Global Scientific JOURNALS

GSJ: Volume 8, Issue 5, May 2020, Online: ISSN 2320-9186
www.globalscientificjournal.com

Computer Science and Engineering Journal

INFORMATION PROTECTION AGAINST SECURITY THREATS IN AN INSECURE ENVIRONMENT USING CRYPTOGRAPHY AND STEGANOGRAPHY

Enihe Raphael Ozighor, Ikechukwu Izegbu

Keywords:
Cryptography, Steganography, Information Security, Security Threats.

ABSTRACT

These days almost everyone is using Internet and its applications for communication and transferring data from one point to the other to fulfill their day to day activities whether it is personal or business related. Due to the rapid growth of the technology, Internet is so advantageous and it has become the flexible medium for everyone for their personal and business related matters. Information transfer over the Internet is inherently insecure due to its basic underlying model. The vulnerabilities that exist in the Internet are exploited by security threats to carry out attack on our valuable information thereby compromising their Confidentiality, Integrity and Availability. Hence the need for Information protection against security threats in an insecure environment using cryptography and steganography. Cryptography distorts the message and steganography hides the existence of the message. Combining the strengths of these methods yields an *enhanced method of information protection which will help secure vital, valuable and confidential information communication over the Internet from security threats such as malware, eavesdropping, packet sniffing, information tempering, hackers, unauthorized access etc. We combined Triple DES Cryptography algorithm and the F5 DCT Steganography algorithm in implementing this system using Java (jdk-8u11-windows-x64) programming language and NetBeans IDE8.0 to achieve the enhanced Information Security system.*

1. INTRODUCTION

These days a lot of people are using Internet and its applications for communication and transferring data from one point to the other to accomplish their everyday activities whether it is personal or business related. Due to the rapid growth of the technology, Internet is so advantageous and it has become the flexible medium for everyone for their personal and business related matters. Internet based communications are increasing at a tremendous rate. Data security is a paramount concern in today's networked society that has increased dependence on Internet due to its ubiquity, cost effectiveness and availability. Information transfer on Internet is inherently insecure due to its basic underlying model hence the Internet has become a hostile environment with both wired and wireless channels offering no inherent assurance of confidentiality (Suryakant and Madhav, 2012).

The vulnerabilities that exist in the Internet (being the major insecure environment of information transmission) are exploited by security threats to carry out attack on our valuable information thereby compromising their Confidentiality, Integrity and Availability.

The Integrity, confidentiality and availability of vital and sensitive information (such as bank account statements, personal information, credit card numbers, trade secrets, government documents etc’s) transmitted over the insecure Internet environment can be compromised by security threats such as Deliberate Software Attacks, Espionage or Trespass, Intrusion attack or Hacking, Spoofing, Man-in-the-Middle, Eavesdropping, Denial-of-service attack, Malicious Software, etc.

As there exist no single solution to all of life’s problems, so there exist no single solution to all of these security threats. Though there have been some other solutions to mitigate some of these security threats, but in order to protect and secure information transmission over the insecure Internet, we are proposing an enhanced information security approach using cryptography and steganography.

Cryptography and steganography are the two popular methods available to provide information security. One hides the existence of the message and the other distorts the message itself. Using cryptography, the data is transformed into some other gibberish form and then the encrypted data is transmitted. In steganography, the data is embedded in another message before transmission, thus the existence of the main message is unknown. The combination of cryptography and steganography will enable us encrypt our information then hide it in another media before transmitting it over an insecure environment.

This study is aimed at developing enhanced information security software for securing information before transmitting them over the Internet or any other insecure environment.

The specific objectives used to achieve the aim are as follows:

1. To design the system structure for encryption and steganography using Unified Modeling Language (UML) diagram.
2. To develop enhanced information security software that is capable of encrypting information using a symmetric encryption technique and embedding the encrypted information in another media (or file) using steganography technique.

2. LITERATURE REVIEW

2.1 Overview of Cryptography

Cryptography is a vital element of any strategy to address message transmission security requirements. Cryptography is the transformation of readable and understandable data into a form which cannot be understood in order to secure data. cryptography refers exactly to the methodology of concealing the content of messages, the word cryptography comes from the Greek word "Kryptos", that means hidden, and "graphikos" which means writing. The information that we need to hide, is called plaintext , It's the original text, It could be in a form of characters, numerical data, executable programs, pictures, or any other kind of information, The data that will be transmitted is called cipher text, it's a term refers to the string of "meaningless" data, or unclear text that nobody must understand, except the recipients.. (Kumari S. 2017).

Cryptography uses two types of keys: symmetric and asymmetric for data encryption and decrytion. Data encryption is a random string of bits created explicitly for scrambling and unscrambling data. Cipher text results from plaintext by applying the encryption key. Decryption is the process of retrieving the plaintext back from the cipher text. Key: Encryption and decryption usually make use of a key, and the coding method is such that decryption can be performed only by knowing the proper key (Kumari S. 2017).

.

2.2 Cryptography Algorithms

There are several ways of classifying cryptographic algorithms. For purpose of this work, they will be categorized based on the number of keys that are employed for encryption and decryption, and further defined by their application and use. The three types of algorithms that falls into these categories are: Secret Key Cryptography (SKC): This uses a single key for both encryption and decryption; Public Key Cryptography (PKC): This uses one key for encryption and another for decryption; Hash Functions: It uses a mathematical transformation to irreversibly "encrypt" information.

2.3 Overview of Steganography

Steganography can be described as the art and science of covert communications which involves the process of hiding information inside other information. Unlike cryptography, steganography messages do not draw attention to themselves, as data is hidden in such a way as to make it undetectable to the human eye. The word steganography is derived from the Greek words “stegos” meaning “cover” and “grafia” meaning “writing”, defining it as “covered writing” (Mandy D. et al 2017). Secret information is encoded in a way such that the very existence of the information is concealed in a human perceptible.

The aim of steganography is to communicate securely in a completely undetectable manner (Chandramouli et al, 2001) and to avoid drawing suspicion to the transmission of a hidden data. Therefore, in existing communication methods, steganography can be used to carry out hidden exchanges. The idea of steganography is to keep people from thinking that the information even exists and not to keep them from knowing the hidden information. If a steganography method causes anybody to suspect there is secret information in a carrier medium, then the method has failed (Artz, 2001).

2.3.1 Typesof Steganography

There are basically three types of steganographic protocols used (Hamid et al., 2010a). They are:

Pure Steganography: Pure Steganography is defined as a steganographic system that does not require the exchange of a cipher such as a stego-key. This method of Steganography is the least secure means by which to communicate secretly because the sender and receiver can rely only upon the presumption that no other parties are aware of this secret message. Using open systems such as the Internet, we know this is not the case at all.

Secret Key Steganography: Secret Key Steganography is defined as a steganographic system that requires the exchange of a secret key (stego-key) prior to communication. Secret key Steganography takes a cover message and embeds the secret message inside of it by using a secret key (stego-key). Only the parties who know the secret key can reverse the process and read the secret message. Unlike Pure Steganography where a perceived invisible communication channel is present, Secret Key Steganography exchanges a stego-key, which makes it more susceptible to interception. The benefit to Secret Key Steganography is even if it is intercepted; only parties who know the secret key can extract the secret message.

Public Key Steganography: Public Key Steganography takes the concepts from Public Key Cryptography as explained below. Public Key Steganography is defined as a steganographic system that uses a public key and a private key to secure the communication between the parties wanting to communicate secretly. The sender will use the public key during the encoding process and only the private key, which has a direct mathematical relationship with the public key, can decipher the secret message. Public Key Steganography provides a more robust way of implementing a steganographic system because it can utilize a much more robust and researched technology in Public Key Cryptography. It also has multiple levels of security in that unwanted parties must first suspect the use of Steganography and then they would have to find a way to crack the algorithm used by the public key system before they could intercept the secret message.

