Republic of Iraq
Ministry of Higher Education and
Scientific Research
University of Diyala
College of Education For Pure Science
Department of Computer

Encrypt Secret Document and hide it in image by Using Steganography

Prepared by

Abdula Hussein Swafy

Supervised By

L.Basim Najm Aldeen

2019 A.D. 1440 A.H.

Chapter one

1.1 *Introduction*

Two techniques are available to those wishing to transmit secrets using unprotected communications media . One is ***cryptography****, where the sender uses an encryption key to scramble the message, this scrambled message is transmitted through the insecure public channel, and the reconstruction of the original unencrypted message is possible only if the receiver has the appropriate decryption key. The second method is* ***steganography****, where the secret message is embedded in another*

message; using this technology even the fact that a secret is being transmitted has to be secret .While cryptography is about concealing the content of messages, steganography is about concealing their existence

Cryptography *is used when someone wants to hide*

information from being read as plain text. If a piece of text looks suspicious, it is easy to suspect that someone wants to hide something from the reader. When having an encrypted message, different kinds of decrypting methods can be applied, e.g., dictionary attacks or more time-consuming brute force methods. With steganography, the opportunity to suspect that there is something hidden, is not given. This means that the level of security has increased by at least one step with a hiding layer .

1.2 Encryption

Cryptography is a way of secure transmission and storage of data such that only the party for whom it is intended can read and others cannot. Cryptanalysis is the art of breaking codes, cipher text and cryptosystems without knowing the key or algorithm. Cryptology includes the study of both cryptography and cryptanalysis. Encryption is the process of converting plaintext to cipher text with the help of suitable schemes, algorithms and key. Thus the message encrypted can only be decrypted by the intended recipient with the help of corresponding decryption algorithms and key.
kryptos which means hidden. Since the earliest of times, humans have been interested in keeping certain sensitive information that they possess out of the reach of others for
Different people have made use of cryptography for different reasons. The Assyrians wanted to protect their trade secret of manufacturing pottery. The Chinese wanted to protect their trade secret of manufacturing silk. The Germans wanted to protect their military secrets. With the advancement of computers and internet, various firms, businesses, industries,
etc. had to protect their official data from intruders. In this paper, we will see how various encryption methods have been developed from earlier times to the present day.

***Encryption** or **Ciphering** is called in English.*
*, where the first word is taken from **Cryptography** and the second is taken from the word **Cipher**, which is said to refer to the Arabic word "reset" or to make the value equal to "zero" meaningless.*

From the beginning of this science until the moment of the modern era, there has been a marked development. The methods and methods of encryption differed significantly from those of previous centuries. So we can classify encryption into two or two main types :

1.Classical Encryption
2. Modern Encryption.

1.2.1 Historical Review to Encryption

The ancient form of cryptography mainly includes the classical methods. The most famous ones are the transposition ciphers and the substitution ciphers. The transposition ciphers work by rearranging the alphabets or changing the order of the alphabets appearing in a word. For example, ***„first"*** *becomes* ***„ifrts"****, whereas substitution ciphers works by replacing letters or group of letters with other letters or group of letters. The first noted example of written cryptography was the ciphertext, in the form of non-standard hieroglyphs, which was carved on monuments by the Egyptians about 1900 BC. These did not provide much concealment or was not much of an attempt at secret communication, but for the amusement of literate onlookers. About 500-600 BC, Hebrew scribes came up with a simple substitution cipher known as Atbash. Atbash works by reversing the alphabets in the following manner, i.e. the letter* ***„a"*** *is replaced by the letter* ***„z",*** *the second letter* ***„b"*** *is replaced by the letter „y" and so on. For example, „world" is replaced by „dliow."*

