International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 05 | May - 2023 Impact Factor: 8.176 ISSN: 2582-3930

Efficient Approach for Secure Data Transfer Using Cryptography and Steganography Technique

Balasubramanyan. A

Computer Science and Engineering & P. A. College of Engineering and Technology

---

Abstract - Steganography is the practise of concealing information within other information in order to disguise the fact that communication is occurring. Although there are other carrier file types available, digital photographs are the most widely employed due to their prevalence online. There are several different steganography techniques available for covering up sensitive information in images and audio, some of which are more difficult than others. Each technique has its own strengths and weaknesses. Different applications can need the secret information to be completely undetectable, while others might need a sizable secret message to be concealed.

Key Words: Image security, steganography algorithms, cryptography, Data security, video or audio content.

1.INTRODUCTION

One of the reasons that intruders can be successful is the most of the information they acquire from a system is in a form that they can read and comprehend. Intruders may reveal the information to others, modify it to misrepresent an individual or organization, or use it to launch an attack. One solution to this problem is, through the use of steganography. Steganography is a technique of hiding information in digital media. In contrast to cryptography, it is not to keep others from knowing the hidden information but it is to keep others from thinking that the information even exists. Due to advances in ICT, most of information is kept electronically. Consequently, the security of information has become a fundamental issue. Besides cryptography, steganography can be employed to secure information. In cryptography, the message or encrypted message is embedded in a digital host before passing it through the network, thus the existence of the message is unknown. Besides hiding data for confidentiality, this approach of information hiding can be extended to copyright protection for digital media: audio, video and images.

1.1 Importance of Steganography

Steganography has advanced significantly in recent years as a result of the ability of digital tools to conceal information inside of other information in novel ways. Armed forces were the first to deploy covert communication methods, such as radio transmissions, due to the strategic value of secure communication and the need to mask the source as much as possible. Steganography and cryptography both aim to shield information from unauthorized persons in the digital realm. While Steganography and Cryptography are both excellent tools for achieving this, neither technology is infallible on its own and both can be exploited. For this reason, the majority of experts advise employing both to provide additional protection levels. In today's digital age, there are many different data types that can apply steganography. The most often utilized file types are.bmp,.doc,.gif,.jpeg,.mp3,.txt, and.wav. primarily because the steganographic tools that use them are simple to use and they are widely used on the Internet.

1.2 steganography protocols

In practice there are three types of steganography protocols used:

Pure steganography

In order for the recipient to read the message, a steganographic system is considered to be pure steganography if no stego-key or password exchange is required.The sender and recipient must rely only on the assumption that no other parties are aware of this secret communication, making this kind of steganography the least secure way to communicate in secret.

Secrete key steganography

Secret Code A steganographic system is defined as one that calls for the exchange of a secret key (stego-key) before communication may take place. Only those with access to this secret key can use a Stego-key to reverse the process and view the message. The advantage of Secret Key Steganography is that even if it is intercepted, the secret message cannot be deciphered without the secret key.

Public key steganography

Private Key A steganographic system that uses a public key and a private key to secure communication between parties seeking to communicate in secret is referred to as a steganographic system. Only the private key, which has a direct mathematical link with the public key, can be used by the receiver to decode the message after it has been encoded by the sender using the public key. It also has many degrees of security in that unauthorized parties would first need to be suspicious of the usage of steganography before they could intercept the secret message, and even then, they would need to figure out how to break the public key system's encryption algorithm.

2. MODEL OF STEGANOGRAPHY

The Greek words "Seganos," which mean covered or secret, and "graphy," which means writing or drawing, are the origin of the word "steganography." Steganography is thus defined as covered writing in its literal sense. It is both an art and a science to conceal information so that conversation can take place without anyone noticing. A covert information is one that has been encoded in a way that hides its very existence. Steganography can be utilized to conduct covert communications when combined with currently used communication channels. The major objective of this work is to securely communicate in an entirely undetectable manner and to prevent suspicion from being raised regarding the transmission of a hider data. Steganography has seen a sharp rise in popularity for two reasons:

Techniques for obscuring encrypted copyright indications and serial numbers in digital movies, audio recordings, books, and multimedia items have attracted the attention of the publishing and broadcasting industries.

