International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

Information Security using Steganography

Mr. Mukesh Gilda,
Asst. Professor, Dept. of ECE,
Sphoorthy Engineering College,
Hyderabad, India,
g.mukesh@sphoorthyengg.ac.in

Ramasani Dheeraj Reddy,
Dept of ECE,
Sphoorthy Engineering College,
Hyderabad, India
dheerajreddyramasani@gmail..com

Surasani Sai Kumar Reddy,
Dept of ECE,
Sphoorthy Engineering College,
Hyderabad, India
saikumarreddysurasani@gmail.com

Chirag kumar Vyas
Dept of ECE,
Sphoorthy Engineering College,
Hyderabad, India
chiragkumarvyas11@gmail.com

Guduru Rohit Reddy,
Dept of ECE,
Sphoorthy Engineering College,
Hyderabad, India
gudrurohitreddy2002@gmail.com

***Abstract*- Information Security has always been a very substantial facet when it comes to hindering unauthorised access, destruction or inspection of confidential data. Today every field in the world makes use of multimedia information. There is need to secure the confidential information used in these areas. There are multiple approaches to secure information. One of them is Steganography, which is the nothing but hiding the information inside other data such that there is no detectable change in cover information. The auxiliary technique of securing information is cryptography, an encryption technique which scrambles the information into a scribbled form which is generally referred to as cipher. Both Steganography and Cryptography have their own advantages and limitations. Even though both methods provide security, to add multiple layers of security it is always a good practice to use Cryptography and Steganography together. So when cryptography and steganography are used together, it results in multi-layer security model. The main objective of the proposed work is to provide extra layer of security by introducing cryptography along with steganography to encrypt and embed the confidential information to be sent over a nonsecure channel.**

Keywords: - Cryptography, Steganography, Unauthorised access, encrypt, embed.

I. INTRODUCTION

In any communication, security is the most important task. With the advancement of technology and the wide use of World Wide Web for communication increase the challenges of security. However, the challenges can be manageable with the advanced technologies of secure networks but every time these technologies may not be reliable for communication of secrete information over a long distance that produce a need of additional security mechanisms to secure secrete information. In this context, to provide the security two techniques has been used widely, Cryptography and Steganography. Cryptography is used to scramble the information, deals with changing the meaning and appearance of message. It changes the plain text into cipher text by the process of encryption, uses the mathematical techniques and various algorithms such as the public key cryptography, private key or symmetric and asymmetric algorithm for securing the information. However, cryptography provide secure solutions to a set of parties, by encrypting plain text into cipher text but the cyber attacker easily arouse these text and intercepts the communication between two separate users to modify, inject, or drop any communication packet. To improve these limitations and to reduce the issues of cryptographic methods an alternative mechanism, the steganography has use widely. Generally the concepts of this techniques differ from the cryptography, where the cryptography method converted the information in a encrypted form that an eavesdropper and cannot be understand, the Steganography technique embeds hidden content in unremarkable cover media so as not to arouse an eavesdropper's suspicion in some cases, sending encrypted information may draw attention, while invisible information will not. However, both cryptography and steganography provide the security but no one standalone techniques are enough of secure information efficiently and different security categories have different requirements and problems.

II. EASE OF USE

Cryptography has followed man through many stages of evolution. Cryptography can be found as far back as 1900 B.C. in ancient Egyptian scribe using non-standard hieroglyphics in an inscription. From 500 – 600 B.C. Hebrew scribes used ATBASH, a reversed alphabet simple solution

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

cipher. From 50 - 60 B.C. Julius Caesar used a simple substitution with the normal alphabet in government communications.

Cryptography continued through history with many variations. Today cryptography has reached a new level, quantum cryptography. Quantum cryptography combines physics and cryptography to produce a new cryptosystem that cannot be defeated without the sender and receiver having the knowledge of the attempted and failed intrusion. steganography was developed and flourished on its own.

Steganography comes from the Greek steganos (covered or secret) and -graphy (writing or drawing). Steganography can be defined as the hiding of information by embedding messages within other, seemingly harmless messages, graphics or sounds. The first steganographic technique was developed in ancient Greece around 440 B.C. The Greek ruler Histaeus employed an early version of steganography which involved: shaving the head of a slave, tattooing the message on the slaves scalp, waiting for the growth of hair to disclose the secret message, and sending the slave on his way to deliver the message. The recipient would have the slave's head to uncover the message. The recipient would reply in the same form of steganography.

