Chapter 21
Improved Secure Data Transfer Using Video Steganographic Technique

V. Lokeswara Reddy
K.S.R.M College of Engineering, India

ABSTRACT

Information security using data hiding in video provides high embedding capacity and security. Steganography is one of the oldest data protecting methodologies deals with the embedding of data. Video Steganography hides secret information file within a video. Present day communications are treated to be "un-trusted" in terms of security, i.e. they are relatively easy to be hacked. The proposed technique is invented to hide secret information into a video file keeping two considerations in mind which are size and security of the cover video file. At the sender side, the secret information which is to be hidden is encoded into cover video file. Double layered security for the secret data can be achieved by encrypting confidential information and by embedding confidential information into cover video file frames using encrypted embedding technique.

1. INTRODUCTION

1.1. Overview of Steganography

The aim of digital Steganography is to modify a digital medium (cover) to encode and conceal a sequence of bits (Secret data) to facilitate covert communication. In the traditional architecture there existed only the client and the server. In most cases the server was only a data base server that can only offer data. Therefore, majority of the business logic, i.e., validations, etc., had to be placed on the clients' system. This makes maintenance expensive. Such clients are called as 'fat clients'. This also means that every client has to be trained as to how to use the application and even the security in the communication is also the factor to be considered. Since the actual processing of the information takes place on the remote client the information has to be carried over the network, which requires a secured format of

DOI: 10.4018/978-1-7998-1763-5.ch021

the transfer method. A Steganography system, in general, is expected to meet three key requirements, namely, imperceptibility of hiding data, accurate recovery of hidden secret data, and huge payload. In a pure Steganography framework, the technique of encoding confidential data should be unidentified to anyone other than the receiver and the sender. An effective Steganography should possess the following characteristics (Suneetha, Hima Bindu, Sarath Chandra, 2013): Secrecy: Extraction of embedded secret data from the host medium should not be possible without the knowledge of the proper secret key used at the extracting. Imperceptibility: After hiding the confidential data in the cover file, it should be imperceptible from the original file. High capacity: The maximum size of the embedded secret information that can be hidden can be as long as possible. Resistance: The embedded secret information should be able to survive when the host medium has been manipulated. Accurate extraction: The extraction of the embedded secret data from the medium should be reliable and accurate. This paper explains a way in which so that a video file is used as a host medium to embed secret information without changing the file structure and content of the video file. Because degradation in the quality of the cover medium leads to noticeable change in the cover medium which may leads to the failure of objective of Steganography. The contents are processed during video embedding and de-embedding. This makes less vulnerable to video steg analysis methods. A single bit is embedded in the least significant bit of each motion vector.

In this digital world the information security and secret data communication is changing and advancing day by day. Broad band internet connections almost an errorless data transmission, which helps people to distribute large multimedia files and makes identical data copies of them. Sending secret information and secret files over the internet are carried in an unsecured form but everyone has got something to keep in secret. The aim of Steganography is to embed the secret information inside the cover file without changing the overall quality of cover file. In Steganography actual confidential data is not maintained in its original format but it is transformed in such a way that it can be embedded inside multimedia cover file e.g. image, video, audio. The current industries mainly demand for finger printing and digital watermarking of image, audio and video Steganography. The music and movie industries are continually searching for new methods for Steganography. In "broadcast monitoring" broadcast detectors are used to retrieve the watermark of a given file and report to the broadcasting events to notify the owner or distributor of broadcast status (medium played, time and date). Since internet is now the major medium for the communication and data transfer purpose it become necessary for each nation to make some counter measures to prevent the foul use of internet (Sunil Moon, Rajesree Raut, 2014). The cybercrimes are also informing immediately nowadays hence the steganographic methods should be that much effective and secure so that crimes can be minimized for that cryptography should be mixed with Steganography for the confidentiality of the secret data. Information Hiding is the process of embedding secret information into a host medium. In general, visual media is preferred due to their wide presence and the tolerance of human perceptual systems involved. For instance, audio/video data embedding share many common points; however, video data hiding demands more complex designs as a result of the additional temporal dimension. Therefore, video secret information embedding continues to constitute an active research area. LSB audio Steganography with location identification and it provides good audio quality and robustness (Pathak, Nag, 2014). Steganography helps not only to keep others from understanding that the secret data exists but also to bypass drawing suspicion to hide the information (Johnson, and Jajodia, Sushil, 1998 & Provos. and Honeyman, 2001). The rest of the paper is organized as follows: in Section 1 we overview the literature survey of Steganography and its methods. The proposed method and algorithm is given in Section 2 followed by the experimental results and analysis in Sections 3 and 4. Finally, the paper is concluded in Section 5.