People are studying ways to hide private messages in seemingly innocent cover messages as a result of efforts by various governments to restrict the use of encryption services.

The Carrier, Message, and Password components make up the fundamental steganography model. Carrier, in which the message is embedded and used to conceal its existence, is also known as a cover-object.

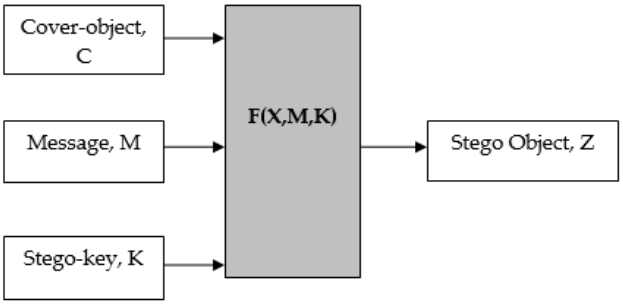

Fig -1: Model for steganography

The information in a message is information that the sender wants to keep private. It can be anything that can be included in a bit stream, including plain text, ciphertext, other images, serial numbers, and copyright marks. Stego-key, a password, makes sure that only recipients who are aware of the appropriate decoding key will be able to decode the message from a cover-object. The Stego-object is the cover-object with the hidden message buried in it.

If a stego-key was used during the encoding procedure, the cover-object itself and the matching decoding key are needed to recover the message from a stego-object. Most applications may or may not require the original image in order to extract the message.

Below are a few carriers that could serve as the cover-object:

• Internet protocol suites like TCP, IP, and UDP

• Digital audio files in the wav, midi, avi, mpeg, mpi, and voc formats

• Text such as null characters, similar as morse code, including html and java

• Images file such as bmp, gif, and jpg, where they may be both colour and grayscale.

• File and Disc that can hide and append files by exploiting the slack space.

The information concealing method often removes unnecessary bits from the cover item. There are two steps in the procedure:

(i)Identification of redundant bits in a cover-object. Redundant bits are those bits that can be modified without corrupting the quality or destroying the integrity of the cover-object.

(ii) Embedding process then selects the subset of the redundant bits to be replaced with data from a secret message. The stego-object is created by replacing the selected redundant bits with message bits.

3. TYPES OF STEGANOGRAPHY

(i) Text Steganography
Text files can contain steganography, which involves discreetly storing information. With this technique, each word's letter contains an encoded version of the hidden data.

(ii) Image Steganography
picture steganography is the second kind of steganography, which involves hiding data by utilising a picture of an alternative object as a cover. The secret to data steganography in images is pixel intensities.

(iii) Audio Steganography
Audio steganography is the study of concealing information in sound. It safeguards against unauthorized reproduction when used digitally. By encrypting one piece of data (the message) inside another (the "carrier"), watermarking is a technique. Media playback, primarily audio clips, is what it is typically used for.

(iv) Video Steganography
Using video steganography, data or other files can be covertly included in video files on a computer. The "carrier" in this design can be video (a compilation of still images). The discrete cosine transform (DCT), which is invisible to the naked eye, is frequently used to insert values that can be utilised to obscure the data in each image in the movie. H.264, MP4, MPEG, and AVI are the most frequently used file formats for video steganography.

(v) Network or Protocol Steganography
Network or Protocol Steganography entails hiding data by utilising a network protocol as a cover object, such as TCP, UDP, ICMP, IP, etc. In the case of covert channels, which exist in the OSI layer network model, steganography can be applied.

3.1 Steganography Tools

Steganography support tools and software are now widely available. The majority conceal information, but some increase protection by encrypting it first. The following internet resources for steganography are free:

Steghide: A free programme called Steghide uses steganography to hide data in other files, such media or text, by encrypting it.