III. CRYPTOGRAPHY

Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication. In addition, Cryptography is also known as the science of secret writing. The goal of cryptography is to make data unreadable by a third party. Cryptography algorithms are divided into symmetric (secret-key) and asymmetric (public-key) network security protocols. *Symmetric algorithms* are used to cipher and decipher original messages (plaintext) by using the same key. While A*symmetric algorithms* uses public-key cryptosystem to exchange key and then use faster secret key algorithms to ensure confidentiality of stream data. In Public-key encryption algorithms, there is a pair of keys, one key is known to the public, and is used to encrypt information to be sent to a receiver who owns the corresponding private key. The private and public keys are both different and need for key exchange.

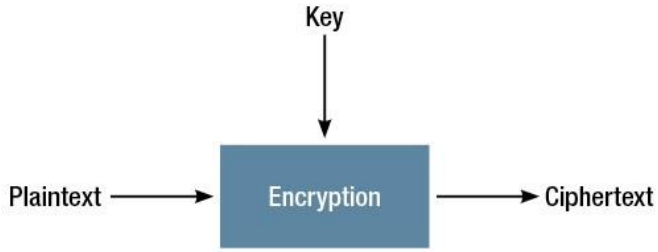

Fig. 1: Cryptographic system

Cryptographic systems are generically classified along three independent dimensions.

1. <u>*Methodology for transforming plain text to cipher text*</u> All encryption algorithms are based on two general principles: substitution, in which each element in the plaintext is mapped into another element, and transposition, in which elements in the plaintext are rearranged. The fundamental requirement is that no information be lost.

2. <u>*Methodology for number of keys used*</u> There are some standards methods which is used with cryptography such as secret key, public key, digital signature and hash function.

Digital Signature: The use of digital signature came from the need of ensuring the authentication. The digital signature is more like stamp or signature of the sender which is embedded together with the data and encrypts it with the private key in order to send it to the other party. In addition, the signature assures that any change made to the data that has been signed is easy to detect by the receiver.

Hash Function: The hash function is a one way encryption, the hash function is a well defined procedure or mathematical formula that represents a small size of bits which is generated from a large sized file, the result of this function can be called hash code or hashes. The generating of hash code is faster than other methods which make it more desired for authentication and integrity. Cryptographic hash functions are much used for digital signature and cheap constructions are highly desirable. The use of cryptographic hash functions for message authentication has become a standard approach in many applications, particularly internet security protocols. The authentication and the integrity considered as main issues in information security, the hash code can be attached to the original file then at any time the users are able to check the authentication and integrity after sending the secure data by applying the hash function to the message again and compare the result to the sender hash code, if it's similar that is mean the message came from the original sender without altering because if there is any changed has been made to the data will changed the hash code at the receiver side.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

3. Methodology for processing plain text

A block cipher processes the input one block of elements at a time, producing an output block for each input block. A stream cipher processes the input elements continuously, producing output one element at a time, as it goes along.

IV. Steganography

Steganography is the science of writing hidden messages to guarantee information which is accessible only by authorized parties. It is the practice of hiding information usually text messages, inside other files (host files). The practice of hiding information is called stego. Information can be hidden or embedded inside any type of multimedia files especially image files. The host files can then be exchanged over an insecure medium without anyone knowing what really lies inside them. Therefore, steganography in contrast with cryptography, where the existence of the message is clear, but the meaning is obscured. Steganography applications conceal information in other, seemingly innocent media. Steganographic results may masquerade as other file for data types, be concealed within various media, or even hidden in network traffic or disk space. Information hiding techniques provide an interesting challenge for digital forensic investigations. Information can easily traverse through firewalls undetected.

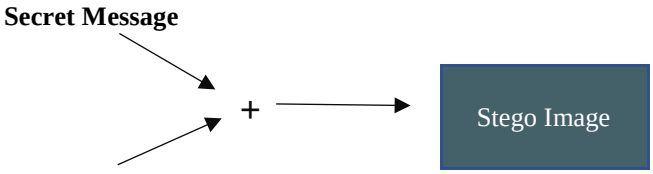

Fig. 2: Steganographic system

V. Encoding Secret Messages In Images

Coding secret messages in digital images is the most widely used of all methods in the digital world. This is because it can take advantage of the limited power of the human visual system (HVS). Almost any plain text, cipher text, image and any other media that can be encoded into a bit stream can be hidden in a digital image. With the continued growth of strong graphics power in computers and the research being put into image based Steganography, this field will continue to grow at a very rapid pace.