2.3.2 Steganographic Mediums

Encoding Secret Messages in Text
Encoding Secret Messages in Images
Encoding Secret Messages in Audio
Encoding Secret Messages in Video
Encoding Secret Messages in Protocols

2.3.3 Characterization of Steganography Systems

Steganographic techniques hides message inside a cover. Various features characterize the strength and weaknesses of the methods. The relative importance of each feature depends on the application (Hamid et al, 2010b).

2.3.3.1 Capacity

The notion of capacity in data hiding indicates the total number of bits hidden and successfully recovered by the Stego system (Hamid et al, 2009).

2.3.3.2 Robustness

Robustness refers to the ability of the embedded data to remain intact if the stego-system undergoes transformation, such as linear and non-linear filtering; addition of random noise; and scaling, rotation, and loose compression (Mahmoud et al, 2010).

2.3.3.3 Undetectable

The embedded algorithm is undetectable if the image with the embedded message is consistent with a model of the source from which images are drawn. For example, if a Steganography method uses the noise component of digital images to embed a secret message, it should do so while not making statistical changes to the noise in the carrier. Undetectability is directly affected by the size of the secret message and the format of the content of the cover image (Hamid et al, 2009).

2.3.3.4 Invisibility (Perceptual Transparency)

This concept is based on the properties of the human visual system or the human audio system. The embedded information is imperceptible if an average human subject is unable to distinguish between carriers that do contain hidden information and those that do not. It is important that the embedding occurs without a significant degradation or loss of perceptual quality of the cover (Hamid et al, 2009), (Mahmoud et al, 2010).

2.3.3.5 Security

It is said that the embedded algorithm is secure if the embedded information is not subject to removal after being discovered by the attacker and it depends on the total information about the embedded algorithm and secret key.

2.4 Related Works

Steganography and cryptography are not something new; both of them have been around since before World War I. Over the years both steganography and cryptography have evolved and now they both are being used to ensure the secrecy and privacy of information. Some previous works that are related to the problem domain are discussed below.

Evaluation of Performance Characteristics of Cryptosystem using Text Files designed by (Challa and Jayaram, 2008). They considered the performance comparison for variable sized text files as input. An analysis on computational running times results in significant difference among the methods. They believe that the performance of DES, especially in decryption method is very high than the alternatives. Despite the key distribution, DES is more suitable to the application, which has the decryption as the highest priority. They proposed and performed the test cases on the two PKCS methods i.e., RSA and NTRU Though the encryption, decryption and complexity are high in NTRU, the RSA provides the highest security to the business application. He presented all these parameters with computational running times for all the methods, so as to select the appropriate method (Challa and Jayaram, 2008).

Ramesh and Umarani, (2012) in 2010 designed the UR5 algorithm: they proposed a block encryption algorithm. In this Algorithm, a series of transformations have been used depending on S-BOX, XOR Gate, and AND Gate. The algorithm encrypts a plaintext of size 64-bits by a key size of 64-bits. It goes through eight rounds for encryption or decryption process. It overcomes some drawbacks of the other algorithms.

Dasgupta et al, (2012), in their paper, proposed a hash based least significant bit (LSB) method. This is spatial domain technique that hides messages in the LSB of the cover media. Eight bits of the secret information is divided into 3,3,2 and embedded into the RGB pixel values of the cover frames respectively. A hash function is used to select the position of insertion in LSB bits. They evaluated the technique using both Peak Signal to Noise Ratio (PSNR) compared to the original cover video and the Mean Square Error (MSE) measured between the original and steganographic files averaged over all video frames. They also measured Image
Fidelity (IF) and observed minimal degradation of the steganographic video file. The proposed method when compared with existing LSB based steganography, yielded an encouraging. Result.

Agrawal and Mishra, (2012) did an analysis of the popular symmetric key encryption algorithms such as DES, TRIPLE DES, AES, and Blowfish. Their analysis shows that Symmetric Key algorithms run faster than Asymmetric Key algorithms such as RSA etc and the memory requirement of Symmetric algorithms is lesser than Asymmetric encryption algorithms. They also asserted that the security aspect of Symmetric key encryption is superior than Asymmetric key encryption.

Parisa et al, (2012) proposed a method that uses Particle Swarm Optimization (PSO) for finding the best pixel locations, after which the secret image is transformed to a new secret image. Optimal Pixel Adjustment (OPA) technique is applied to enhance the image quality. Results are then compared with those obtained by Simple LSB, Wang’s et al. method, Wu’s et al. method. The experimental results confirmed that Peak signal to noise ratio of the method is higher than mentioned methods hence an improvement in the image imperceptibility. Also the results illustrate that the proposed approach is robust against chi-square attack.

Abdel-Karim, (2010) presented simulation results showed that Blowfish has a better performance than other common encryption algorithms used. Since Blowfish has not any known security weak points so far, which makes it an excellent candidate to be considered as a standard encryption algorithm. AES showed poor performance results compared to other algorithms since it requires more processing power. Using CBC mode has added extra processing time, but overall it was relatively negligible especially for certain application that requires more secure encryption to a relatively large data blocks.

Mamoun, (2011) proposed a steganographic technique of embedding a digital color image into a color image. This requires the use of uncompressed 24-bit windows format bitmap image. The major characteristic of this algorithm is the ability of embedding a large digital image into a small digital image and vice versa. This method allows for embedding a text message into a cover image and produces a high degree of security and privacy. This method also includes a password in the stego image, so that no one can extract the secret image except for those who know the password. The limitation of this technique is that it solely based on steganography and does not involve encryption, hence does not give privacy if steganography fails.

Yi-zhen et al, (2010), an improved adaptive steganography algorithm—SVBA algorithm, which fully analyzes the statistical properties and adopts HVS features. SVBA algorithm first divides the image into 8*8 blocks and analyzes the mean, variance and entropy value of grey by block, then sets a sensitivity vector for each block with considering HVS features and adjusts the steganography schema dynamically according to the block sensitivity vectors. Simulation experiment results onMatlab7.0 shows this algorithm has a balanced performance on efficiency, capacity, imperceptibility and robustness.

(Asad et al, 2011), proposed an enhanced least significant bit for audio steganography. This paper proposes two ways to improve the conventional LSB modification technique. The first way is to randomize bit number of host message used for embedding secret message while the second way is to randomize sample number containing next secret message bit. The improvised proposed technique works against steganalysis and decreases the probability of secret message being extracted by an intruder.

Hamdaqa and Tahvildari, (2011) used VoIP (Voice over IP) for real time network steganography, which utilizes VoIP protocols and traffic as a covert channel to conceal secret messages. This paper modifies the (k, n) threshold secret sharing scheme, which is based on Lagrange’s Interpolation, and then applies a two phase approach on the LACK steganography mechanism to provide reliability and fault tolerance and to increase steganalysis complexity.

3. PROPOSED WORK

In this work, we are proposing an information security system that is capable of encrypting our information and then embed the cipher text in an image with the help of a stego key. The proposed technique consists of four parts; the first part deals with encrypting the secret message using DES algorithm, the second part embeds the encrypted data into cover-image using a stego key generated from a passhrase to get the stego-image, while the third part deals with extracting the encrypted data (cipher text) from the stego-image, and the fourth part decrypts the extracted cipher text to get the secret message. This technique combines the effect of cryptography and steganography methods to enhance the security of information. All these are to have enhanced information security software for the protection of information transmission over an insecure Internet environment against security threats.

Considering the various methodologies that exist, this study adopts the Object Oriented Model in its design and implementation phase of this study.

To achieve an enhanced information security system as required in our aim, we proposed an information security system that implements the combination of the Triple Data Encryption Standard (3DES) (Option 3) Cryptography and the F5 Discrete Cosine Transform (DCT) Steganography. The 3DES Cryptography is a block cipher cryptography that uses 168 bit key size (3 time DES key size), hence its more secure and difficult to crack compare to the DES Cryptography that uses 56 bit key size. The F5 DCT Steganography is a Transform Domain Steganography with high capacity, robustness and security compared to the LSB Spatial Domain Steganography. This method encrypts the plain text first, before embedding it in an innocuous image file.