Stegosuite is a free steganography tool that runs on Java. Data in images can be easily obscured for covert purposes using Stegosuite.

With the aid of **Open Puff**, you can cloak data in different media kinds including pictures, movies, and Flash animations. It is a top-notch steganographic tool.

Xiao Steganography: Use the free Xiao Steganography programme to hide data in WAV or BMP files.

SSuite Picsel: The free portable programme SSuite Picsel provides an additional choice for obfuscating text within an image file, although it does it in a somewhat different way than other programmes.

4. IMAGE STEGANOGRAPHY AND BITMAP

One of the most widely used methods for steganography is the use of bitmap images to conceal sensitive information. There are several different kinds of software designed for this purpose; some of these use password securities to encrypt data on images. Because the algorithm for "BMP" pictures for steganography is straightforward, using other types of pictures like "JPEG" or "GIF" or any other types is rarely or never used with this software. Additionally, we are aware that "JPEG" and other image types other than "BMP" are the most popular image types on the web, so this issue needs to be solved. This software offers a solution to the issue; it can use any kind of image to conceal data files, but in the end, it only produces "BMP" images with concealed files.

4.1 Bitmap Steganography

The bitmap format is the most basic type of image because it lacks any technology for file size reduction. These files have the structure of a bitmap image, where each pixel is made up of three colours (red, green, and blue, or RGB), with each colour representing one byte of information that demonstrates the density of that colour. Every colour we see in these images is the result of combining these three hues. The concept for employing steganography science came from the fact that every byte in computer science is made up of 8 bits, with the first bit being the Most-Significant-Bit (MSB) and the final bit being the Least-Significant-Bit (LSB). We use the LSB bit for encoding our security information inside BMP photos. As a result, if we only use the eighth layer of information, we must modify the final bit of each pixel. Since each pixel has three bits, we can store information in 3*high*width bits of memory. However, we must first write the file's name, size, and size of the data before we can write our data. By allocating a few first layers of memory, we can achieve this.

(00101101 00011101 11011100)

(10100110 11000101 00001100)

(11010010 10101100 01100011)

Using each 3 pixel of picture to save a byte of data. This method involves transforming plain text into cypher text. By using a cryptography approach, highly secure data can be encrypted. This method aids in converting material in a way that prevents comprehension. The encrypted data can only be decrypted by the permitted user.

For a secure delivery of message signals, a successful steganographic technique should have the following desired properties:

Secrecy: Disabling aperson to extract the covert data from the host medium without the prior knowledge of the proper secret password or key which is used in the extracting procedure.

Imperceptibility: The medium after being embedded with the covert data should be indiscernible from the original medium. One should not be so suspicious of the existence of the covert data within the medium.

High capacity: Highest length of the covert message that can be embedded should be as long as possible case can handle.

Resistance: The covert data should survive even when the host medium has been manipulated, for example by some lossy compression scheme.

Accurate extraction: The retrival of the covert data from the medium should be accurate and reliable.

4.2 Low-Bit Encoding of Audio Files

One of the easiest methods for incorporating data into other data structures is low-bit encoding. We can encode a substantial quantity of data in an audio signal by substituting a coded binary string for the least significant bit of each sampling point. In a noiseless channel, the bit rate will be 8 kbps for an 8 kHz sampled sequence and 44 kbps for a 44 kHz sample sequence. The channel capacity should ideally be 1 kb per second (kbps) per 1 kilohertz (kHz). This large channel capacity comes with the addition of audible noise. The impact of this noise depends directly on the host signal's content; for example, crowd noise at a live sporting event would cover up low-bit encoding noise that would otherwise be audible.