As Duncan Sellars explains:"To a computer, an image is an array of numbers that represent light intensities at various points, or pixels. These pixels make up the images raster data.". 24-bit image files are considered as carrier media candidates for hiding information in our proposed method of study. One of those methods is Least Significant Bit (LSB) Method. LSB insertion is an approach of embedding information in a cover image. The least significant bit of some or all bytes inside an image is changed to bits of the secret message. When using a 24-bit image, a bit of each of the red, green and blue color components can be used, since they are represented by a byte. In other words one can store 3 bits in each pixel. For example, a grid of 3 pixels of a 24-bit image is as follows:

(00101101 00011100 11011100) (10100110 11000100 00001100)
(11010010 10101101 01100011)

When the number 200, for which binary representation is 11001000, is embedded into the least significant bits of this part of this image, the resulting grid is as follows:

(00101101 00011101 11011100) (10100110 11000101 00001100)
(11010010 10101100 01100011)

Although the number was embedded into the first 8 bytes of the grid, only 3 underlined bits are changed according to the embedded message. On average, only half of the bits in an image will need to be modified to hide a secret message. Since there are 256 possible intensities of each primary color, changing the LSB of a pixel results in small changes in the intensity of the colors. These changes cannot be perceived by the human eye- thus the message is successfully hidden. With a well chosen image, one can even hide the message in the least as well as second to least significant bit and still not see the difference.

In the above example, consecutive bytes are used to embed the information. This approach is very easy to detect. A slightly more secure system is to share a secret key which specifies which pixels to be changed between sender and receiver. This process needs a secret key called the stego-key. This key is used to control the process such as the selection of pixels. The selected pixels will then be used to embed secret binary information.

VI. Public-Key Cryptosystem

During the early history of cryptography, two parties would rely upon a key using a secure, but noncryptographic, method; for example, a face-to-face meeting or an exchange via a trusted courier. This key, which both parties kept

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

absolutely secret, could then be used to exchange encrypted messages. A number of significant practical difficulties arise in this approach of distributing keys. Public-key cryptography addresses these drawbacks so that users can communicate securely over a public channel without having to agree upon a shared key beforehand. An asymmetric-key cryptosystem was published in 1976 by Whitfield Diffie and Martin Hellman, who, influenced by Ralph Merkle's work on public-key distribution, disclosed a method of public-key agreement. This method of key exchange, which uses exponentiation in a finite field, came to be known as Diffie–Hellman key exchange. The Diffie-Hellman key exchange protocol was the first system to utilize public-key or two-key cryptography. For this reason, it is sometime called as Asymmetric encryption. This was the first published practical method for establishing a shared secret-key over an authenticated (but not private) communications channel without using a prior shared secret.

Public-key Cryptography:

Public-key cryptography refers to a cryptographic system requiring two separate keys, one to lock or encrypt the plaintext, and one to unlock or decrypt the cipher-text. Neither key will do both functions.

