secret text into an array of binary bytes to be encrypted using blowfish algorithm. The second layer, i.e. steganography layer, also asks for an RGB image as cover media, such that its pixels are also converted into binary form.

This stego-layer can start its process at the same time while crypto layer is running, i.e. preparing the image as binary bits, but cannot start hiding data except after cipher text is generated from the crypto layer. Each pixel within the RGB image has three channels, namely red, green and blue (RGB) representing a byte of 8-bits each. Therefore, using the least significant bits (LSB) image based steganography in our original system hides three channels.

Advantages Of The Hybrid System

i. **Ease of Use:** the system should be simple and easy to use. Documentation of user manual should be provided to the users, to ensure that the users are able to use and operate the system by themselves.
ii. **Maintainability:** Maintainability is the ease with which a program can be corrected if an error is encountered, adapted if its environment changes, or enhanced if the customer desires a change in requirement. In order to make the system easily maintained, the program must be easily understandable by the maintenance programmer and easily modified and tested when updating is done to meet new requirements, rectifying a deficiency or correcting errors.

iii. **Reliability:** Reliability is the extent to which a program can be expected to perform its intended function with requirement precision. This system should be reliable, where it does not produce dangerous or costly failure when it is used in a reasonable manner.

iv. **Robustness:** Robustness refers to the ability of the system to be able to handle or continue in operation when faced with unexpected circumstances such as handling improper data. The system should be robust enough to handle anticipated or unanticipated error.

v. **Response Time / Speed:** The system should be able to process any transaction at the highest speed and avoid unnecessary interaction. At a low response time, the users may feel frustrated and decide not to use the system.

vi. **Security:** This system should have security measures to minimize the risk of data exposure to unauthorized user. Only the authorized users with the correct login and password are allowed to access and manipulate the data kept in the database.

vii. **User-Friendly:** A user friendly interface enables the users who are with or without technical background able to operate and use this system. A user friendly system will satisfy users and allow interaction with this website and able to utilize this system to the maximum.

viii. **Correctness:** Correctness refers to the degree to which the software performs its required function. Thus, programs for the system must be operating correctly for the user to retrieve the desired outputs. To ensure this system quality, numerous testing and trial-and-errors were carried out.

Program Screenshot

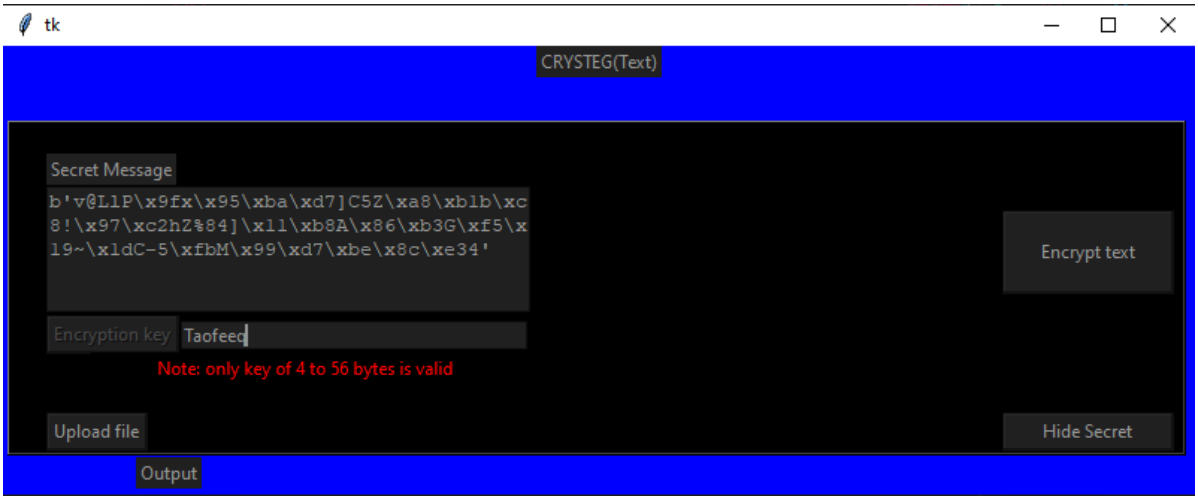
Encryption and Steganography

This reveals the content of the encryption option. Here, the sender uploads the transcript he/she wants to send using the "upload file" option.