This variance has been offset using adaptive data attenuation. This method's weak immunity to manipulation is its main benefit. Unless information is encoded using redundancy techniques, it can be destroyed by channel noise, re-sampling, etc. These strategies decrease the data flow in order to be robust, which may result in the demand of a host of higher magnitude, frequently by one to two orders of magnitude. This technology only works in closed, digital-to-digital situations in real life.

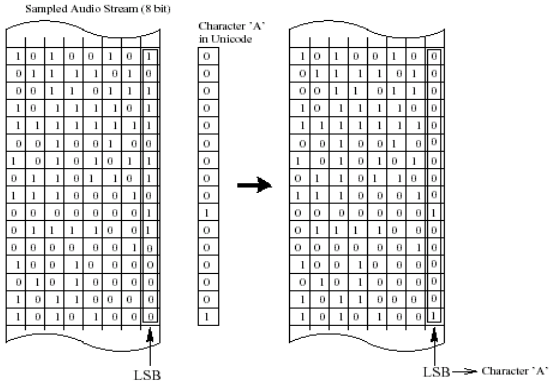

Fig -2: Adaptive data attenuation technique

4.3 Phase Encoding

The phase of an initial audio segment is replaced with a reference phase that represents the data in the phase coding method. The relative phase between segments is maintained by adjusting the phase of succeeding segments. In terms of the signal to perceived noise ratio, phase coding is one of the best coding techniques. A notable phase dispersion will arise when there is a significant change in the phase relationship between each frequency component. However, an inaudible coding can be achieved as long as the phase modification is sufficiently minor. The phase of an initial audio segment is replaced with a reference phase that represents the data in the phase coding method. The phase coding process is as follows:

- The original audio stream is divided into N discrete segments.
- Each segment is subjected to a Discrete Fourier Transform (DFT) in order to separate and produce a matrix of the phase magnitude.
- Each adjacent segment's phase difference is determined.

• For the first segment, segment S0, an artificial absolute phase p0 is produced.

• New phase frames are made for the other segments.

• A new segment, Sn, is created by combining the original magnitude and the new phase.

• The encoded output is then produced by joining the new segments.

Prior to decoding, the sequence is synchronized for the decoding process. The receiver must be aware of the segment length, DFT points, and data interval. It is determined that the underlying phase of the first segment has a value of 0 or 1, which stands for the binary coded string. From our perspective, this is intriguing for a number of reasons. First off, a watermark that is incorporated into the DFT phase would resist tampering pretty well. The primary data that makes up watermarks is almost usually highly redundantly encoded. Consequently, for a watermark to be successfully transmitted, background noise and intentional phase distortions from a "enemy" would need to be very noticeable. The image quality would suffer unacceptable harm as a result. Second, it is generally known from communications theory that angle modulation has better noise resilience than amplitude modulation. Additionally, we discover that phase is fairly resilient to variations in image contrast.

4.4 Steganography Techniques

Numerous steganography methods that incorporate secret messages into multimedia objects have been put forth in recent years. There are several ways to change an image in a way that is perceptually undetectable while yet concealing information or messages. LSB, Masking and filtering, and transform techniques are common ways. A straightforward method for including data in image files is to use the least significant bit (LSB) insertion. The simplest steganography methods directly embed the message's bits in the cover image's least significant bit plane in a predetermined order. Because the amplitude of the change is small, modulating the least significant bit does not produce a difference that is perceptible to humans. Using two or more least significant bits in this method can boost the embedding capacity. The risk of making the embedded message statistically detectable increases at the same time that the image fidelity deteriorates.

This leads to the presentation of a variable size LSB embedding scheme, where the number of LSBs used for message embedding/extracting varies on the local features of the pixel. The simplicity of implementation and large message pay-load of the LSB-based approach are advantages. Although LSB conceals the message in a way that humans cannot perceive it, the opponent may still be able to retrieve the message due to the technique's simplicity. Therefore, if someone is malicious and suspects that the image contains hidden information, they can try to extract the message from the beginning of the image.

