Information Transmission in Crime Branch using Steganography

K. Manoj Kumar, R. Muthuvel
Department of Computer Science and Engineering. Sri Vidya College of Engineering & Technology. Virudhunagar;

S. Guru Ragavendran
Assistant Professor of Department of Computer Science and Engineering
Sri Vidya College of Engineering & Technology. Virudhunagar

Abstract:- To provide the security for the information transmit over the internet between one crime branch to the another using Steganography using.Steganography is the term used for hiding secret messages within an image. Any color pixel is made of a combination of RED-GREEN-BLUE (RGB) wherein each RGB components consists of 8 bits. If the letters in ASCII are to be represented within the color pixels, the rightmost digit, called the Least Significant Bit (LSB), can be altered. Any variation in the value of this bit leads to minimal variation in color.This project contains DOUBLE SECURITY where TWO LEVEL AUTHENTICATION is required- the ENCRYPTION KEY and VALIDATION CODE. If you have lost the Encryption Key or Validation code then users can refer HISTORY DATABASE- where the encryption key and the validation code is recorded. This code uses SAFE HIDING where no modification is done the source image. After hiding secret messages you can also Test the Images to verify that the image is corrupt or not.

Keywords—Least Significant Bit (LSB),, steganography, encryption key, validation code

INTRODUCTION

Steganography is the art of passing information through original files in a manner that the existence of the message is unknown. The term steganography is arrived from Greek word means, “Covered Writing”. The innocent files can be referred to as cover text, cover image, or cover audio as appropriate. After embedding the secret message it is referred to as stego-medium. A stego-key is used to control the hiding process so as to restrict detection and/or recovery of the embedded data. While cryptography is about protecting the content of messages (their meaning), steganography is about hiding the message so that intermediate persons cannot see the message. Steganography refers to information or a file that has been concealed inside a digital Picture, Video or Audio file. Images can be more than what we see with our Human Visual System (HVS); hence, they can convey more than merely 1000 words.

RELATED WORKS

Dipti, K. S.etal Steganography and Cryptography are two popular ways of sending vital information in a secret way. One hides the existence of the message and the other distorts the message itself. There are many cryptography techniques available; among them AES is one of the most powerful techniques. In Steganography we have various techniques in different domains like spatial domain, frequency domain etc. to hide the message. It is very difficult to detect hidden message in frequency domain and for this domain we use various transformations like DCT, FFT and Wavelets etc. In this project we are developing a system where we develop a new technique in which Cryptography and Steganography are used as integrated part along with newly developed enhanced security module. In Cryptography we are using AES algorithm to encrypt a message and a part of the message is hidden in DCT of an image; remaining part of the message is used to generate two secret keys which make this system highly secured.

Jayaram, P. et al Increase in the number of attack recorded during electronic exchange of information between the source and intended destination has indeed called for a more robust method for securing data transfer. Cryptography and steganography are well known and widely used techniques that manipulate information in order to cipher or hide their existence. These two techniques share the common goals and services of protecting the confidentiality, integrity and availability of information from unauthorized access. In this paper, a data hiding system that is based on audio steganography and cryptography is proposed to secure data transfer between the source and destination. Audio medium is used for the steganography and a LSB (Least Significant Bit) algorithm is employed to encode the message inside the audio file.

Niels, P. et al Although people have hidden secrets in plain sight-now called steganography- throughout the ages, the recent growth in computational power and technology has propelled it to the forefront of today's security techniques. Essentially, the information-hiding process in a steganographic system starts by identifying a cover medium's redundant bits (those that can be modified without destroying that medium's integrity). The embedding process creates a stego medium by replacing these redundant bits with data from the hidden message. This article discusses existing steganographic systems and presents recent research in detecting them via statistical steganalysis. Here, we present recent research and discuss the practical application of detection algorithms and the mechanisms for getting around them.