3.1 Algorithm of the Proposed System

The two major segments of the algorithm are the sender's segment and the receiver's segment. The sender encrypts and then embeds the encrypted while the receiver extract and then decrypt the extracted file as illustrated in the following algorithm:

Sender side:

A. Encryption Algorithm:

```
Step 1: Read Plain text file and 3 different passphrases
Step 2: Search if Input file exist
        If found proceed to step 3
        Else return to step 1
Step 3: Generate 3DES key from passphrases
Step 4: Perform 3DES encryption of the Plain text file.
Step 5: Write the encrypted file.
```

B. Embedding Algorithm:

```
Step 1: Read Cover Image, Encrypted file and Passphrase
Step 2: Search if cover image file and encrypted file exist
        If found proceed to step 3
        Else return to step 1.
Step 3: Perform F5 DCT Steganography embedding
Step 4: Write out Stego-image
```

Receiver side:

A. Extraction Algorithm:

```
Step 1: Read stego-image and passphrase.
Step 2: Search if Stego-image file exist
        If found perform F5 IDCT Steganography extraction algorithm and proceed to step 3
        Else return to step 1
Step 3: Write Extracted Encrypted file.
```

B. Decryption Algorithm:

```
Step 1: Read Extracted Encrypted file and 3 different Passphrases
Step 2: Search if inputted file exist
        If found proceed to step 3
        Else return to step 1.
Step 3: Generate 3DES key from passphrases
Step 4: Perform 3DES Decryption on the file using the key
Step 5: Write the Plain text file.
```

3.1.2. Triple DES Algorithm

It's segmented into Encryption and Decryption segments illustrated as follows:
Encryption Algorithm
Step 1: Perform DES encryption on plain text using key 1 to generate cipher text 1
Step 2: Perform DES encryption on cipher text 1 using key 2 to generate cipher text 2
Step 3: Perform DES encryption on cipher text 2 using key 3 to generate cipher text 3
Decryption Algorithm
Step 1: Perform DES Decryption on cipher-text with key 3 to generate ciphertext 3
Step 2: Perform DES Decryption on cipher-text 3 with key 2 to generate cipher-text 2
Step 3: Perform DES Decryption on cipher-text 2 with key 1 to generate the plaintext file.

3.1.3. F5 DCT Steganography Algorithm

This algorithm entails the Embedding algorithm and the Extraction algorithm.
Embedding Algorithm:
Step1: Start JPEG compression. Stop after the quantisation of coefficients.
Step 2: Initialise a cryptographically strong random number generator with the key derived from the passphrase.
Step 3: Instantiate a permutation (two parameters: random generator and number of coefficients).
Step 4: Determine the parameter k from the capacity of the carrier medium, and the length of the secret message.
Step 5: Calculate the code word length $n = 2k - 1$.
Step 6: Embed the secret message with (1, n, k) matrix encoding.
(a) Fill a buffer with n nonzero coefficients.
(b) Hash this buffer (generate a hash value with k bit-places).
(c) Add the next k bits of the message to the hash value (bit by bit, xor).
(d) If the sum is 0, the buffer is left unchanged. Otherwise the sum is the buffer's index 1 . . .n, the absolute value of its element has to be decremented.
(e) Test for shrinkage, i. e. whether we produced a zero. If so, adjust the buffer (eliminate the 0 by reading one more nonzero coefficient, i. e. repeat step 6a beginning from the same coefficient).

If no shrinkage occurred, advance to new coefficients behind the actual buffer.

If there is still message data continue with step 6a.

Step 7: Continue JPEG compression (Huffman coding etc.)
Extraction Algorithm:
Step1: We have the Stego Image S, we need to extract two things out of the Stego Image i.e. the Secret message and the Cover Image.
Step2: Perform Jpeg lossless compression on the stego Image using the Huffman algorithm.
Step 3: Apply the Inverse DCT using the formula:

$$f(x) = \sum_{u=0}^{N-1} a(u)C(u)cos\left[\frac{\pi(2x+1)u}{2N}\right]$$

For u,v = 0,1,2,…,N-1 and a(u) and a(v). The inverse transform is defined as

$$f(x,y) = \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} a\ u\ a\ v\ C\ u,v\ cos\left[\frac{\pi\ 2x+1\ u}{2N}\right] cos\left[\frac{\pi\ 2y+1\ v}{2N}\right]$$

Step 4: After this, we can extract the secret message and have two things i.e. the secret message as well as the cover (Raman Chadha et al, 2014).

3.2 Architecture of the Proposed System

Illustration of the Architectural diagram of the proposed system is depicted in figure 3.1