*About 487 BC, the Greeks and the Spartans used the „scytale" transposition cipher to secretly communicate during military campaigns. This scheme consists of a rod around which a strip of parchment or leather is wound with a message written over it. This rod is called the encryption rod. The recipient is supposed to have a rod of the same diameter and wound the parchment around it to read the message. This way others, not having the rod of same diameter, cannot read the message. The recipient"s rod is called the decryption rod. About 100-44 BC, Julius Caesar used a simple substitution cipher to secretly communicate with his generals. So he replaced every A by a D, every B by an E, and so on. Only someone who knew the ``**shift by 3"** rule could decipher his message*

Encryption in modern times is achieved by using algorithms that have a key to encrypt and decrypt information. These keys convert the messages and data into "digital gibberish" through encryption and then return them to the original form through decryption. In general, the longer the key is, the more difficult it is to crack the code. This holds true because

deciphering an encrypted message by brute force would require the attacker to try every possible key. To put this in context, each binary unit

of information, or bit, has a value of 0 or 1. An 8-bit key would then have 256 or 2^8 possible keys. A 56-bit key would have 2^56, or 72 quadrillion, possible keys to try and decipher the message. With modern technology, cyphers using keys with these lengths are becoming easier to decipher. DES, an early US Government approved cypher, has an effective key length of 56 bits, and test messages using that cypher have been broken by brute force key search. However, as technology advances, so does the quality of encryption. Since World War II, one of the most notable advances in the study of cryptography is the introduction of the asymmetric key cyphers (sometimes termed public-key cyphers). These are algorithms which use two mathematically related keys for encryption of the same message. Some of these algorithms permit publication of one of the keys, due to it being extremely difficult to determine one key simply from knowledge of the other.

1.2.2 Types Encryption

- **Symmetric Encryption**

Is a method of encryption using a secret key to encrypt and decrypt a message, called encryption using the symmetric key because the key used to encrypt the message is the same as the one used to decrypt it,

*There are several algorithms to do this type of encryption, the most famous of which is the(**Data Encryption Standard**)(**DES**), which is still widely used to achieve secure online communication under SSL and other similar fields. It is also the algorithm declared as an encryption algorithm Government Departments in the United States of America since 1976.*

*However, (**DES**) has begun to show weakness in recent years against cryptographic decryption methods and has been replaced in several places with modified versions such as the (**Triple DES**)algorithm. However, (**DES**)*

*was completely replaced as an algorithm approved by the US government at the end of 2001 with the (**Advanced Encryption Standard**) (**AES**).*

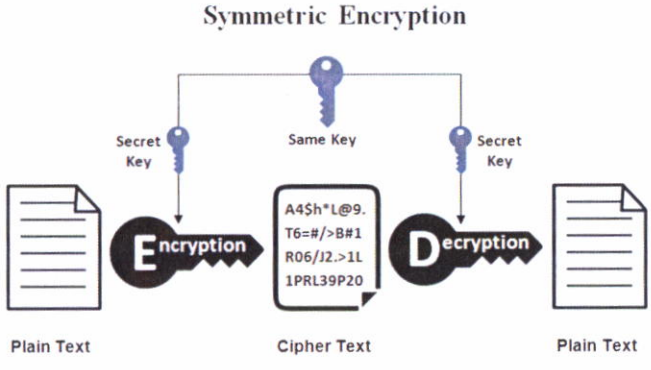

Figure 1.1 Symmetric Encryption

- **Asymmetric Encryption**

Asymmetric encryption is the existence of two keys to complete encryption and decryption, not one key as in Symmetric Encryption.
Asymmetric encryption consists of two keys:

1- ***public key:*** *The public key that is used to encrypt the message, and is sent to the person (group, group ..).*
2- ***Private key****: The private key that is used for decryption is stored on your own device. No one knows the secret of the private key. The code can only be decrypted by the private key. If the private key is lost, you can not decrypt the message!*

Note: The private key is called the secret key too, and can be considered as a password for decryption.