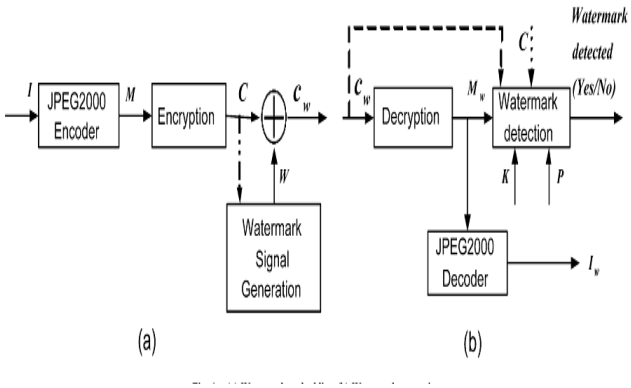
Raphael, A. J. et al Digital communication has become an essential part of infrastructure nowadays, a lot of

applications are Internet based and it is important that communication be made secret. As a result, the security of information passed over an open channel has become a fundamental issue and therefore, the confidentiality and data integrity are required to protect against unauthorized access and use. This has resulted in an unstable growth in the field of information hiding. Cryptography and steganography are the two popular methods available to provide 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 an image file and the image file is transmitted. This paper focuses on the strength of combining cryptography and stegnography methods to enhance the security of communication over an open channel

Domenico, B. et al In this paper we describe a method for integrating together cryptography and teganography through image processing. In particular, we present a system able to perform steganography and cryptography at the same time using images as cover objects for steganography and as keys for cryptography. We will show such system is an effective steganographic one (making a comparison with the well known F5 algorithm) and is also a theoretically unbreakable cryptographic one (demonstrating its equivalence to the Vernam Cipher)

Sujay, N. et al The science of securing a data by encryption is Cryptography whereas the method of hiding secret messages in other messages is Steganography, so that the secret's very existence is concealed. The term 'Steganography' describes the method of hiding cognitive content in another medium to avoid detection by the intruders. This paper introduces two new methods wherein cryptography and steganography are combined to encrypt the data as well as to hide the encrypted data in another medium so the fact that a message being sent is concealed. One of the methods shows how to secure the image by converting it into cipher text by S-DES algorithm using a secret key and conceal this text in another image by steganographic method. Another method shows a new way of hiding an image in another image by encrypting the image directly by S-DES algorithm using a key image and the data obtained is concealed in another image. The proposed method prevents the possibilities of steganalysis also.

METHODOLOGIES



- User details
- Branch Creation
- User Creation.
- User Configuration
- Sender side
- Receiving Side

the Steganography is a secret way to hides the message itself. In steganography, the data is embedded in an image file and the image file is transmitted. message and the other distorts the message itself. In Steganography we have various techniques in different domains like spatial domain, frequency domain etc. to hide the message. It is very difficult to detect hidden message in frequency domain and for this domain we use various transformations. In this project we are developing a system where we develop a new technique in which Steganography is used as integrated part along with newly developed enhanced security module.

A data hiding system that is based on image steganography is proposed to secure data transfer between the source and destination. Image medium is used for the steganography and a LSB (Least Significant Bit) algorithm is employed to encode the message inside the image file.

The information-hiding process in a steganographic system starts by identifying a cover medium's redundant bits. The embedding process creates a stego medium by replacing these redundant bits with data from the hidden message. This article discusses existing steganographic systems and presents recent research in detecting them via statistical steganalysis. Here, we present recent research and discuss the practical application of detection algorithms and the mechanisms for getting around them.

Digital communication has become an essential part of infrastructure nowadays.As a result, the security of information passed over an open channel has become a fundamental issue and therefore. This has resulted in an unstable growth in the field of information hiding. One hides the existence of the message and the other distorts the The term 'Steganography' describes the method of hiding cognitive content in another medium to avoid detection by the intruders. This paper introduces

steganography are combined to encrypt the data as well as to hide the encrypted data in another medium so the fact that a message being sent is concealed. One of the methods shows how to secure the image by converting it into cipher text by S-DES algorithm using a secret key and conceal this text Steganography is a branch of information hiding. It allows the people to communicate secretly. As increasingly more material becomes available electronically, the influence of steganography on our lives will continue to grow. Many confidential information were leaked to a rival firm using steganographic tools that hid the information in music and picture files.

Steganography has long been regarded as a tool used for illicit and destructive purposes such as crime and warfare. Currently, digital tools are widely available to ordinary computer users also. Steganography software allows both illicit and legitimate users to hide messages so that they will not be detected in transit.