Encryption and steganography phase

Text Encryption

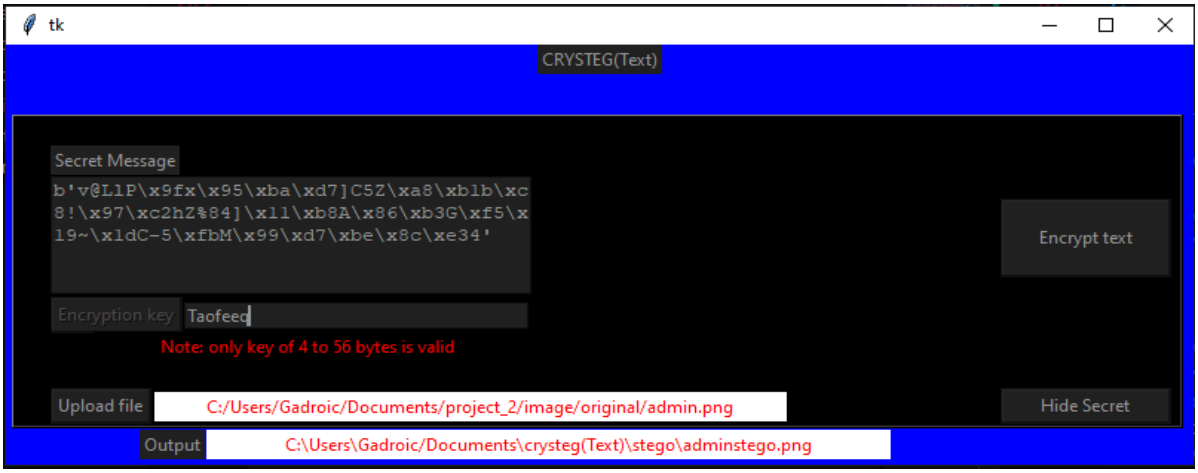
The sender inputs the symmetric encryption key after the transcript has being uploaded and the secret message is encrypted using the user's encryption key.



Text encryption phase

Select Transcript

Here the sender will click on the 'hide secret' option to hide the encrypted text in the uploaded transcript. By doing so, a stego-image is created.

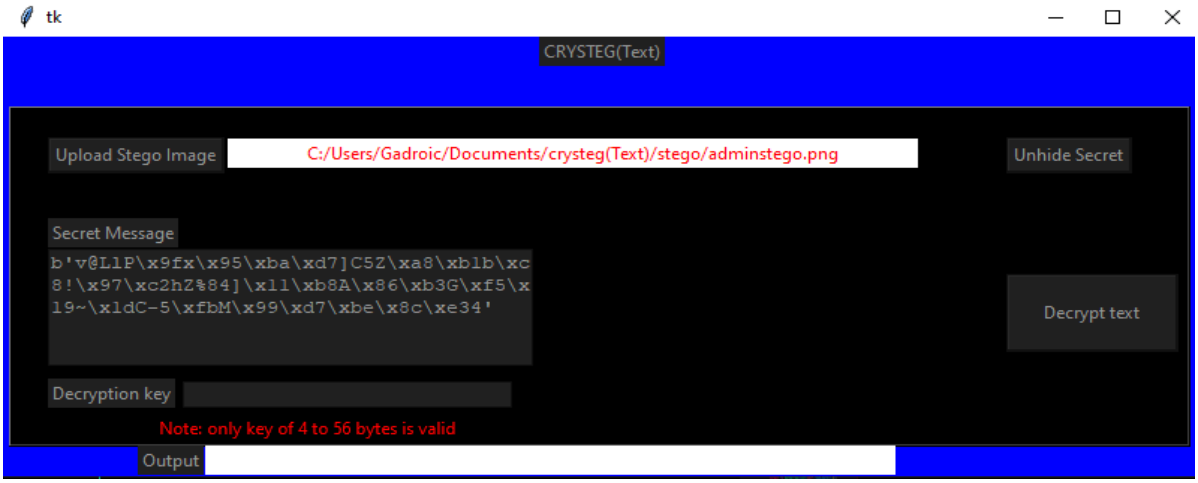


Receiver Opens the Stego Image

The receiver launches the steganography app and opens the stego-image sent to him/her by the sender. By clicking the "unhide secret" option the encrypted secret text is revealed.