Mechanism of action:

After you configure the two keys, you send the public key to whom you want (person, group ..), the public key job is to encrypt only the message and not the decryption, the receiving party encrypts the message by using your public key sent to it, The receiver sends the encrypted message to the original sender who sent the public key to it. When the sender receives the encrypted message, it only decrypts the private key, which is the only one that can decrypt from that file

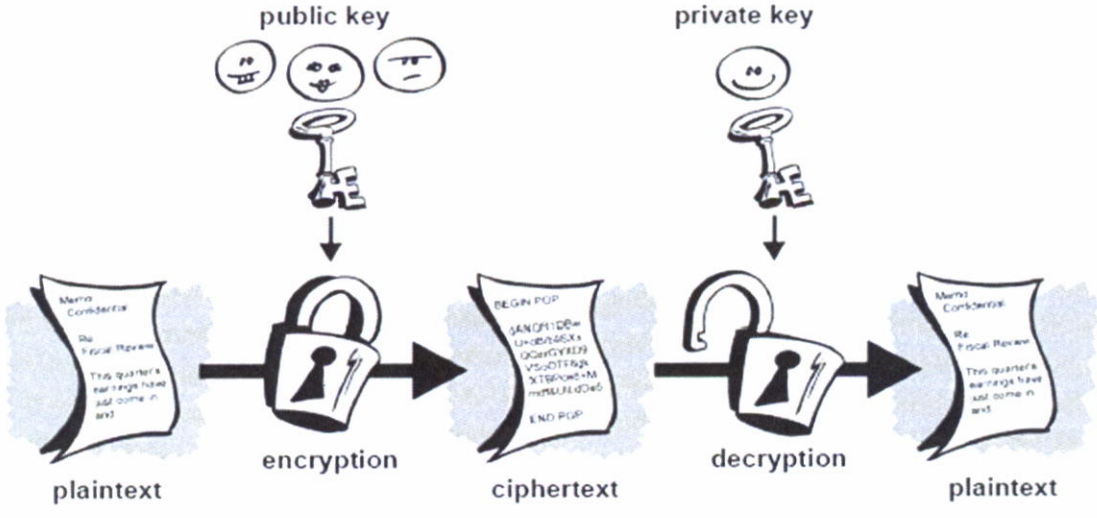

Figure 1.2 Asymmetric Encryption

1.2.3 The main objectives of using cryptography

There are four main objectives behind the use of cryptography:

- *Confidentiality or Privacy: Confidentiality is a service used to store the content of information from all persons except those who have been told to inform it.*
- *Integrity: A service that is used to save information from change (delete, add or modify), by unauthorized persons to make the change.*
- *Authentication: A service used to establish the identity of the customer with the data (authorized).*
- *Non-repudiation: a service used to prevent a person from denying him to do something.*

Therefore, the main objectives of encryption are to provide people with the above services to maintain the security of their information.

1.2.4 The Difference Between Encryption Steganogaraphy

When encrypting information, the third party can tell that there is a two-way connection (two or two) but can not understand the information because it is encrypted.

In the case of stegano graphy, the third party does not know that there is something hidden in secret or that there is a connection between two.

1.3 Steganogaraphy

Steganography is defined as the art and science of writing hidden messages in such a way that no one else, apart from the intended recepient knows the existence of the message. The word "steganography" is basically of Greek origin which means "hidden writing". The word is clas

sified into two parts: steganos which means "secret" and "graphic" which means "writing". However, in hiding information, the meaning of steganography is hiding text or secret messages into another media file such as image, text, sound or video The word "steganography" is often considered similar to
"cryptography" and "watermarking". Whilst watermarking ensures message integrity and cryptography scrambles the message, steganography hides it.