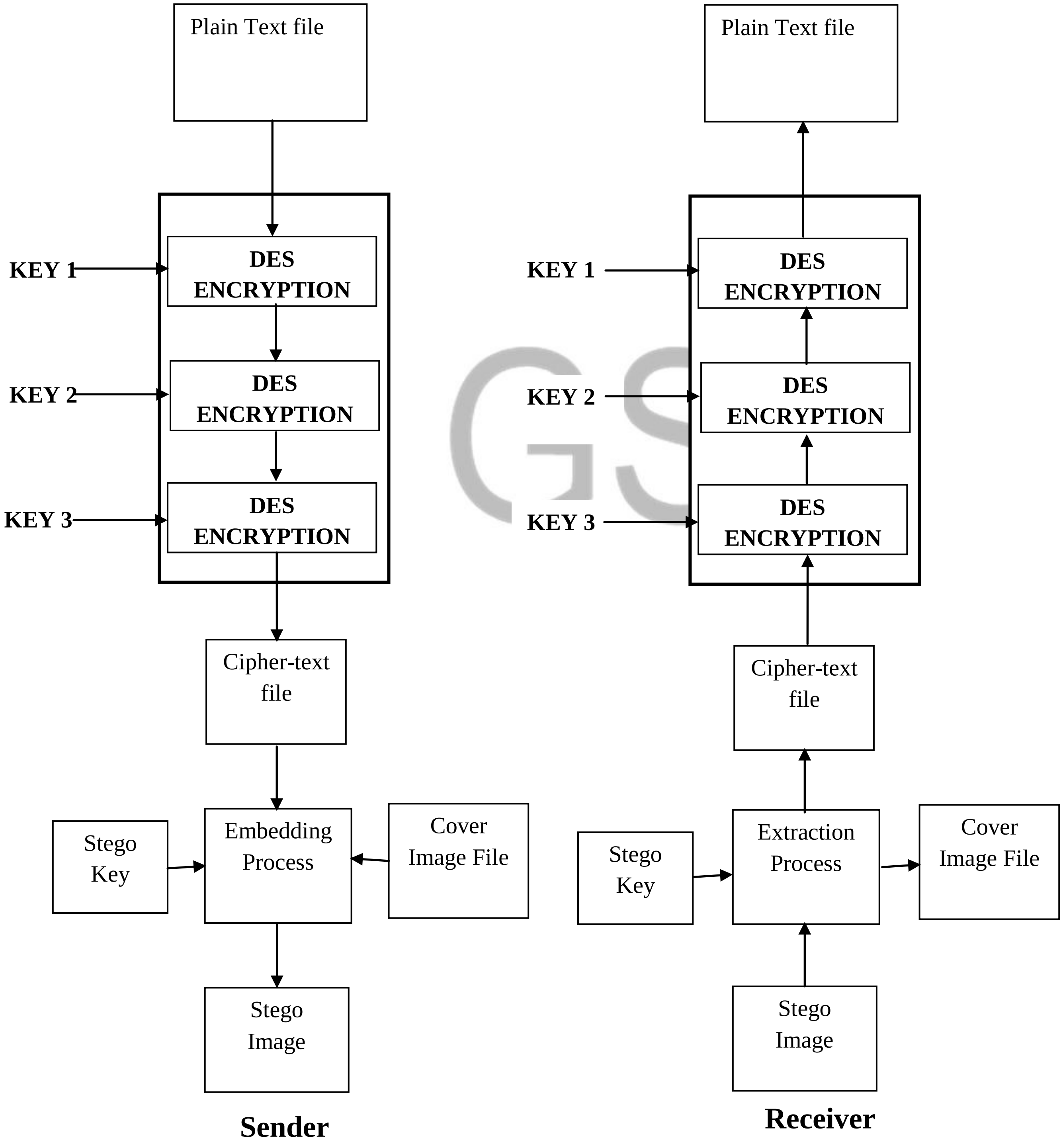


Figure 3.1: Architectural Diagram of the Proposed System

3.3. Advantages of the Proposed System

1. To enhance the performance of DES, Triple DES was introduced in 1998 which has a key size of 64 bits. Triple DES encrypts the data by using three different keys. Each triple encryption algorithm encrypts one block of 64 bits of data by different three 56-bit keys, which enhance size of key to 168 bits thereby increasing the security levels.

2. DES was superseded by triple DES (3DES) in November 1998, concentrating on the noticeable imperfections in DES without changing the original structure of DES algorithm.

3. 3DES is still approved for use by US governmental systems.

4. F5 DCT steganography has high payload capacity.

5. F5 DCT steganography is a robust steganography system

6. This method results in a high image quality of stego image hence its imperceptibility quality is high.

4. IMPLEMENTATION, EVALUATION, AND RESULTS DISCUSSION

4.1. Implementation and Evaluations

The proposed system was implemented using java an Object Oriented Programming Language.

4.1.1 Experiments and Evaluations

In order to validate the implemented system against the aim of this study, which is to develop an enhanced information security software for securing information before transmitting them over the Internet or any other insecure channel such that its confidentiality and integrity is maintained and the information is protected against security threats, we carried out some experiment with the implemented system and evaluate its security, and imperceptibility; which are generally acceptable criteria in evaluating steganography systems (Amin et al, 2013).

The proposed system was experimented to prove its efficiency as discussed in the following section.

Sender Encrypt and Embed

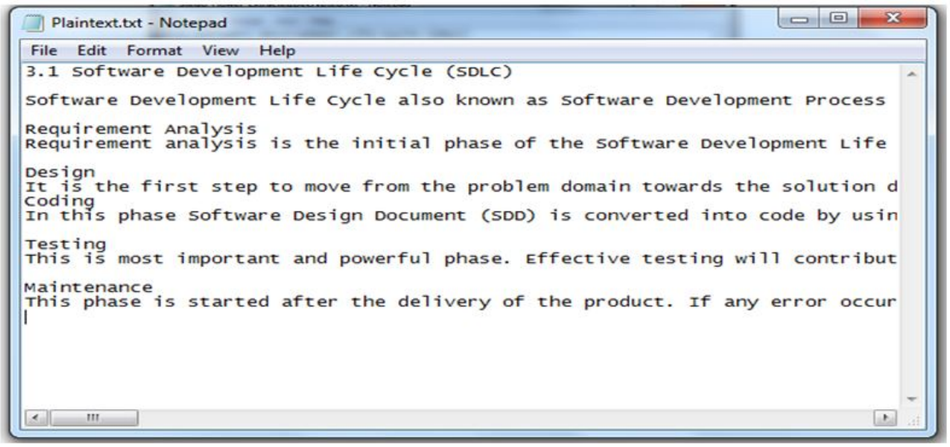
From the sender's angle, a plain-text file (depicted in figure 4.1) was first encrypted to generate the encrypted file (depicted in figure 4.2) using the Triple Data Encryption Standard (3DES) substitution cipher method. Three different passphrases where supplied which was used in generating a 168 bit size 3DES key used in the encryption; which is based on symmetric cryptosystem, where same key is used for both encryption and decryption process.

Thereafter the encrypted-text was embedded inside the JPEG Cover image file (shown in figure 4.3a) using a supplied passphrase (used in generating a secure key) and the Discrete Cosine Transform (DCT) technique (a Transform Domain Steganography method) that embeds the information in the frequency domain to generate the stego-image (shown in figure 4.3b). The generated stego-image can then be sent over an insecure internet channel or environment to the receiver. The whole idea of the proposed method is to develop software that enables secure data communication between sender and receiver over an insecure environment in other to protect the message against security threats. By this approach the message was successfully embedded into the cover image. In the experiment messages of different file sizes were successfully embedded into different set of images.

Receiver Extract and Decrypt

At the receiver's end, in other to retrieve the plain-text message, the cipher-text was first extracted from the stego-image by supplying same passphrase (to generate same secure key) that was used in embedding it. The encrypted-text was then decrypted by also supplying same three passphrases (for generating same 3DES keys) used for encryption to get back the original plain-text message (shown in figure 4.4). If the key does not match in any of the cases (i.e the passphrase for extracting differs from that of embedding or the passphrases for decrypting differs from that used in encryption) you will not be able to extract the cipher-text from the stego-image nor decrypt the extracted cipher-text respectively.

The messages that were embedded into the images were extracted successfully.



```
3.1 Software Development Life Cycle (SDLC)

Software Development Life Cycle also known as Software Development Process

Requirement Analysis
Requirement analysis is the initial phase of the Software Development Life

Design
It is the first step to move from the problem domain towards the solution d
Coding
In this phase Software Design Document (SDD) is converted into code by usin

Testing
This is most important and powerful phase. Effective testing will contribut

Maintenance
This phase is started after the delivery of the product. If any error occur
```

Figure 4.1: Plain text file

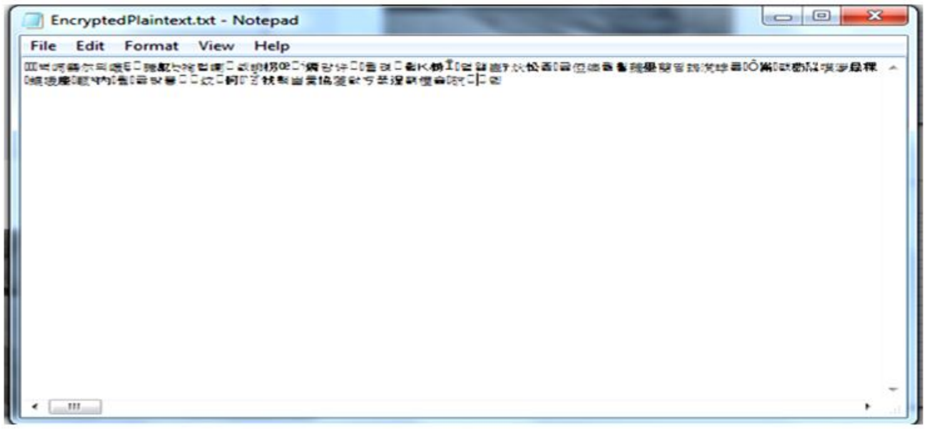


Figure 4.2: Encrypted File

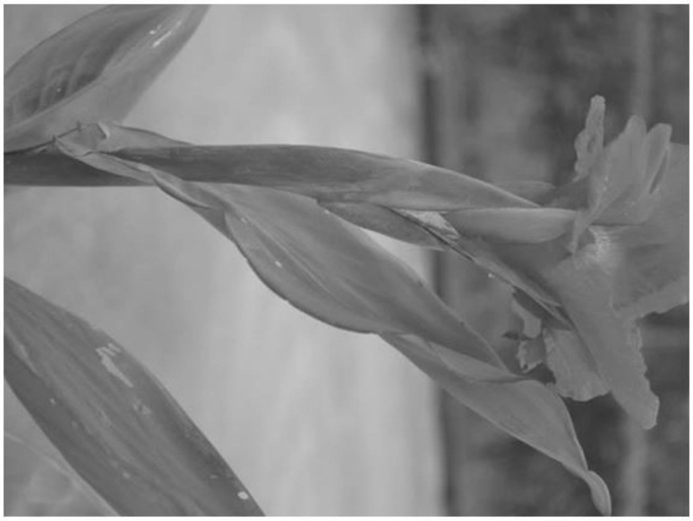


Figure 4.3a: Cover Image (a)