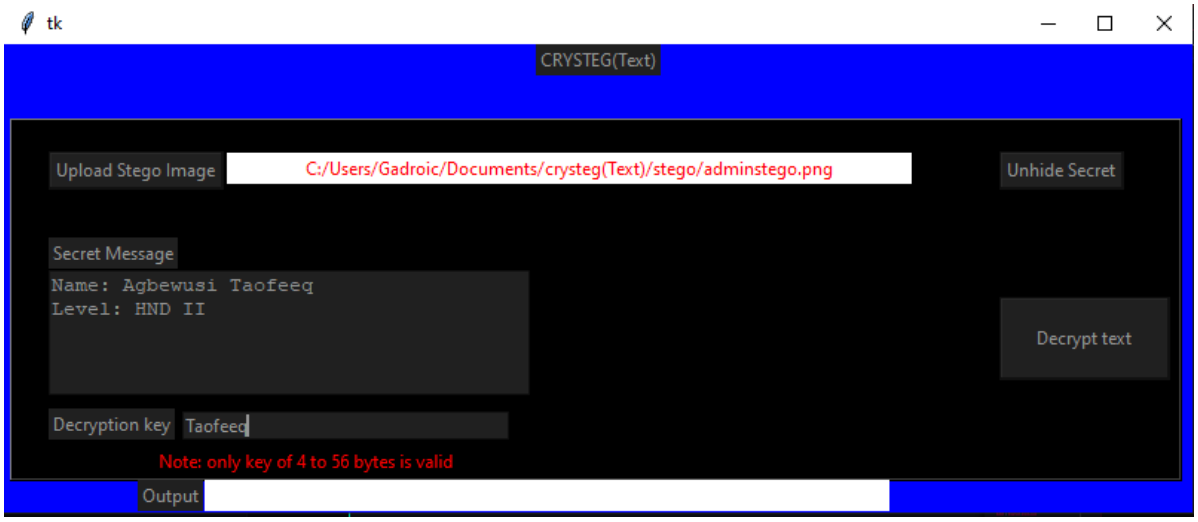
Encrypted Text Is Retrieved

The encrypted text inside the image will be retrieved.



Receiver Inputs the Decryption Key

The receiver then inputs the same encryption key the sender used to encrypt the transcript secret. The encrypted transcript secret is successfully decrypted using the same key by the sender.



Analysis of the Cover Image

Analysis shows that there is no physical difference between the image before and after steganography, however the image extension changed from .jpg to .png, also the final size of the stego image is slightly larger than the size of the original image.

5. CONCLUSION

This work presents a state of the art investigation work in the area of two popular information security approaches, namely cryptography and steganography. However both techniques provides security for secret information, where cryptography modifies the set-up of the information in a way that only its authorized recipient/person can get the text message, while the steganography hides the complete information in the cover media, so no one can easily identify that any message is hidden in the presented content but no one standalone approach is so good for practice. The approach in this project uses a new steganographic approach called image steganography, the application creates a stego image in which the transcript is embedded and is protected with a password which is highly secure. The main intention of the project is to develop a cryptography and steganography application that provides good security.

The approach provides higher security and can protect the message form stego attacks. The image resolution doesn't change much and is negligible when we embed the message into the image, and the image is protected with the personal password. So it's not possible to damage the data by unauthorized personnel. We are using the Least Significant Bit algorithm and Blowfish algorithm in this project for developing the application which is faster, reliable and compression ratio is moderate.

Therefore, to provide more security to the information at the time of communication over unsecured channel a novel advance technique for data security was need, which gave rise to this project which combined cryptography and steganography to ensure the full security of data over an unsecured channel.

REFERENCES

[1] Abboud, A. J. (2015). Protecting Documents Using Visual Cryptography, *3*(2), 464–470.Advanced Steganography Algorithmusing encrypted secret message,JoyshreeNath and AsokeNath,International Journal of Advanced Computer Science and aplication(IJACSA) Vol-2 No.3,Page 19-24 ,March 2011.

[2] Anderson, J.P. (2005). Information security in a multi-user computer environment in advance in computers, New York Vol.12

[3] Alan Siper, Roger and Crag Lombardo, (2005). The Rise of Steganography,*Proceedings of Student/Faculty Research Day, CSIS*

[4] Bajpai, S. and Saxena, K. (2012). Techniques of Steganography for Securing Information : A Survey, *3*(1), 48–54

[5] Biham, E., and Shamir, A. (2003). A Differential Cryptanalysis of the Data Encryption Standard, *New York: Springer-Verlag*, pp. 27-134.

