Design and Implementation of Steganographic Engine for Authentication of Videos and Secret Data Sharing: An Overture

The field of Information hiding is a recently rapidly developed technique in the field of information security and has received significant attention from both industry and academia [1] [2]. This hiding of information also means communication of information in numerous forms and is used in many applications. In a large number of these applications, it is desired that the communication to be done in secrete. Such secrete communication ranges from the obvious cases of bank transfers, corporate communications and credit card purchases, on down to a large percentage of everyday email.

Information hiding consists of two main branches: digital watermarking and steganography. Where the former is mainly concerned with for copyright protection of electronic products. While steganography, is supposed to be a new way of covert communication, the main purpose is to convey data secretly by concealing the very existence of communication. The carrier for steganography ranges from image files (JPEG, GIF, BMP), audio files (WAV, MP3) or video files (MPEG, AVI). Though image is supposed to be the most familiar carrier, but size of the carrier (image) inevitably restricts the capacity of embedding. So for transmitting large number of secret messages, video steganography is and effective alternative. Thus using the Internet, secret information hidden in the carrier can be transmitted quickly, secretly, and securely. Another paradigm is authentication of videos for Intellectual Property Rights. This helps the publishers and broadcasting industries for hiding encrypted copyright marks and serial numbers in digital films and multimedia products. Literature survey reveals that some work done in both spatial and transform domain. Varying from the least significant bit (LSB) approach [3] to a secure self-embedding technique based on spatio-temporal approach [4] and lossless steganography on AVI file using Swapping algorithm [5] to name a few. Whereas in transform domain a series of changes are done to the cover image before hiding information. To select the best areas the Discrete Cosine Transform DCT, Wavelet Transform, etc. are used.

Before going into the details of the scope of the proposed work, it is worth a while to discuss the intricacies related to *Video*. A *video* is said to be consisting of sequence of still images (also called as *frames*). These digital videos are nowadays widely available due to the advances in increasingly cheaper yet powerful computer facilities and broadband Internet technologies. This makes streaming of high-quality videos on the Internet very easy and there are several websites such as YouTube, Yahoo! Video, DailyMotion, etc. offer free video viewing and sharing services. Also with the rapid development in the field of portable devices watching videos anytime and anywhere has become peoples most popular daily activity. Thus, digital videos are ubiquitous and are the major circulated multimedia content nowadays. But these digital videos needs to go though compression before transmission. Since human vision systems perception towards models are not perfect, lossy compression is usually preferred to increase the coding efficiency of digital videos without affecting the humans perception. Thus *Video coding* or compression is done to remove redundancy in a video. The simplest way can be said as compressing each frame individually. Wheras predictive technique temporally predicts the current frame from the previous one(s) that must be stored. The temporal prediction assumes that the consecutive frames in a video sequences exhibit very close similarity, except for the fact that the objects or the parts of a frame in general may get somewhat displaced in position. The predicted frame generated by the exploitation of temporal redundancy is subtracted from the incoming video frame, pixel by pixel and the difference is the error image, which will in general exhibit considerable spatial redundancy. The error image goes through transform which can be DCT for MPEG-1, MPEG-2 and ITU-T standard H 261, H 263 etc. The latest ITU-T standard H 264 uses an integer-DCT and MPEG-4 supports wavelet transforms. The transformed coefficients are then quantized and entropy coded before adding to the bit stream. The encoder also has a built in decoder to reconstruct the error frame, which will not be exact, because of the quantizer. The error frame is added to the predicted frame to generate the buffer. The motion estimation block determines the displacement between the current frame and the stored frame. The displacements so computed are applied on the stored frame in the motion compensation unit to generate the predicted frame. There are several standards for video coding viz.

1. ITU standards such as, H.261 for ISDN video conferencing, H.263 for very low bit-rate and Plain Old Telephone Systems (POTS) video conferencing and the latest H.264 for video telephony and video streaming in wireless applications. H.264/Advanced Video Coding (AVC) is the state-of-the-art video codec and its decent coding performance lends itself to become the major coding mechanism in various applications

2. ISO MPEG-1, for storing movies on CD-ROM.

3. ISO-MPEG-2 for broadcast and storing video on digital video disks (DVD). This standard is also addressed as High Definition Television

(HDTV) applications.

4. MPEG-7 standard for multimedia meta-data

Many popular digital video formats/containers exist such as FLV (Flash Video), MKV (Matroska Multimedia Container), AVI (Audio Video Interleave) and MP4, etc., Presence of certain amount of redundancy in these digital video files can serve as an invisible channel from the viewpoint of communication. One can make good use of it and embed high volume messages with the digital videos as the camouflage. Steganography in video although in the same lines as image, however is quite different the first important difference is the size of the host media. Since videos contain many frames so more sample pixels or the number of transform domain coefficients, a video has higher capacity than a still image and more data can be embedded in the video. Also, the perceptual redundancy in videos can be utilized to embed messages efficiently without much harm to originality as far as human vision system is concerned. Also Steganography in video has to be considered in terms two major conceptual aspects, one is embedding data in uncompressed raw video, which is compressed afterwards. The other and the more difficult one, tries to embed data directly in compressed video stream. The problem of the former is how to make the embedded message resist video compression another point of relevance is that the video basically exists in a compressed way. For evaluating the performance of any steganographic system two important factors are considered capacity and imperceptibility. Capacity refers to the amount of data that can be hidden in the cover medium so that no perceptible distortion is introduced. Imperceptibility or transparency represents the invisibility of the hidden data in the cover media without degrading the perceptual quality by data embedding. Security is also considered to be an important parameter in the steganographic systems, which refers to an unauthorized persons inability to detect hidden data.An effort is being made to design Steganographic Engine which can work in synergism with all the above issues, thus developing a robust and failsafe system.

This work plan is aimed at designing and implementation of Steganographic Engine for Authentication of Video and sharing of secret message. The problem is to be addressed in both spatial and frequency domain. In spatial domain data will be embedded directly in the frames by using hash function for efficient and more secured Stego. A complete framework is being designed for the Steganographic Engine. The main aspect of this effort lies in utilizing the inherent redundancy of video keeping the quality aspect in consideration. Evolution of newer and novel *soft computing* approaches are also on the fray for deriving more space- and time-efficient methodologies. Where as in frequency approaches like DCT and wavelets is being used for more effective embedding. The work plan is invested to bring about a paradigm shift in Video Steganography by introducing new approaches for Streaming video and Video conferencing which is need of the hour.

Working on the work plan some techniques have already been devised
Following the work plan some more techniques will be incorporated pertaining to the problem for Mobile and wireless communication.

References

1. Eric Cole, *Hiding in Plain Sight: Steganography and the Art of Covert Communication*, Willey Publishing Inc.

2. Stefan Katzenbeisser and Fabien A. P. Petitcolas, *Information Hiding Techniques for Steganography and Digital Watermarking*, Artech House.

3. Mritha Ramalingam, *Stego Machine Video Steganography using Modified LSB Algorithm*, in World Academy of Science, Engineering and Technology 74, pp. 502-505, 2011.

4. Pratheepan. Y, Joan V. Condell, Kevin Curran, Paul Mc Kevit and Abbas Cheddad, *Video Authentication: A Self Embedding Steganography approach.*

5. R.Kavitha and A. Murugan, *Lossless Steganography on AVI File using Swapping Algorithm*, in International Conference on Computational Intelligence and Multimedia Applications, pp. 83–88, 2007.

[Kousik Dasgupta]

Supervisors

[Jyotsna Kumar Mondal]
Internal

[Paramartha Dutta]
External