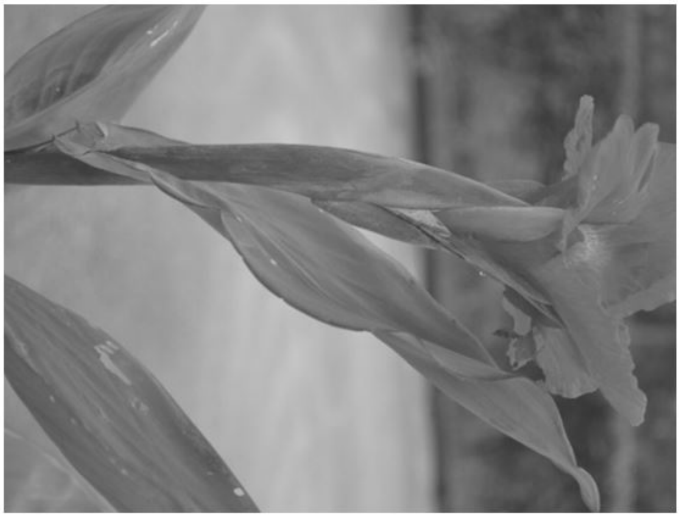
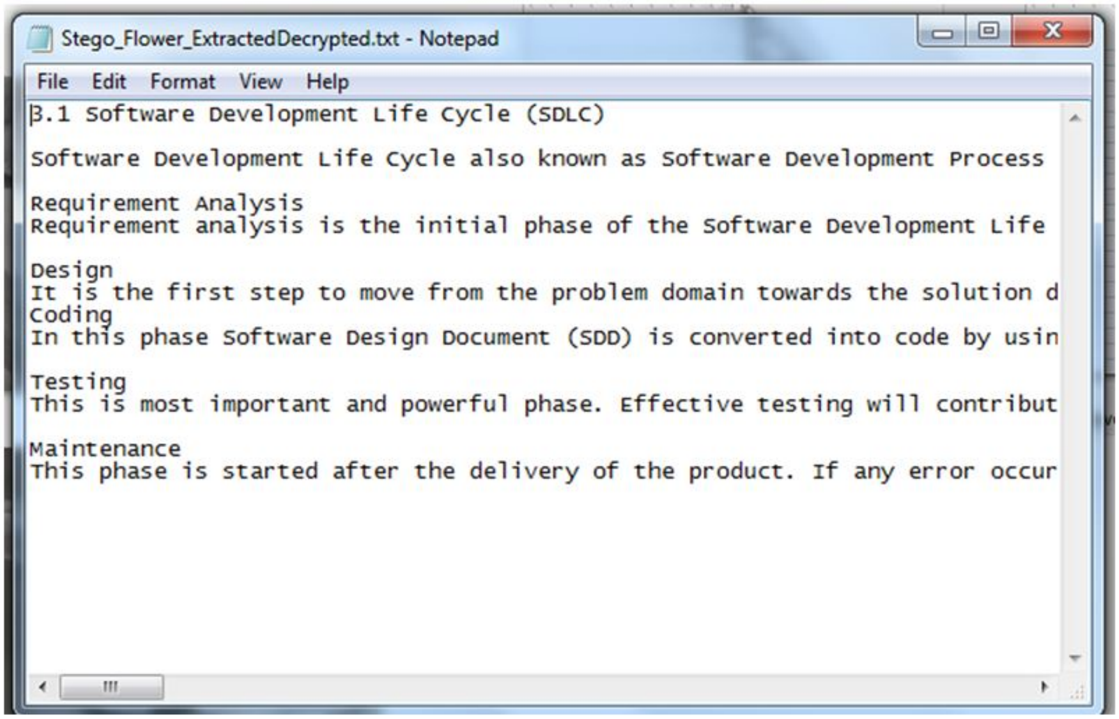


Figure 4.3b: Stego Image (a)



Stego_Flower_ExtractedDecrypted.txt - Notepad
File Edit Format View Help

```
3.1 Software Development Life Cycle (SDLC)

Software Development Life Cycle also known as Software Development Process

Requirement Analysis
Requirement analysis is the initial phase of the Software Development Life

Design
It is the first step to move from the problem domain towards the solution d
Coding
In this phase Software Design Document (SDD) is converted into code by usin

Testing
This is most important and powerful phase. Effective testing will contribut

Maintenance
This phase is started after the delivery of the product. If any error occur
```

Figure 4.4 Decrypted File (a)

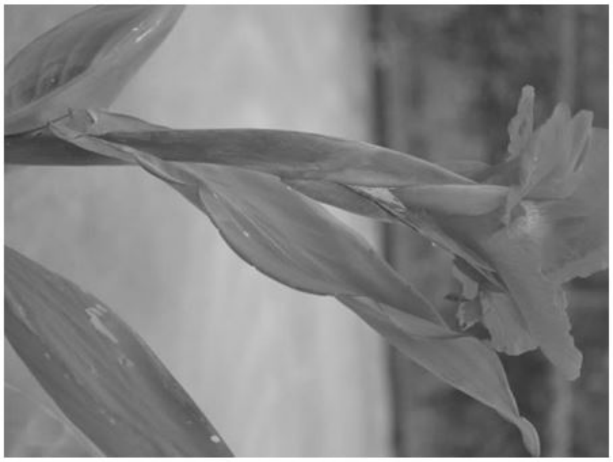


Figure 4.5a: StegoImage (a1)

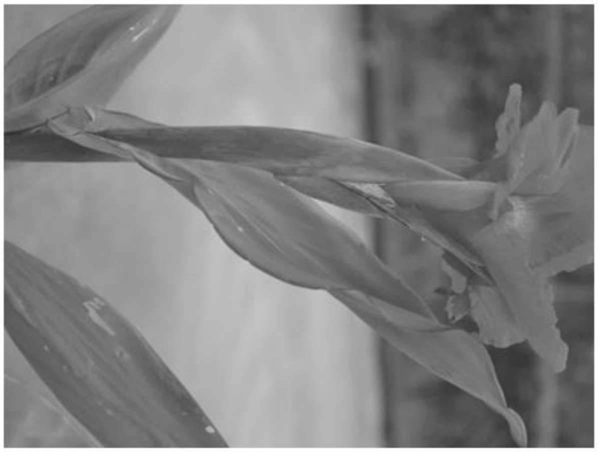


Figure 4.5b: StegoImage (a2)

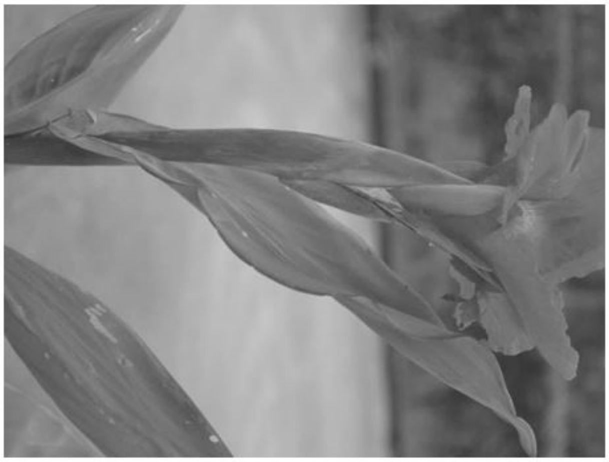


Figure 4.5c: StegoImage (a3)