As a result, the Secure Information Hiding solution (SIHS) is suggested as a solution to enhance the LSB technique. The sequence-mapping issue is solved by embedding the massage into a collection of random pixels that are dispersed over the cover image. In a manner akin to paper watermarks, masking and filtering techniques, which are typically limited to 24 bits and grey scale images, conceal information by marking an image. The method analyses the image and embeds the information in key regions, making the concealed message more vital to the cover image than simply burying it in the background noise. By modulating a coefficient in a transform domain, transform algorithms, such the Discrete Fourier Transform or Wavelet Transform, incorporate the message. These techniques are more resistant to assault because they conceal messages in substantial portions of the cover image. You can apply transformations to an image's full surface, to individual pixels, or in other ways.

4.5 Steganography Vs Cryptography

In essence, the goal of steganography and cryptography is to enable hidden communication. Steganography, however, differs from cryptography in several ways. Steganography even conceals the presence of the communication, while cryptography obscures the contents of a secret message from malevolent individuals. The system is compromised in cryptography when the secret message may be read by the attacker. In order to defeat a steganography system, the attacker must recognize its use. By employing cryptography to encrypt the message and steganography to conceal it, the two techniques can be combined. The generated stego-image can be transferred covertly while yet maintaining confidentiality.

4.6 Steganography Vs Watermarking:

Steganography focuses on the degree of invisibility, whereas watermarking places a greater emphasis on the message's robustness and ability to fend off removal attempts, such as image operations (rotation, cropping, filtering), and audio operations (rerecording, filtering), in the case of watermarked images and audio files, respectively. The delectability of a vessel with introduced data (a steganographic message or a watermark) is undoubtedly a function of the algorithm's changeability function over the vessel.

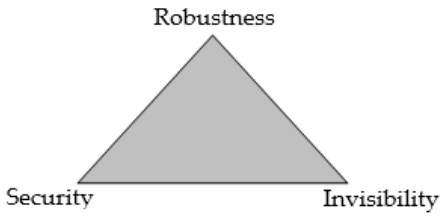

Fig -3: Triangle of conflict

Since delectability is a function of file characteristics deviation from the norm, embedding operation attitude and change severity of such change decides vessel file delectability, that is how the algorithm changes the vessel, and the severity of such an operation determines without a doubt the delectability of the message. Invisibility, Robustness, and Security in a message serve as a common triangle of conflict. The in notability of the message's contents inside the vessel is gauged by its invisibility. Robustness is the ability of the communication to withstand attacks that would cause it to be altered or removed without being compromised. It is frequently utilised in the field of watermarking because while watermarking aims to make the watermark resistant to attacks, steganographic signals typically have a high susceptibility to such attacks. Because encryption requires storage, messages that are more difficult to read are also less reliable because there is no error checking or recovery mechanism.

5. SYSTEM DESIGN

Any kind of image file is needed for steganography, as well as the information or message that needs to be concealed. It features two encryption and decryption modules.

The company Microsoft. The Net Framework provides programmers with a vast array of tools and alternatives for straightforward programming. One of .The majority of picture kinds are automatically converted to BMP format by Net programmes for pictures and images.

Instead of using just the LSB layer of the image, the technique utilised for encryption and decryption in this application uses many layers. Since the significance of the bottom layer, the eighth or LSB layer, is the least significant, writing data begins there because the significance of every subsequent layer has doubled. Therefore, image quality degrades and image retouching occurs as we move up the layers.

Information is concealed in an image using the encrypt module; neither the information nor the file is visible to anyone. This module accepts any kind of image and message and outputs a single image file.

To unlock the information that is buried within an image file, utilize the decrypt module. It uses the image file as an output and outputs two files—one of which is the identical image file and the other is a hidden message file—to the target folder.

Before encrypting the file inside the image, we must save the file's name and size in a certain location on the image. In the LSB layer, we could save the file name before the file information and the file size and file name size in the image's most right-down pixels. To retrieve a file from an encrypted image in the decrypted state, this information must be written.