1.3.1 Historical Review to steganography

There are many ancient stories that count the tricks and methods used to hiding information, among these stories are:

- *The ancient Greeks and the Romans shaved slaves' crowns and hid messages on their heads. Then, when the hair had grown out, each slave was sent to a receiver, who shaved the crown again to read the message*
- *In China, they hide a code ideogram at a prearranged place in a dispatch. The hidden codes were then uncovered by putting a template over the message .This method was reinvented in the early 16^{th} century by Cardan (1501-1576), an Italian mathematician and was used by a British bank in 1992 where customers concealed their personal information number used with their cash machine card.*
- *In Tudor England, when Mary Queen of Scots was imprisoned at Chartly Castle, she sent secret messages to the Catholics including the French Ambassador, by hiding the letters inside the empty beer barrels that left the Castle .*
- *Microdots are also another form of steganography used in modern times. The microdot is essentially a photograph of the secret message that is to be delivered. With technological advancements,*

it is possible to take a picture of the message and shrink it down to a circular photograph of 0.05 inches in diameter. This tiny photograph is then glued onto either a period or a dot of an "i" on another message to be delivered. Only those that know to look for this microdot should be able to detect its presence .

1.3.2Steganography Techniques

Many different steganographic methods have been proposed during the last few years; most of them can be seen as substitution systems. Such methods try to substitute redundant part of the signal with a secret massage; their main disadvantage is the relative weakness against cover modification.

There are several approaches in the classifying Steganographic Techniques. One of these approaches is to categorize them according to the cover modifications applied in the embedding process. Mainly, Steganographic Techniques may be grouped in to five categories as follows :

1. ***Substitution Techniques:*** *Substitute redundant parts of a cover with a secret message. Basic substitution systems try to encode secret information by substituting insignificant parts of the cover by secret message bits; the receiver can extract the information if he has knowledge of the positions where secret information has been embedded. Since only minor modifications are made in the embedding process, the sender assumes that they will not be noticed by an attacker. There are six types of substitution techniques: least significant bit substitution, pseudorandom permutations, audio down grading, cover-regions and parity bits, pallet-based audios, and quantization method. The Substitution Technique was used in the suggested work.*

2. ***Transform Domain Techniques:*** *Embed secret information in a transform space of the signal. The substitution modification techniques are easy way to embed information, but they are highly vulnerable to even small cover modifications. An attacker can simply apply signal processing techniques in order to destroy the secret information entirely. It has been noted early in the development of steganographic systems that embedding information in the frequency domain of a signal can be much more robust than embedding rules operating in the time domain.*

3. ***Spread Spectrum Techniques:*** *Spread Spectrum (SS) is a mean of transmission in which the signal occupies a bandwidth in excess of the minimum necessary to send the information.*

4. ***Statistical Techniques:*** *This technique utilize the existence of 1bit steganography schemes, which embed one bit of information in a digital carrier. Encode information by changing several statistical properties of cover.*
5. ***Distortion Techniques:*** *Store information by signal distortion and measure the deviation from the original cover in the decoding step.*