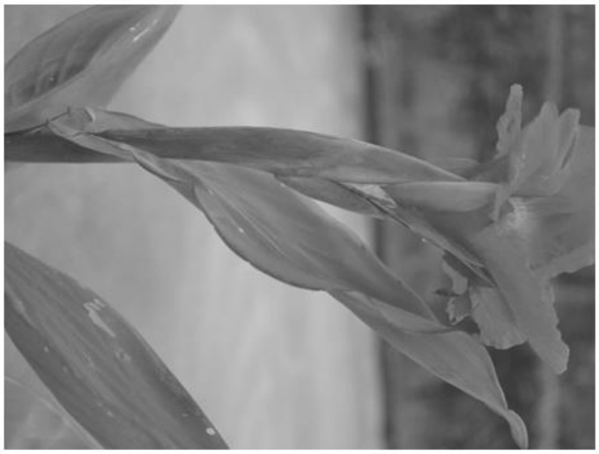
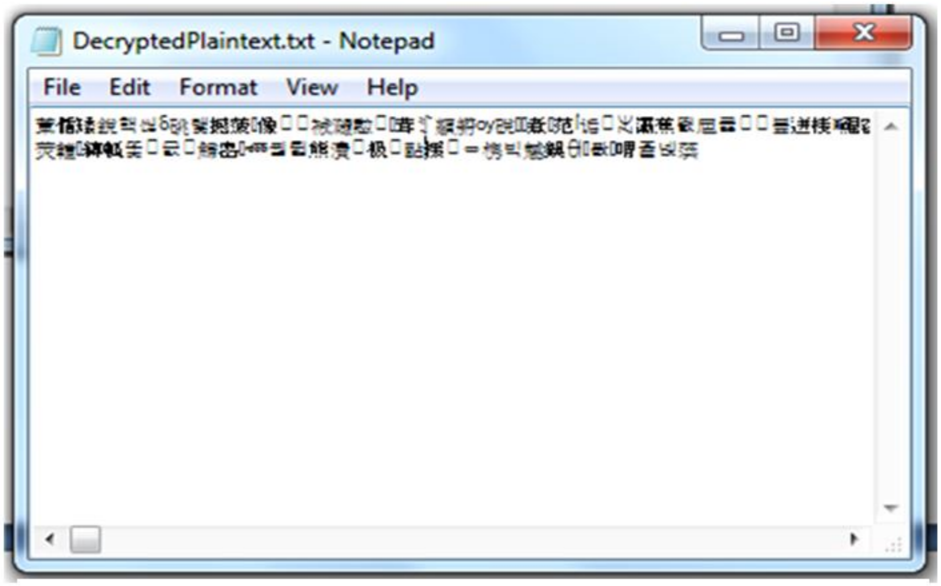


Figure 4.5d: CoverImage (a4)



[illegible]
[illegible]

Figure 4.6: Wrong Passphrase Decrypted File

4.1.2 System Performance and Efficiency Evaluation

To further evaluate the system based on security, and imperceptibility as earlier stated to validate our aim, the following activities of experimentation and evaluation were performed.

4.1.3 Imperceptibility (Invisibility) Evaluation

The aim of steganography is to conceal the very existence of hidden communication, so imperceptibility is the primary demand. The secret message should be truly undetectable, so that the host file cannot be distinguished from the Stego file.

After embedding, distortion normally occurs which in turns affects the Stego file. It is difficult to quantify how imperceptible embedded data is. In the case of image steganography, there are two methods to measure imperceptibility of steganography:

- **Subjective Evaluation**: in designed experiments, some observers are chosen to rate the images by specified rules. Here the imperceptibility of the embedded data is indicated by illustrating the original image and its counterpart (the stego image) with embedded data so that their visual differences, if any, can be determined. This is known as the Human Visual System (HVS). HVS-Based Imperceptibility Evaluation maps the absolute errors between cover images and stego images into JNDs(Just noticeable differences) that can be perceived by human vision. When errors are higher than sensitive threshold, they can be perceived, else be ignored.

In carrying out the subjective evaluation of our system, we performed the experiment again by encrypting three different plain text file with different file sizes to generate three encrypted files which were embedded using the same cover image file (shown in figure 4.5d) separately for the three encrypted files to generate three different stego image files depicted in figure 4.5a, b, c.

After the experiment, the stego images were subjected to the HVS of different people, by visually observing the files alongside the cover image to notice whether there were any differences between them, or any distortion in the stego images.

- **Objective Evaluation**: here algorithms are used to evaluate the image degrades or measure the imperceptibility by measuring the difference between the host file and Stego file. Examples of such algorithms or metrics are Mean Square Error (MSE), PSNR. The Mean Squared Error (MSE) is the averaged term-by-term squared difference between the input signal (the original image, P) and the output signal (the secret message, P'), as shown in the following equation (Zeki et al, 2012).

$$MSE = \frac{1}{N}\sum^{N}(P_i' - p_i)^2)$$

The PSNR is given in below Equation in which P_{peak} is the peak value of the input signal.
Usually 255 for 8 bit Gray scale images.

$$PSNR(db) = 10\log_{10}\frac{p_{peak}^2}{MSE}$$

The larger the PSNR, the better the image quality will be.

It has been observed that when the payload increases, the MSE increases, and this affects the PSNR inversely (Stefan et al, 2012). So, from trade-off it was found that MSE decrease causes PSNR increase and vice-versa. PSNR is often expressed on a logarithmic scale in decibels (dB). PSNR values falling below 30 dB indicate a fairly low quality, i.e. distortion caused by embedding can be obvious. However, a high quality stego-image should strive for 40 dB and above (Piva et al, 1997).

The work did not only (stop at or) consider preserving the visual integrity of the image used for embedding but also ensure the method should be free from statistical attacks by limiting distortion or quality difference between the original cover image and the stego images. The invisibility of the hidden message also denoted by the distortion between the two images was measured by considering Mean Square Error (MSE), and PSNR (peak signal to noise ratio). The result of the evaluation is depicted in table 4.1.

Table 4.1: Imperceptibility Performance Evaluation Result

Cover Image	Stego Image	No of bytes embedded	MSE	PSNR	No of bytes extracted
CoverImage(a) 640x480 162KB	StegoImage(a1) 640X480 22.5KB	2.07KB	4.0	42.11	2.07KB
CoverImage(a) 640x480 162KB	StegoImage(a2) 640X480 25.0KB	537B	3.0	43.36	537B
CoverImage(a) 640x480 162KB	StegoImage(a3) 640X480 22.7KB	1.90KB	3.0	43.36	1.90KB

4.1.4. Security Evaluation

In order to enhance the security in this system a multi-level security mechanism or approach that covers encrypting, embedding, extracting and decryption was applied as discussed in the following sections.

4.1.4.1. Encryption and Decryption Security

Generally, when deploying ciphers, users have to decide on the size of the crypto variable or key. This is very important, because the strength of many encryption applications and cryptosystems is measured by key size. This system implemented symmetric Triple DES Key, third option. Triple DES uses a 128 bit size key which makes the encryption more secure and more difficult to be broken compared to the normal DES that uses a 56 bit key size. It is 3 times more secure and stronger than DES. It uses three different keys to encrypt the plain text in three phases. The first phase uses the first key to encrypt the plain text. The output from the first phase is encrypted in the second phase with the second key. The encryption is further strengthened in the third phase by encrypting the cipher-text generated from the second phase with the third key.

In testing the security feature or quality of the system, we inputted different passphrases other than the passphrases used in encrypting the plain text file in figure 4.1, and the resulted output file is shown in figure 4.6.