In the present situation, to shield mystery message from being stolen amid transmission, there Steganalysis technique for the detection of secret message in the image. The strong and weak point of this technique is mentioned briefly. Steganography function is used to hide a secret message in any media such as text, image, audio and video. There are many algorithms used for hiding the information. One of the simplest and best known techniques is Least Significant Bit (LSB). This paper focuses on image Steganography and hiding the message in the Least Significant Bit (LSB) method. We also discuss the LSB method used for various file formats. The challenge of steganographic methods is to create a rational balance between the quality of the file and the size of data that can be transferred. In addition, the robustness of the technique and security of the obscure data are the facts that cannot be dissembled. The Least Significant Bit (LSB) insertion approach provides a high degree of visual quality and a large amount of capacity for the concealed data, but the covert message is not well protected in this method. In the proposed method, the secret data is firstly encoded by using the Vigenere encryption method to guarantee the protection of the hidden message An architecture description is a formal description of a system, organized in a way that supports reasoning about the structural properties of the system. It defines the system components or building blocks and provides a plan from which products can be procured, and systems developed , that will work together to implement the overall system.

User details:

This module lists all the available users in the crime branch.

Branch Creation:

It gives branch information of various applications and it is identified by unique branch id.

User Creation:

In User Creation module, user has registered himself by supplying his personal information, which gets store in database, which are using as Backend. By registering himself user will get his login id and Password.

User Configuration:

This module gives rights to send and receive message between the crime branches will be made by others such as constable or some of the genuine persons. This permission is allotted by the person those who are in higher positions such as Inspector, Sub Inspector, and Inspector general.

Sender side:

a. Encrypted Domain Watermarking and Watermarking Retrieval

In this module, in an encrypted piece of content, changing even a single bit may lead to a random decryption. Therefore the encryption should be such that the distortion due to embedding can be controlled to maintain the image quality. It should also be possible to detect the watermark correctly even after the content is decrypted. Also, the compression gain should not be lost as encryption may lead to cipher text expansion.

b. Embedding the encrypted watermark information in the image:

Rather represent the secret message as an integer directly, we generate encrypt the secret message with a conventional, much faster symmetrical algorithm like LSB algorithm. This is not change the actual image and no variations in the image and thus the actual text is hide in the image.

c. Sending the image:

This Encrypted message is send with a random key (ie) valuation code and with password to the sender. This valuation code and password is for security purpose.

Receiving Side:

a.Extracting the information from watermark:

The sender A then transmits a message to the recipient B in a encrypted format. The recipient B would extract the encrypted data and use the valuation code and its password to decrypt it.

b. Decrypting the information using key:

He would then use this valuation code and password with a LSB algorithm to decrypt the actual message. Typically the transmission would include in secret message details of the encryption algorithms used. These key values are used to decrypt the actual message from the image

RESULT AND CONCLUSION:

Here, I kindly convey that special feature of this software is the geniality and it can be worded on the personal computer, since the web page gives a variety option and the message gives clear understanding of the next page it is easy to follow and use.We are sure that this

software will be useful for all Crime Branch office. To use this software, there is no need of knowledge of the computer operating method because, to enter into the menu just enter into windows and type the particular directory, in which the project is stored. From the prompt, just enter the project name this will enter into the home page. From this 'Home Page' We can do our specified job mentioned early.At last I say that this software is less Expensive and more friendly

REFERENCES:

[1] S. Agrawal, S. Chaudhuri, and G. Das. Dbxplorer: A system for keyword-based search over relational databases. In Proc. of International Conference on Data Engineering (ICDE), pages 5–16, 2002.

[2] N. Beckmann, H. Kriegel, R. Schneider, and B. Seeger. The R*-tree: An efficient and robust access method for points and rectangles. In Proc. of ACM Management of Data (SIGMOD), pages 322–331, 1990.

[3] G. Bhalotia, A. Hulgeri, C. Nakhe, S. Chakrabarti, and S. Sudarshan. Keyword searching and browsing in databases using banks. In Proc. Of International Conference on Data Engineering (ICDE), pages 431– 440, 2002.

[4] X. Cao, L. Chen, G. Cong, C. S. Jensen, Q. Qu, A. Skovsgaard, D. Wu, and M. L. Yiu. Spatial keyword querying. In ER, pages 16–29, 2012.

[5] X. Cao, G. Cong, and C. S. Jensen. Retrieving top-k prestige-based relevant spatial web objects. PVLDB, 3(1):373–384, 2010.

[6] X. Cao, G. Cong, C. S. Jensen, and B. C. Ooi. Collective spatial keyword querying. In Proc. of ACM Management of Data (SIGMOD), pages 373–384, 2011.