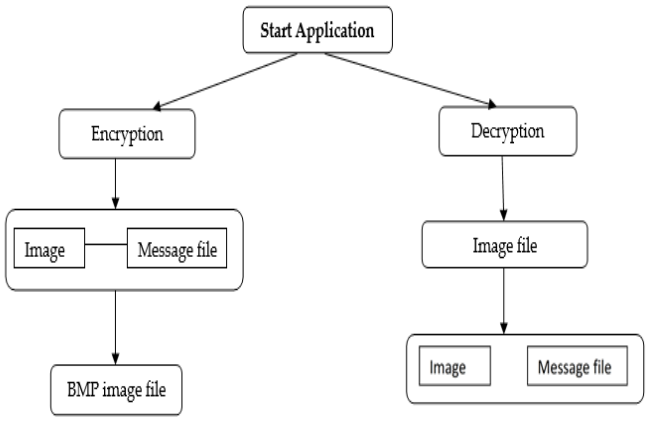

Fig -4: Graphical representation

5.1 Modules

Data hiding and extracting from an audio file is done in four main modules.

1) Login

2) Adding files

3) Embed module.

4) Extract module.

Login Module:

In this module the user can log in to the project and can proceed with the data hiding.

Adding Files:

In this module the authorized user can add the files that are used to embedding process. The files should be the input and output files of wave and text files. For the embedding process the key file should be chosen.

Embed module

(To embed the text file into the audio file)

In this module, the first step is selecting an input audio file. The selection is made through opening a new dialog box and the path selected is displayed through a text box. The second step is selecting an output audio file in which text data or a text file is embedded. The third step is choosing a text file or typing any text message for embedding. Fourth step is selecting a key file. In the fifth step what ever the files that we have selected are viewed and verification of the path is done. In the sixth process data is embedded in to the audio file using low bit encoding technique. After embedding the content both the audio files are played and a listener cannot find any difference between the audios.

Extract module

(To extract the text file from the audio file)

In this module, the first step is the process of selecting the encrypted audio file. This is the file, that a user has to extract information from the output audio. Second process involved in selecting a new text file to display the embedded meassage. Symmetric encryption method is used here, so the key selected during the embedding process is used in decrypting the message. All the process done till now are displayed using a list box and finally the embedded message can be viewed with the help of a file or in a textbox**.**

6. SYSTEM RESULT AND ANALYSIS

This is the first screen which has two-tab options – one is Encrypt Image for encryption and another is Decrypt image for decryption. In right –top panel is displaying the information about the image such as size, height and width.