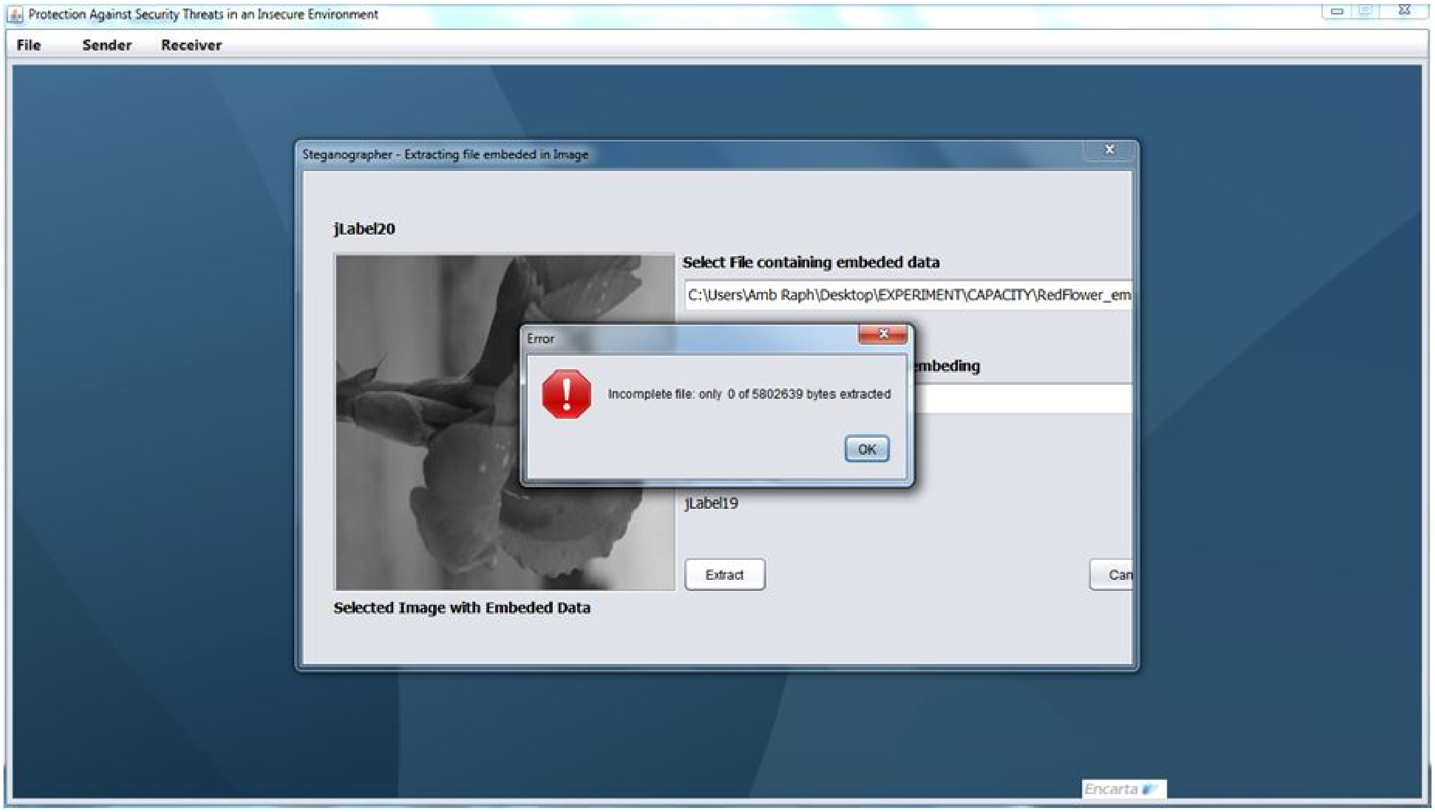
4.1.4.2. Embedding and Extraction Security

An embedding algorithm is said to be secure if the embedded information is not subject to removal after being discovered by the attacker. This highly depends on the total information about the embedding algorithm and the secret key.

For the enhanced security of the steganography segment, a private key mechanism was also implemented. Here after the plain text is encrypted, the encrypted file and passphrase is inputted for embedding. The system uses the passphrase to generate a stego key which is used in embedding the encrypted file in the cover image to generate the stego image. Note that this same passphrase is required by the receiver to be able to extract the encrypted message. Hence, even if an attacker is able to identify the existence of the message in the image, he is unable to extract the message without the passphrase. This further validates our goal of an enhanced information security system.

To validate the above, we attempted extracting the embedded message in the stego image file seen in figure 4.7 with a different passphrase other than that used in embedding it. The outcome of this action is depicted in figure 4.8.

Figure 4.7: StegoImage


Protection Against Security Threats in an Insecure Environment
File
Sender
Receiver
Steganographer - Extracting file embeded in Image
jLabel20
Select File containing embeded data
mbeding
Error
OK
jLabel19
Extract
Can
Selected Image with Embeded Data
Encarta

C:\Users\Amb Raph\Desktop\EXPERIMENT\CAPACITY\RedFlower_em

Incomplete file: only 0 of 5802639 bytes extracted

Figure 4.8: GUI error message on attempt to extract with wrong passphrase.

4.2. Discussion of Results

The following section discusses the results from our evaluation of the implemented system.

4.2.1. Imperceptibility (Invisibility) Evaluation Result's Discussion

We shall discuss the results of the system Imperceptibility (Invisibility) Evaluation in two segments based on how it was evaluated.

Subjective Evaluation Result Discussion

From the result obtained when we carried out subjective evaluation on the stego images and the cover image, It was observed that the Human Visual System (HVS) cannot distinguish the cover-image and stego images the complexity of the image is not disturbed as shown in figure 4.5(a) and (b), (c) and (d).

Objective Evaluation Result Discussion

After the Objective Evaluation of the cover image and stego images as shown in table 4.1, it was observed that when the payload increases, the MSE increases, and this affects the PSNR inversely. So, from trade-off it was found that MSE decrease causes PSNR increase and vice-versa. Our results indicate that embedding process introduces less perceptual distortion and higher PSNR. It is to be noted that PSNR ranging from 42dB to 43dB as shown in our result implies that the quality degradations could hardly be perceived by a human eye.

From the above discussions, it is proven that information can be hidden in an (unsuspected) image with this system and transmitted from the sender to the receiver without an attacker noticing the existence of such information in the image. By this we achieve the goal of information confidentiality which is a required feature of an enhanced security in information security system as proposed.

4.2.2. Security Evaluation Result's Discussion

With the results obtained (shown in figure 4.7 and 4.8) from the security evaluation of the implemented system, it was observed firstly from the steganography security evaluation that for one to be able to extract the encrypted message from the stego image, the same passphrase (that generates the stego key) used in embedding the message into the cover image is required. If the keys do not match (i.e the passphrase for extracting differs from that of embedding) an attacker or any other person will be unable to extract the message from the image even if he was able to notice its existence. Secondly, from the cryptography security evaluation, we found out that also the three different passphrases (that generates the 3DES key) used in encrypting the plaintext file is required at the point of decryption. If the encryption and decryption keys do not match (i.e the passphrases for decrypting differs from that used in encryption) the plaintext will not be decrypted from the cipher text, we'll end up having an unreadable file which will make no sense to the attacker.

The above discussion proves the enhanced security feature of our information security system as proposed. By this we are able to preserve the integrity of information as it is transmitted over an insecure channel which is also another required feature of an information security system.

5. SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.1. Summary

The rapid development in the field of Information and Communication Technology has made the accessibility and availability of the Internet easy and common in our society today; hence it's usage in transmitting vital and confidential information by individuals and well as corporate Organisations, Government, Military, etc a modus in our society. This calls for an enhanced information security mechanism to protect our information against security threats and attacks such as hacking, etc that the Internet exposes the information to. Though several studies have revealed the usage of either Cryptography or Steganography, to achieve the goal of an enhanced information security system, we proposed "Protection against Security Threats in an Insecure Environment using DES Cryptography and Steganography". We first applied the more secure Triple DES Cryptography Algorithm on plain text file to make it unreadable after which we applied a robust and highly secured F5 Discrete Cosine Transform (DCT) Steganography to hide the encrypted data in an innocuous image file. The proposed method adopts the Object Oriented Software Methodology in its Design and Implementation Phase. The system was implemented using java jdk-8u11-windows-x64 and NetBeans IDE8.0 for windows.