[6] Biham, E., and Shamir, A. (2008). Power Analysis of the key Scheduling of the AES candidates proceedings, *Second AES Candidate Conference,* pp. 27-34.
[7] Bloisi D.D. and Iocchi L. (2007). Image based Steganography and Cryptography, *In VISAPP07,* pp. 17-19.
[8] B.Schneier,Description of a new Variable-Length Key,64-bit Block Cipher(Blowfish)Fast Software Encryption,Cambridge Security Workshop Proceedings(December 1993),Springer-Verlag,1994,pp.191-204.
[9] Chaharlang, M. Mosleh, and S. R. Heikalabad, "A Novel Quantum Audio Steganography-Steganalysis Approach Using LSFQ based Embedding and QKNN-based Classifier," Circuits, Systems, and Signal Processing, vol. 39, pp. 3925-3957, 2020.
[10] Denning, D., (2002). Cryptography and Data Security. Reading, MA: Addisson-Wesley, pp. 27-134.
[11] Diffie W. and Heilman M. (2016). Exhaustive cryptanalysis of the NBS data encryption standard, *Proceedings of the IEEE,* pp. 12-13.
[12] D. M. Ballesteros and J. M. Moreno, "Highly transparent steganography model of speech signals using Efficient Wavelet Masking," Expert Systems with Applications, vol. 39, no. 10, pp. 9141-9149, 2012.
[13] D. Yan, R. Wang, X. Yu, and J. Zhu, "Steganography for MP3 audio by exploiting the rule of window switching," Computers &Security, vol. 31, no. 5, pp. 704-716, 2012.
[14] Ellis, J, (2015). The History of Non-Secret Encryption Cryptologia. *Second AES Candidate conference,* pp. 27-34.
[15] Fiestel, H. (2013). Cryptography and computer Privacy Scientific American. Pp. 7-34.
[16] Gardner, M. (2012). Codes, Ciphers, and Secret Writing. New York: Dover., pp. 2- 34.
[17] Halder, R., Sengupta, S., Ghosh, S. and Kundu, D. (2016). A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique. *18*(1), 39–43.
[18] Harshitha, K.M. and Vijaya, P.A. (2012). Secure data hiding algorithm using encrypted secret message, IJSRP, vol. 2, no. 6.
[19] Jain, V., Kumar, L., Sharma, M., Sadiq, M. and Rastogi, K. (2012). Public key steganography based on matching method. Vol. 3, no. 6
[20] JawaharThakur,Nagesh Kumar, "DES, AES and Blowfish: symmetric key cryptography algorithms simulation based
[21] performance analysis",in International Journal of Emerging Technology and Advanced Engineering Volume1,Issue 2,December 2011.
[22] Kallam Ravindra Babu, Dr. S. Udaya Kumar, Dr. A. Vinaya Babu, (2010). A Survey on Cryptography and Steganography Methods for Information Security, International *Journal of Computer Applications* (0975-8887). Vol. 12, No. 2.
[23] Kavitha, KavitaKadam, AshwiniKoshiti, PriyaDunghav (2012). Steganography Using Least Significant Bit algorithm, *International Journal of Engineering Research and Applications.*
[24] Lars, R., Knudsen, J., and Erik, M. (2002). A chosen plaintext linear attack on DES. *New Jersy: prentice hall inc. press*
[25] M. Tayel, A. Gamal and H. Shawky, "A proposed implementation method of an audio steganography technique," International Conference on Advanced Communication Technology (ICACT), 2016, pp. 180-184, doi:10.1109/ICACT.2016.7423320.
[26] RatinderKaur,V.K.Banga "Image Security using Encryption based Algorithm" International Conference on Trends in Electrical,Electronics and Power Engineering(ICTEEP 2012)July 15-16,2012 Singapore.
[27] Zaidoon kh.AL-Ani, A.A.Zaidan, B.B.Zaidan and Hamdan.O.Alanazi "Overview: Main Fundamentals for Steganography" Journal of computing,Volume 2,Issue 3,March 2010 ISSN 2151-9617.