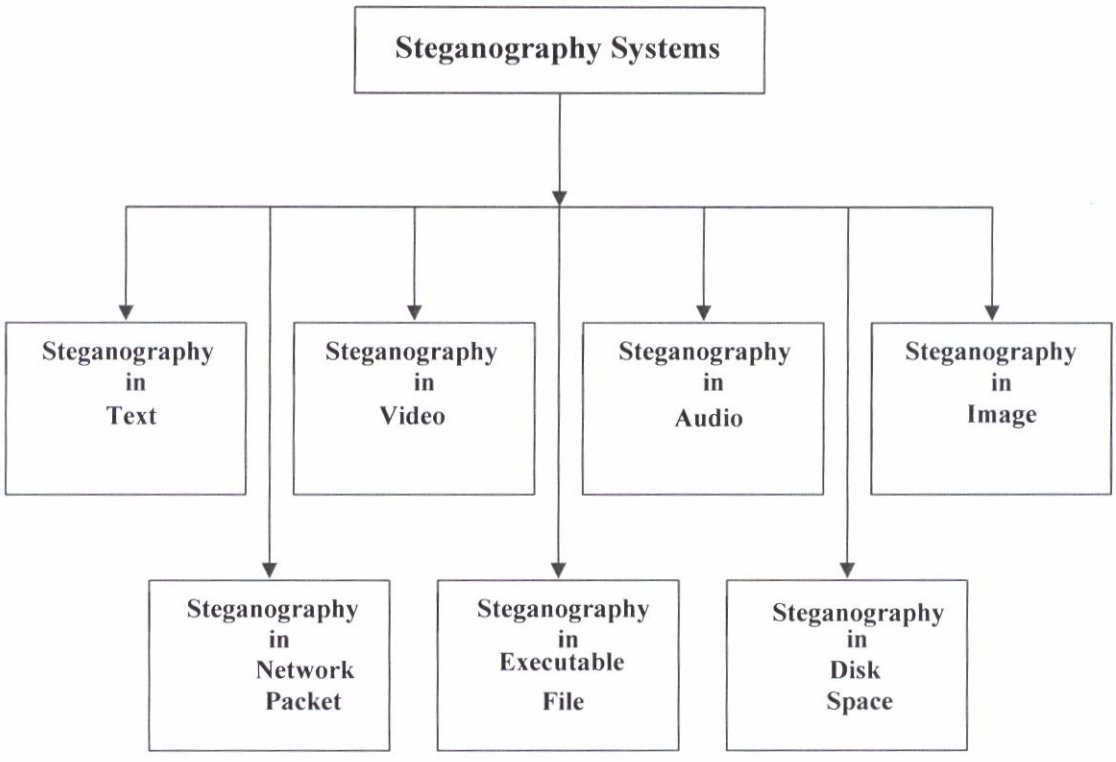

Figure 1.3. Steganography classification over different covers .

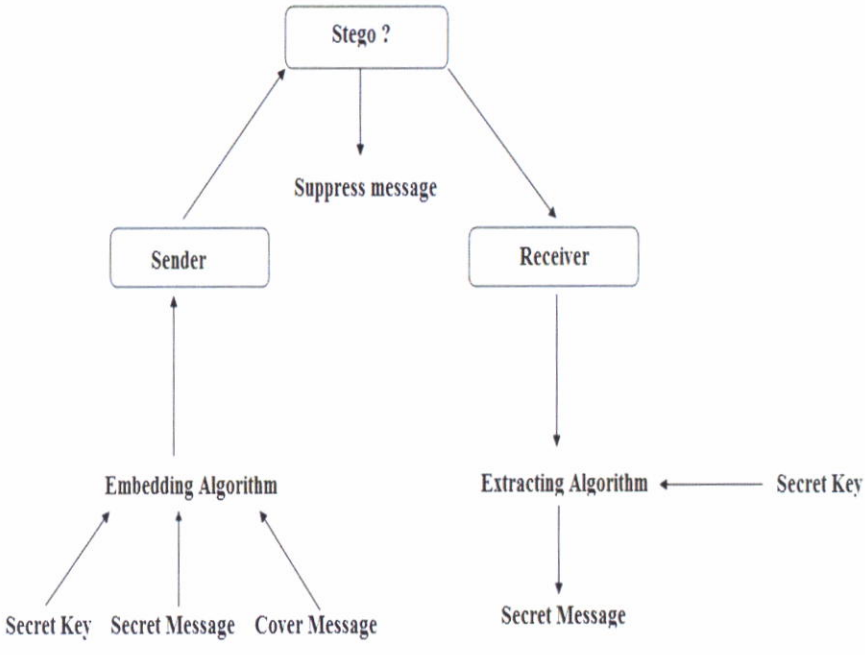

Figure 1.4: General Steganographic Approach.

1.4 Microsoft Visual studio 2010

is an integrated development environment (IDE) from Microsoft. It is used to develop computer programs, as well as websites, web apps, web services and mobile apps. Visual Studio uses Microsoft software development platforms such as Windows API, Windows Forms, Windows Presentation Foundation, Windows Store and Microsoft Silverlight. It can produce both native code and managed code.

Visual Studio includes a code editor supporting IntelliSense (the code completion component) as well as code refactoring. The integrated debugger works both as a source-level debugger and a machine-level debugger. Other built-in tools include a code profiler, forms designer for building GUI applications, web designer, class designer, and database schema designer. It accepts plug-ins that enhance the functionality at almost every level—including adding support for source control systems (like Subversion and Git) and adding new toolsets like editors and visual designers for domain-specific languages or toolsets for other aspects of the software development lifecycle (like the Team Foundation Server client: Team Explorer).