5.2. Conclusion

With the results obtained and our evaluations of the implementation of this system (discussed in the previous sections) it is clear that this system can be used to protect the confidentiality and integrity of vital information transmission which is a required characteristic of any information security system and also accomplished our aim of developing an enhanced information security system for securing information before transmitting them over the Internet or any other insecure environment.

5.3. Recommendations

Having successfully achieved the aim of this study, considering our findings from the introductory section of this work, through the literatures reviewed down to the implementation and evaluation of results of the proposed system we hereby recommend the usage of combined cryptography and steganography information security system for Organisations, Government agencies, Military and well as individuals for the enhanced security of their vital and confidential information before transmitting them over the insecure internet environment.

In using this system, though any type of image file can be used as a cover image, we recommend the usage of uncompressed image file types (e.g .bmp image type) in order to obtain a highly imperceptible JPEG stego image, since the system has to compress the cover image in the process of embedding, to generate a compressed stego image.

In addition, future work on this study is to consider improvement on the cryptography segment. Though the Triple DES algorithm implemented is a highly more secure algorithm compare to the DES cryptography, it is three times slower than the DES cryptography (this is not easily noticed in our system due to the specification of the computer system used in its implementation), an improvement in this cryptography segment will further enhance the efficiency of the system.

Finally future research work can also consider improvement on encrypting and embedding other file type (e.g .doc, .pdf, etc) other than the plain text file used in preparing our secret message in this study.

REFERENCES

Abdel-Karim, A. T. (2010). Performance Analysis of Data Encryption. Retrieved September 10, 2014, from http://www.cse.wustl.edu/~jain/cse567-06/encryption_perf.htm

Agrawal, M., and Mishra, P. (May, 2012). A Comparative Survey on Symmetric Key Encryption Techniques. International Journal on Computer Science and Engineering (IJCSE), , Vol. 4, No. 05, pp. 877-882.

Amin, M., Abdullkader, H. M., Ibrahem, H. M., and Sakr, A. S. (2013). A Steganographic Method Based on DCT and New Quantization Technique. International Journal of Network Security , pp. 187-191

Artz, D. (2001, May/June). Digital steganography: hiding data within data. Internet Computing, IEEE , pp. 75-80.

Asad, M., Rawalpindi, P., Gilani, J., and Khalid, A. (2011). An Enhanced Least Significant Bit Modification Technique for Audio Steganography. Computer Networks and Information Technology (ICCNIT), 2011 International Conference (pp. 143 - 147). Abbottabad: IEEE.

Cachin, C. (2004). An Information-Theoretic Model for Steganography. Information and Computation , pp. 41-56.

Challa, N., and Jayaram, P. (2008). Evaluation of Performance Characteristics of Cryptosystem Using Text Files. Journal of Theoretical and Applied Information Technology , pp. 55-59.

Chandramouli, M. N. (2001). Analysis of LSB Based Image Steganography Techniques. Proceedings 2001 International Conference on Image Processing. (pp. 1019 - 1022). Thessaloniki: IEEE.

Dasgupta, K., Mandal, J. K., and Dutta, P. (2012). Hash Based Least Significant Bit Technique for Video Steganography (HLSB). International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, No 2.

Hamdaqa, M., and Tahvildari, L. (2011). ReLACK: A Reliable VoIP Steganography Approach. Fifth International Conference on Secure Software Integration and Reliability on Improvement (pp. 189-197). Jeju Island, Korea: IEEE.

Hamid, J. A., Zaidan, A. A., and Zaidan, B. B. (2010a). A New System for Hiding Data Within (Unused Area + Image Page) of Portable Executable File using Statistical Technique and Advance Encryption. International Journal of Computer Theory and Engineering Vol 2 No 2, pp. 1793-8201.

Hamid, J. A., Zaidan, A. A., and Zaidan, B. B. (2009). Frame Seleceted Approach for Hiding Data within MPEG Video using Bit Plane Complexity Segmentation. Journal of Computing Vol 1 No 1 , pp.108-113.

Hamid, J. A., Zaidan, A. A., and Zaidan, B. B. (2010b). New Design for Information Hiding with in Steganography Using Distortion Techniques. International Journal of Engineering and Technology Vol 2 No 1 , pp. 1793-8236.

Kumari S. (2017). A research paper on cryptography encryption and compression techniques, International Journal Of Engineering And Computer Science Volume 6 Issue 4 April 2017, pp. 20915-20919

Mahmoud, E., Zaidan, A. A., Zaidan, B. B., Mohamed, E., Sharif, M. and Hamdan, O. A. (February 2010). Optimization Digital Image Watermarking Technique for Patent Protection. Journal of Computing (JOC), Vol.2, Issue 2, pp. 142-148.

Mamoun, A. R. (2011). Colored Image in Image Hiding. Ubiquitous Computing and Communication Journal (UBICC) , pp. 2-5.

Mandy D., Karen B., Mark L., Kevin C., (2017). An overview of steganography techniques applied to the protection of biometric data, Multimed Tools Appl (2018) 77:17333–17373

Parisa, G., Subariah, I., and Morteza, B. (October, 2012). Least Significant Bit Image Steganography using Particle Swarm Optimization and Optical Pixel Adjustment. International Journal of Computer Applications , Vol. 55, No.2, pp. 0975 – 8887.

Piva, A., Barni, M., Bartolini, F., and Cappellini, V. (October, 1997). DCT-based Watermark Recovering without Resorting to the Uncorrupted Original Image. Proceedings of IEEE Inter. Conference on Image Processing, Vol. 1, pp. 520 - 523. Santa Barbara.

Raman, Chadha and Bhavneet, Kaur. (May, 2014) Secure and Secret Transmission of Messages Using the DCT Technique of Steganography. International Journal of Core Engineering & Management(IJCEM), Volume 1, Issue 2, pp. 41-46

Ramesh, G., and Umarani, R. (2012). UR5: A Novel Symmetrical Encryption Algorithm with Fast Flexible and High Security Based on Key Updation. European Journal of Scientific Research , Vol.77, No.2, pp. 275-292.

Stallings, W. (2006). Cryptography and Network Security Principles and Practise. New york: Pearson Education, Inc. pp.62-64

Stefan, W., Elisa, D., and Gelasca, T. (April, 2002). Perceptual Quality Assessment for Video Watermarking. Proceedings of International Conference on Information Technology: Coding and Computing (ITCC). Las Vegas, pp.90-94.

Suryakant, T., and Madhav, B. (2012). A Dymanic Method to Secure Confidential Data using Signcryption with Steganography. International Journal of Engineering and Advanced Technology, 2 (2), pp. 183-191.

Venigalla, S. P., Nagesh, B. M., Srinivas, B., and Santhi, S. G. (March, 2012). Implementation of the Triple-DES Block Cipher. International Journal of Advances in Engineering and Technology , Vol. 3, Issue 1, pp. 117-128.

Whitman, M. E., and Mattord, H. J. (2005). Principles of Information Security, (4th Edition). Boston: Cengage Learning. pp. 349-350

Yi-zhen, C., Zhi, H., Shu-ping, L., Chun-hui, L., and Xiao-Hui, Y. (2010). An adaptive steganography algorithm based on block sensitivity vectors using HVS features. Image and Signal Processing (CISP), 2010 3rd International Congress on Vol.3 (pp. 1151 - 1155). Yantai: IEEE

Zeki, A. M., Ibrahim, A. A., and Manaf, A. A. (2012). Steganographic Software: Analysis and Implementation. International Journal of Computers and Communications , Issue 1, Vol. 6, pp. 35-42