Review Paper of Secure Data Transmission for Application of Covered Communication

Anjali Ahuja¹ and Kavita²

¹M. Tech. Scholar, Shri Baba Mastnath Engineering College, Rohtak (Haryana)  
anjaliahuja125@gmail.com

²Assistant Professor, Shri Baba Mastnath Engineering College, Rohtak (Haryana)  
kavita.kathuria1990@gmail.com

Abstract

With the evolution and huge increase in the computer networks, large amount of data is shared through internet. So the main issue of concern is the security of data that is transmitted over internet. Any person can hack or intercept the data in-between rather than sender and intended recipient. Thus in order to maintain the geniality of original message various secure data transmission schemes are available. However our main problem is to design a secure data transmission method that can provide and maintain the originality of message so that message is accessible to sender and intended recipient and not to any third party. In this proposed this problem of secure data transmission has been reviewed and worked upon. Although there are various cryptographic and steganographic algorithms have been proposed till now but they all have certain limitations regarding to provide the complete or nearly complete security to data. Thus my work is emphasis on the development of the solution towards security problem by some techniques.

Keywords: Security, Stegnography, Cryptography, Transmission Security.

1. Introduction

Transmission security is the capability to send a message electronically from one computer system to another computer system so that only the intended recipient receives and reads the message and the message received is identical to the message sent. The message would not be identical if it was altered in anyway, whether transmitted over faulty channels or intercepted by an eavesdropper. Transmission security translates into secure networks. Although many people regard networks as computers connected by wires, this definition of a network, while technically correct, misses the point. Rather, networks are transmitted data, the data flowing over wires. All transmissions can be intercepted. And the cautious user looks at all transmissions as if they will be intercepted.

A steganographic message (the plaintext) is often first encrypted by some traditional means, producing a cipher text. Then, a cover text is modified in some way to contain the cipher text, resulting in stegotext. For example, the letter size, spacing, typeface, or other characteristics of a cover text can be manipulated to carry the hidden message; only the recipient (who must know the technique used) can recover the message and then decrypt it.

Any person watching the communication should not be able to decide whether the sender is sending covers with messages embedded into them. In other words, a person with a number of cover objects C1, C2 , ……, Cn should not be able to tell which cover object Ci has the message embedded in it, and the security of invisible communication lies in the inability to distinguish cover objects from the stego objects. However, not all the cover objects can be used to hide the data for covert communication, since the modifications done after the data is hidden should not be visible to anyone not involved in the communication. The cover object needs to have sufficient redundant data, which can be replaced by secret information.

Steganography is the art of hiding signals inside other signals. This basically comes down to using unnecessary bits in an innocent file to store your sensitive data. The techniques used make it impossible to detect that there is anything inside the innocent file, but the intended recipient can obtain the hidden data. This way, you not only hide the message itself, but also the fact that you are sending this message.
2. Literature Review

Besides cryptography, steganography can be employed to secure information. Steganography is a technique of hiding information in digital media. Cryptography and steganography techniques of digital images are widely used to prevent and frustrate opponents' attacks from unauthorized access. Thus, reliable image encryption techniques are of utmost importance for the protection of data from counterfeiting, tampering, and unauthorized access. While cryptography and steganography are related, there is a difference between the two.

Cryptography is used to scramble messages so that they cannot be understood. It does not hide the fact that the message exists. On the other hand, steganography conceals the fact that the message exists by hiding the actual message in another. There are many different steganographic methods that have been proposed over the last few years. Most of them are simple techniques that can be broken by careful analysis of statistical properties of the channel’s noise. Recently, several steganographic algorithms for two-color binary images have been proposed. Example of steganography can be found in invisible inks, microdots, character arrangement, digital signatures, covert channels, and spread spectrum communications.

Johnson and Sushil explain steganography and provide a brief history, describe how steganography is applied in hiding information in images, and survey a few steganography software applications for processing images.