Visual Studio supports 36 different programming languages and allows the code editor and debugger to support (to varying degrees) nearly any programming language, provided a language-specific service exists. Built-in languages include C,[7] C++, C++/CLI, Visual Basic .NET, C#, F#,[8] JavaScript, TypeScript, XML, XSLT, HTML, and CSS. Support for other languages such as Python,[9] Ruby, Node.js, and M among others is available via plug-ins. Java (and J#) were supported in the past.

- ***Features Visual studio2010***

1 . Easy and fast language for creating Windows applications.

2. supports object oriented programming but not fully.

3. Easy to learn and understand

4. Easily detect errors in them

5.it contains Code editor,Debugger,Designer, Other tools

6. When you write valid orders, it gives you examples to confirm that the code is correct

7. Allows you to skip some errors when writing a specific code

8. relying on HTML, making it easy to use and understand.

Chapter Two

2.1 Previous Studies On Encryption

[*Geeta Shantanu Joshi on February, 2013*] In this research, the modified RSA algorithm was used to transfer files securely. The RSA algorithm is an asymmetric key encryption, also called public key encryption. There are many situations where we need secure file transfers, for example in banking, shopping, etc. Two keys are created in RSA, one encryption key is used, and the other key that identifies the authenticated recipient can only decrypt the message.

Many improvements have been made to improve RSA such as RSA BATCH, RSA MultiPrime, RSA MultiPower, RSA Rbalanced, RSA RPrime, etc.

The purpose of this search is to encrypt files and transfer encrypted files to the other party where they are decrypted. The project works efficiently for its small size while consuming time for large file size. At one moment only one file can be encrypted and transferred

[***Tanmoy Bishoi on 29 July 2015***] In this research, a key cryptographic algorithm was used that uses ASCII values for input text to encrypt data.

In this research, a coding algorithm was proposed based on symmetric key encryption technology. As the system used in this above research gives good results where the system can be improved using the variable length switch. It can also be improved to decrypt the data message format. With this goal in mind, the algorithm was designed in a very simple way but tried to keep the security problem at a high value.

[***M. A. Murillo-Escobar on 2014***]In this research, a symmetric-based cryptographic algorithm was used. The algorithm uses a 128-bit secret key, two logistic maps with improved pseudo-random sequences, clear text graphics, and only one flipping cycle. Many scurity analyzes were presented as secret key size, secret key sensitivity, replication with histogram, automatic correlation analysis, information entropy analysis, differential analysis, classical attack analysis, and encryption / decryption time. Based on numerical simulation results, the proposed encryption algorithm offers excellent encryption time and time, and can resist a strong / known plain text attack; therefore, it can be implemented in real time applications .

2.2 Previous Studies on Steganography

[Vipul Sharma , Sunny Kumar April 2013] In this research a new design algorithm was proposed that is used to hide a text file inside an image. To increase / increase storage capacity, and use a compression algorithm to compress the data to be included.

The compression algorithm used is used in a range of 1 bit and 8 bits per pixel. By applying this algorithm,

The system was developed in Java based on the proposed algorithm. A few images were tested with different sizes of text files to be hidden as the resulting stego images did not contain any noticeable changes. We also found that for .bmp images, this algorithm works very efficiently

[**Shailender Gupta ,June 2012**] In this research, the common algorithm (Rivest, Shamir, Adleman (RSA), and the Diffie Hellman algorithm were used to encrypt the data.The result shows that the use of encryption in Steganalysis does not affect the complexity of time if this program uses the Diffie dream algorithm instead of the RSA algorithm.

LSB modulation is an easy way to embed information into images, but data can be easily decoded. The proposed schema used in this search encrypts confidential information before it is included in the image. The complexity of the overall process is certainly increasing, but at the same time, the security of that cost is worth it. This encryption scheme can also be used to hide other information.