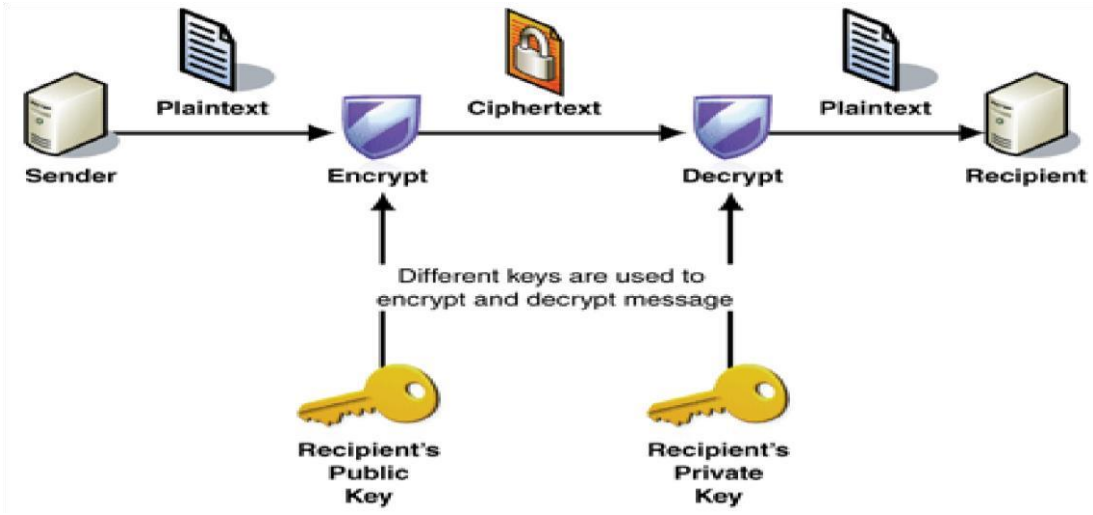

Fig. 3: Public key Cryptography

One of these keys is published or public and the other is kept private. If the lock/encryption key is the one published then the system enables private communication from the public to the unlocking key's owner. If the unlock/decryption key is the one published then the system serves as a signature verifier of documents locked by the owner of the private key. In the Diffie–Hellman key exchange scheme, each party generates a public/private key pair and distributes the public key. After obtaining an authentic copy of each other's public keys, SENDER and RECIPIENT can compute a shared secret offline.

An analogy that can be used to understand the advantages of an asymmetric system is to imagine two people, SENDER and RECIPIENT, sending a secret message through the public mail. In this example, SENDER wants to send a secret message to RECIPIENT, and expects a secret reply from RECIPIENT. With a Symmetric-key system, SENDER first puts the secret message in a box, and locks the box using a padlock to which he has a key. He then sends the box to RECIPIENT through regular mail. When RECIPIENT receives the box, he uses an identical copy of SENDER's key (which he has somehow obtained previously, maybe by a face-to-face me send his secret reply. In an Asymmetric-key system, RECIPIENT and SENDER have separate padlocks. First, SENDER asks RECIPIENT to send his open padlock to him through regular mail, keeping his key to himself. When SENDER receives it he uses it to lock a box containing his message, and sends the locked box to RECIPIENT. RECIPIENT can then unlock the box with his key and reads the message from SENDER. To reply, RECIPIENT must similarly get SENDER's open padlock to lock the box before sending it back to her. The critical advantage in an asymmetric key system is that RECIPIENT and SENDER never need to send a copy of their keys to each other. This prevents a third party (perhaps, in the example, a corrupt postal worker) from copying a key while it is in transit, allowing said third party to spy on all future messages sent between SENDER and RECIPIENT. So in the public key scenario, SENDER and RECIPIENT need not trust the postal service as much. In addition, if RECIPIENT was careless and allowed someone else to copy his key, SENDER's messages to RECIPIENT would be compromised, but SENDER's messages to other people would remain secret, since the other people would be providing different padlocks for SENDER to use. Public key exchange cryptosystem eliminates the key distribution problem by using two keys, a private and a public key. By exchanging the public keys, both parties can calculate a unique shared key, known only to both of them.

The Diffie-Hellman Algorithm for Key Exchange

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

SENDER must do the following:

1. Choose a prime numbers p randomly, and choose two integer numbers a and g.
2. Compute the A (SENDER's public key), as follows: $A = g^a \bmod p$.
3. Send the public value A to RECIPIENT.
4. Compute the secret value K, as follows: $K = B^a \bmod p$.

RECIPIENT must do the following:

1. Choose an integer numbers b randomly.
2. Compute the B (RECIPIENT's public-key), as follows: $B = g^b \bmod p$.
3. Send the public value B to SENDER.
4. Compute the secret value K, as follows: $K = A^b \bmod p$.

VII. Combined Crypto-Steganography

Steganography is not the same as cryptography Data hiding techniques have been widely used to transmission of hiding secret message for long time. Ensuring data security is a big challenge for computer users. Business men, professionals, and home users all have some important data that they want to secure from others. Even though both methods provide security, to add multiple layers of security it is always a good practice to use Cryptography and Steganography together. By combining, the data encryption can be done by a software and then embed the cipher text in an image or any other media with the help of stego key. The combination of these two methods will enhance the security of the data embedded. This combined chemistry will satisfy the requirements such as capacity, security and robustness for secure data transmission over an open channel. A pictorial representation of the combined concept of cryptography and steganography is depicted in figure 4.

In figure 4, both the methods are combined by encrypting message using cryptography and then hiding the encrypted message using steganography. The resulting stego-image can be transmitted without revealing that secret information is being exchanged. Furthermore, even if an attacker were to defeat the steganographic technique to detect the message from the stego-object, he would still require the cryptographic decoding key to decipher the encrypted message. Since then, the steganography approaches can be divided into three types.

Pure Steganography: This technique simply uses the steganography approach only without combining other methods. It is working on hiding information within cover carrier.

Secret Key steganography: The secret key steganography use the combination of the secret key cryptography technique encrypt the secret message or data by secret key approach and to hide the encrypted data within cover carrier. *Public Key Steganography*: The last type of steganography is to combine the public key cryptography approach and the steganography approach. The idea of this type is to encrypt the secret data using the public key approach and then hide the encrypted data within cover carrier.

