Two Tier Shield Unapparent Information Deliver along with the Visual Streams

Eranga, D.M.S. and Weerasinghe, K.G.H.D.

Department of Computer Systems Engineering, University of Kelaniya, Sri Lanka

Email: sachitheranga.1990@gmail.com, hesiri@kln.ac.lk

Abstract

Information put out of sight for various security purposes have become highly exciting topic in the industry and also academic areas. Encryption provides the ability of data hiding. With the development of the technology, people tend to figure out a technique which is not only capable in hiding a message, but also capable in hiding the actuality of the message. Steganography was introduces as a result of those researches. The current study is conducted in order to hide a file inside a video file. Generally, steganography benefits do not use in the industry or students even though it is widely discussing topic in modern information world. The major aim of this research is the ability to hide any type of file in a video file and retrieve hidden information. There are few algorithms/systems developed to embed a file into video files. It is a great challenge to extract secret information directly from the video, which is embedded already. The existing applications require a considerable time to embed a small message and some are not freeware. Focuses areas of the research are confidentiality, authentication, increase hidden data size, integrity, assure unapparent perceptual transparency of video file (cover object) and send/receive video files. Video consists of frames called I, P and B frames. Each frame uses LSB technique to hide information. This original message can be any kind of file type and almost all popular video file formats for carrier. Identifies the type of the message and encrypts the message file using AES256 with given key. Encrypted message size stores in four bytes and type of the message file stores in another four bytes. Propose algorithm decides the number of frames require to hide the secret information according to size of both carrier video and the secret message. Firstly, reads the video header to retrieve important information and skip the header. Video file Splits in to bitmap images with having pre-defined frame gap between two images, corresponding to the secret message size. Every bitmap image consists of red, green and blue colors and bitmap image pixel has 8 bit for each color and total of 24 bits called bit depth. Writes message size followed by the message type in the bitmap images. Then, writes the message. Each encoded image adds into the original video file. In the process of retrieval, skips the header frames and fetches the images from the video according to the pre-defined gap between images. Reads first eight bytes to identify the message size and type of the message respectively. Then, decodes the encrypted message and decrypts the message with same secret key, which used to encrypt the message. Carrier video file can be watched during the both process of encode and decode. This method doesn't increase the size of the carrier, though the existence of the message cannot be detected. AES256 key size encryption supports the dual layer security of classified information. Proposed solution supports unique feature that can delete the hidden

information, which concealed inside the video without affecting the video carrier. Encoded video is guaranteed the original quality of the carrier. So, this proposed way-out emerges along with an application called SilentVideo1.0. The system was tested to assure the quality of the final product. Testing focused on the accuracy of the propose algorithm, which is ability of hiding the existence of the information as well as the ability of retrieving the information correctly using the application. Test results guarantee the success rate of the proposed algorithm goes up to 85 percent. Furthermore, the application was evaluated for exactness of the input and output information by black box tests using 200 samples from different video formats. The aim of this work was propose a strong resolution for steganography in digital media with multi-tier protection. The hidden file capacity will be increased using sound track of the video file as well. Upcoming versions of the system will be upgraded with latest cryptographic involvement and increase the conceal message capacity along with the lowest encoding and decoding time frame.

Keywords: *Steganography, AES, Bitmap, Encode, Decode*