[Jumana Waleed November 2008] In this research Steganography was implemented in audio files to hide your private and confidential data in these files in a way that no one recognizes that you know it exists. The common method of cloaking information in the acoustic envelope involves using a wildcard

(Least Significant Bit (LSB)).

The proposed system uses the concept of hiding blind information that does not require an original audio file at the extraction stage.

To increase latency and system security, secret text is compressed using compression methods

(Run Length Encoding and Shift-coding.) To support the immunity of the proposed concealment system and additional security levels,

From the test results obtained from the proposed system, recommend that audio files have good covers to hide confidential data using the capacity modulation method because they do not lose anything confidential.

Chapter Three

Search Methodology

3.1 Flowchart around the program

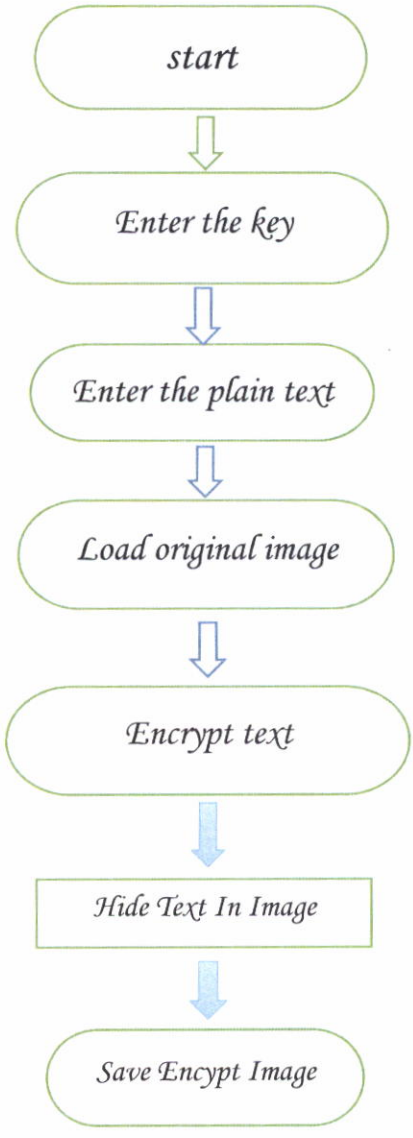

Figure 3.1 : *Encrypt and hide text*

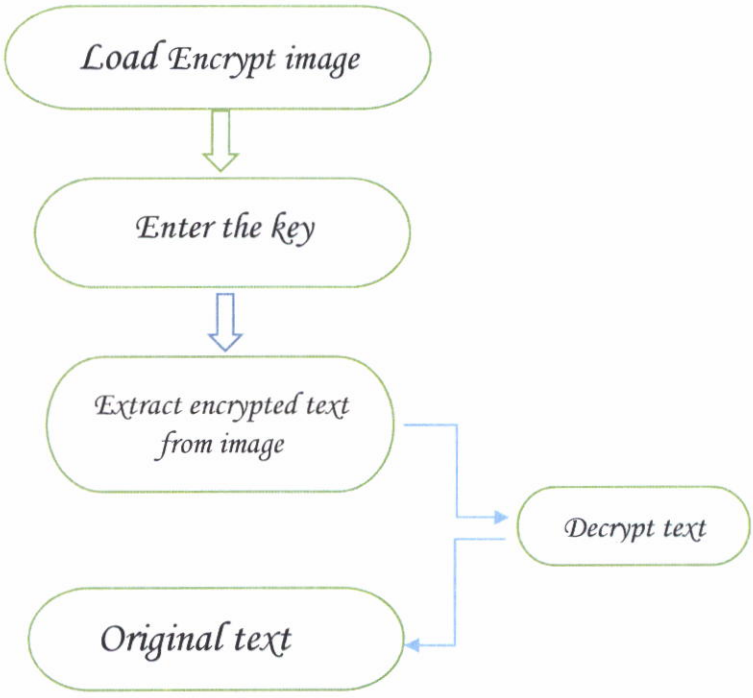

Figure 3.2 *: Extract encrypted text from image and Decrypt text*

3.2 program interfaces

The following program contains two interfaces

3.2.1 The first interface

is a welcome interface that contains the name of the program and the name of the program designer, and contains a button to access the main interface of the program as shown in the figure below.