VIII. Proposed Method

The proposed method describes two steps for hiding the secret information by using the public steganography based on matching method in different regions of an image.

- The First step is converting the Plain text message into cipher text using Public-key Encryption algorithm.
- The next step is to find the shared stego-key between the

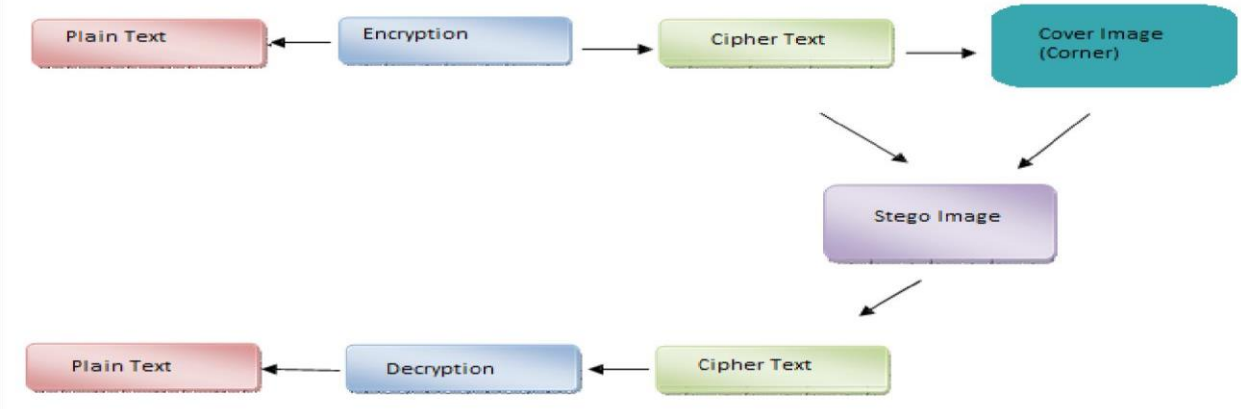

Fig. 4: Combination of Cryptography and Steganography

and the steganography approach. The idea of this type is to two communication parties (SENDER & RECIPIENT)

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

over insecure networks by applying Diffie-Hellman Key exchange protocol (as explained above). At the end the protocol, each side recovers his/her received public key to reach the shared values between them, that's mean SENDER & RECIPIENT have arrived same sego-key value.

- The next step in the proposed method is that the sender uses the secret stego-key to select pixels that it will be used to hide.

IX. Conclusion

Ensuring data security is a big challenge for computer users. Businessmen, professionals, and home users all have some important data that they want to secure from others. Even though both methods provide security, to add multiple layers of security it is always a good practice to use Cryptography and Steganography together. The present study is designed to combine the features of both cryptography and steganography, which will provide a higher level of security. It is better than the technique used separately. Simple LSB method was used to embed the secret message into the image. The LSB in each selected pixel can be used to conceal the message binary code. It is also found that combination of cryptography and steganography enhance the security and reliability of message as first message is encrypted and using steganography hide it to other carrier like digital image, video file or any other.

References

[1] Bharti,P.,and Soni, R.,A New Approach of Data Hiding in Images using Cryptography and Steganography,*International Journalof Computer Applications*,Vol.58,*No.*18,2012,pp1-5.

[2] Dipti Kapoor Sarmah, Neha bajpai, " Proposed System for Data Hiding Using Cryptography and Steganography", International Journal of Computer Applications (0975 – 8887), Volume 8 – No. 9, October 2010 .

[3] Domenico Bloisi and Luca Iocchi, "Image Based Steganography and Cryptography", Sapienza University of Rome, Italy.

[4] Johnson, N.F. & Jajodia, S., "Exploring Steganography: Seeing the Unseen", *Computer Journal*, February 1998 .

[5] Kallam Ravindra Babu, Dr. S.Udaya Kumar, Dr. A.Vinaya Babu, "A Survey on Cryptography and Steganography Methods for Information Security", Internaltional Journal of Computer Applications(0975-8887), Volume 12 – No. 2, November 2010.

[6] Manoj, I. V. S., Cryptography andSteganography. *International Journal of Computer Applications* (0975–8887), Vol.1, No.12, 2010,pp 63-68 .

[7] Rajyaguru, M. H., Combination of Cryptography and Steganography With Rapidly Changing Keys,*International Journal of Emerging Technology and Advanced Engineering*, Vol.2, No.10, 2012 .