Tsung-Yuan and Wen-Hsiang proposed a new steganographic method for data hiding in Microsoft Word documents by a change tracking technique. Sinha and Singh proposed a technique to encrypt an image for secure transmission using the digital signature of the image. Digital signatures enable the recipient of a message to authenticate the sender of a message and verify that the message is intact.

Kisik et al. proposed a steganographic algorithm which embeds a secret message into bitmap images and palette-based images; the proposed algorithm divides a bitmap image into bit-plane images from LSB-plane to MSB-plane for each pixel, and considers each bit-plane image as a binary one. The description of the proposed algorithms are presented below, the first one will be used to generate a mixed data before transmission to the receiver, and the second will be conducted by the receiver to extract the secret information from the encrypted image before decryption take place and thus obtaining the original image. Steganography needs to achieve large capacity, high security level, and high imperceptibility, but does not have to be robust against cover modifications. While digital watermarking has relatively low requirements on imperceptibility, security and capacity, it must be robust against both accidental faults (e.g. noise) and malicious faults (e.g. attacks like clipping, scaling of the cover). Steganography is sometimes referred to as covert communication. A typical application example is to transfer secret messages embedded in images using a public website. Although the images are accessible to all users, only those with the secret key(s) can view the hidden information.

The area of steganography has a long history. It can be traced back to techniques like invisible ink and microdots used by spies. Common approaches to hide information in digital images include least significant bit insertion (LSB), masking (in a manner similar to paper watermarks), and information hiding in transformations (DCT, FFT, WT, etc.). While they all have different advantages for specific applications, they also suffer a similar problem: such systems are unable to deal with subterfuge attacks (collusion and forgery), that is, they cannot deal with the opponents who not only detect a message, but also render it useless, or even worse, modify it to the opponent’s favor. Recent suggestions in US newspapers indicate that terrorists use steganography to communicate in secret with their accomplices. In particular, images on the Internet were mentioned as the communication medium.

It has been suggested in the past that secure message hiding in palette-based images can be obtained by permuting the image palette rather than changing the colors in the image. While this method does not change the appearance of the image, which is certainly an advantage, its security is questionable because many image processing software products order the palette according to luminance, frequency of occurrence, or some other scalar factor. A randomized palette will raise suspicion. Also, displaying the image and resaving it may erase the information because the software routine may rewrite (and reorder) the palette.

3. Objective

The objective of this research is to develop and implement an algorithm that uses the combination of encryption and covert communication to secure transmission of data over internet. Thus here we aim to combine two security approaches collectively encryption and covert communication. However compression can be applied also for long messages transmission. Our main objective of this thesis is to develop an algorithm and
hence technique that combine the security methods in a single unit. The following objectives are the description of the parts of the steganography process; the Secret key, the encrypted image represents the transformed image after encryption and the numbers of horizontal and vertical blocks represent the hidden information. The result is the mixed data; encrypted image that includes the mixing data.

4. Conclusion

Due to the inability of various techniques to provide partial to full security to data over internet attacks and threats increase to data. Neither alone any cryptographic technique nor steganographic technique can provide security to such extent. Combination of these two approaches leads to the dual layered security to data to be transmitted over internet. However the measurement of effective steganographic algorithm depends on the embedding efficiency which is proportional to the amount of distortion in the cover image. An intermediate compression process can be added for large text and images so that the data can be compressed to make effective and faster transmission.

The time taken by algorithm for completion depends upon the size of the image chosen as the cover image and thus generation of blocks and scanning of blocks occur according to size of image. Also the efficiency of procedure depends upon the color intensity of image. More different colors in image posses the more variations and thus more number of pixels that are surrounded by different color pixels. It leads to the hiding of data more efficient and unpredictable.

5. Future Scope

Further work that can be done in this field is to reduce the time taken to scan the whole image so as the faster system can be developed. Although its impossible to design any steganographic system with relative entropy perfectly zero as relative entropy is not symmetric and not follow the triangle inequality, work can be done to generate a system that is secure as its entropy tends more towards zero range.

References