Figure 3.3 : *The first interface*

3.2.2 The main interface

Is the main interface of the program where this interface contains the left side at the top of two lists and each list contains several orders as the file list contains several orders of them

1. load image

2. save photo

3. Exit the program

The action menu also contains a number of commands

1. Encrypt text

2. Hide Text In Image

3. Extract encrypted text from image

4. Decrypt text

The façade also contains a place to insert a key

To encode and decrypt and a place to load the text to be encrypted

And a place to display the encrypted text

It contains a place to display the original picture and place to display the encrypted image as shown in the figure below.

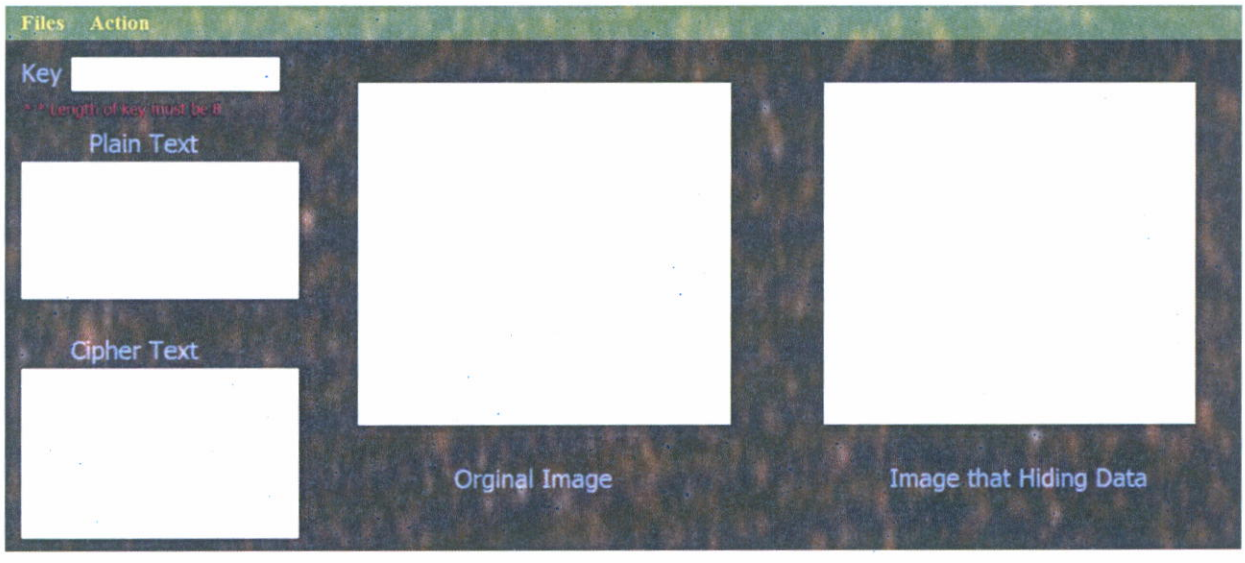

Figure 3.4 : *The main interface*

Let's take an example of how the current program encrypts a text message and hide it in a bitmap. Let's say the message we want to encrypt is:

"The boy stood on the burning deck ..."

- *Mechanism of action of the program as follows*

1.enter the key to encrypt

2. Writing text

3. Load original image

4. Encrypt text

5. Hide Text In Image

***Figure 3.5** : load normal image and Writing text and Encrypt text*

4 .Save encrypted images

- *To decrypt the text we do*

1.load Encrypt imag.

2. Enter the key

3.Extract encrypted text from image

4. Decrypt text