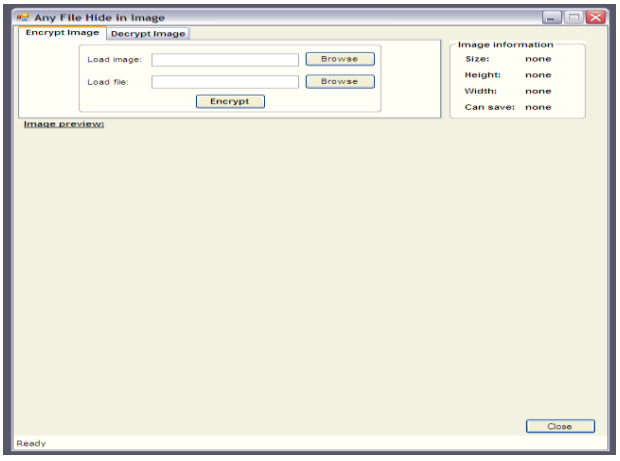

Fig -5: Hide Image by P2P

6.1 Encryption

1. For Encryption select Encrypt Image tab option.

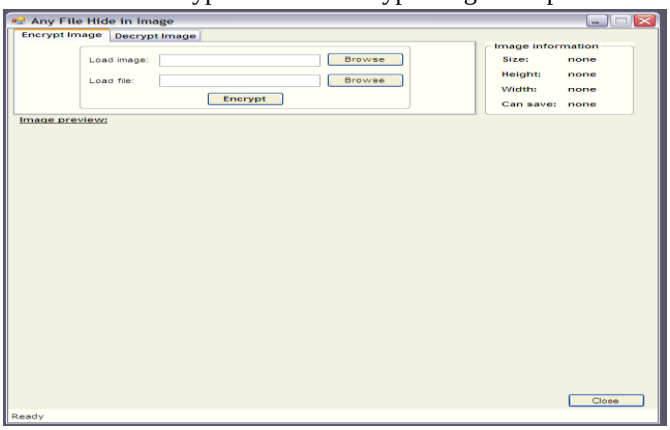

Fig -6 Encrypt image tab option

2. For load image click on button "Browse" that is next to the Load Image textbox. The file open dialog box will display as follows, select the Image file, which you want to use hide information and click on Open button.

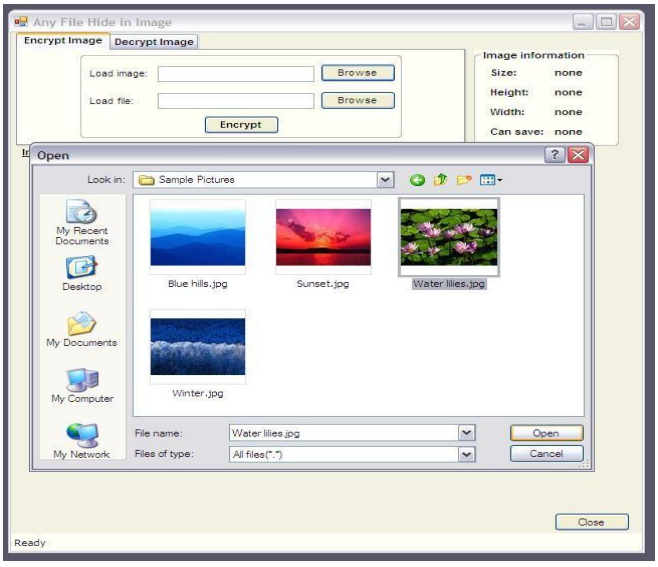

Fig -7 Load image textbox

3.Again the file open dialog box will appear, select any type of file whatever you want to hide with the image and click on ok button.

Fig -8 File open Dialog box

4.The next step is to encrypt the file. Now click on "Encrypt" button, it will open the save dialog box which ask you to select the path to save the New image file and the Image file name. The default format of image file is BMP.

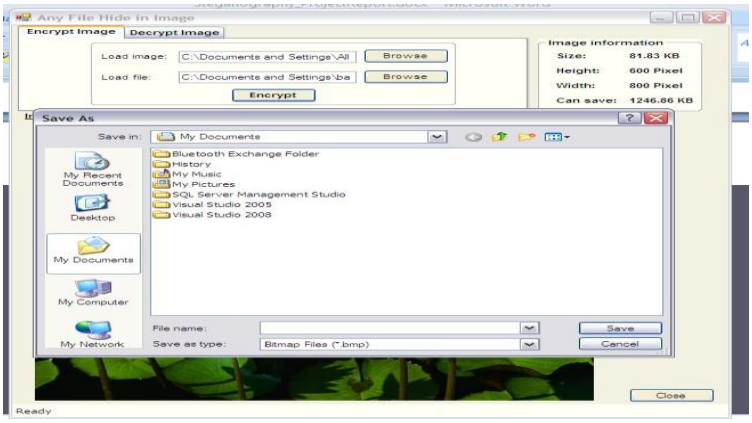

Fig -9 Encrypt File

Fig -10 Encryption Result

6.2 Decryption Process

Now click on Decrypt button, it will decrypt the image, the hidden file and image file is saved into selected folder. The message for successful decryption is displayed on the status bar which is places at bottom of the screen.

Fig -11 Decryption result

7. CONCLUSION

Steganography can be used for hidden communication. We have explored the limits of steganography theory and practice. We printed out the enhancement of the image steganography system using LSB approach to provide a means of secure communication. A stego-key has been applied to the system during embedment of the message into the cover image. Since ancient times, man has found a desire in the ability to communicate covertly. The recent explosion of research in watermarking to protect intellectual property is evidence that steganography is not just limited to military or espionage applications. Steganography, like cryptography, will play an increasing role in the future of secure communication in the "digital world".

REFERENCES

1 1. R. H. Weber, "Internet of Things—New security and privacy challenges," Comput. Law Security Rev., 2010.
2. A. Ukil, J. Sen, and S. Koilakonda, "Embedded security for Internet of Things," in Proc. 2nd Nat. Conf. Emerg. Trends Appl. Comput. Sci. (NCETACS), Mar. 2011.
3. W. Daniels et al., "SμV-the security microvisor: A virtualisation-based security middleware for the Internet of Things," in Proc. ACM 18th ACM/IFIP/USENIX Middleware Conf. Ind. Track, Dec. 2017.
4. U. Banerjee, C. Juvekar, S. H. Fuller, and A. P. Chandrakasan, "eeDTLS: Energy-efficient datagram transport layer security for the Internet of Things," in Proc. GLOBECOM IEEE Glob. Commun. Conf., Dec. 2017.
5. G. Manogaran, C. Thota, D. Lopez, and R. Sundarasekar, "Big data security intelligence for healthcare industry 4.0," in Cybersecurity for Industry 4.0. Cham, Switzerland: Springer, 2017.
6. H. Sun, X. Wang, R. Buyya, and J. Su, "CloudEyes: Cloud-based malware detection with reversible sketch for resource-constrained Internet of Things (IoT) devices," 2017.
7. N. Chervyakov et al., "AR-RRNS: Configurable reliable distributed data storage systems for Internet of Things to ensure security," Future Gener. Comput. Syst., Mar. 2019.
8. S. Raza, H. Shafagh, K. Hewage, R. Hummen, and T. Voigt, "Lithe: Lightweight secure CoAP for the Internet of Things," IEEE Sensors J., Oct. 2013.
9. M. Vucini ˇ c´ et al., "OSCAR: Object security architecture for the Internet of Things," Ad Hoc Netw., vol. 32, Sep. 2015.
10. Y. Yang, X. Liu, and R. H. Deng, "Lightweight break-glass access control system for healthcare Internet-of-Things," IEEE Trans. Ind. Informat., Aug. 2017.
11. A. K. Bairagi, R. Khondoker, and R. Islam, "An efficient steganographic approach for protecting communication in the Internet of Things (IoT) critical infrastructures," Inf. Security J. Glob. Perspective, 2016.
12. C.-T. Huang, M.-Y. Tsai, L.-C. Lin, W.-J. Wang, and S.-J. Wang, "VQ-based data hiding in IoT networks using two-level encoding with adaptive pixel replacements," J. Supercomput., 2018.
13. T. Shanableh, "Data hiding in MPEG video files using multivariate regression and flexible macroblock ordering," IEEE Trans. Inf. Forensics Security, Apr. 2012.
14. X. Liao, J. Yin, S. Guo, X. Li, and A. K. Sangaiah, "Medical JPEG image steganography based on preserving inter-block dependencies," Comput. Elect. Eng., Apr. 2018.
15. C. J. Benvenuto, Galois Field in Cryptography, Univ. Washington, Seattle, WA, USA, 2012.
16. T. Wiegand, G. J. Sullivan, G. Bjontegaard, and A. Luthra, "Overview of the H.264/AVC video coding standard," IEEE Trans. Circuits Syst. Video Technol., Jul. 2003.
17. A. H. Gandomi, X. S. Yang, and A. H. Alavi, "Mixed variable structural optimization using firefly algorithm," Comput. Struct., 2011.