ABSTRACT

This thesis is concerned with secure video transmission over open and wireless network channels. This would facilitate adequate interaction in computational constrained applications among trusted entities such as in disaster/conflict zones, secure airborne transmission of videos for intelligence/security or surveillance purposes, and secure video communication for law enforcing agencies in crime fighting or in proactive forensics. Video content generally is too significant and vulnerable to eavesdropping when it transmitted over open network channels so that compression and encryption become essential for storage and/or transmission. In terms of security, wireless channels are more vulnerable than other kinds of mediums to a variety of attacks and eavesdropping. Since wireless communication is the main mode in the above applications, protecting video transmissions from unauthorized access through such network channels is a must. The main and multi-faceted challenges that one faces in implementing such a task are related to competing, and to some extent conflicting, requirements of a number of standard control factors relating to the constrained bandwidth, reasonably high image quality at the receiving end, the execution time, and robustness against security attacks. Applying both compression and encryption techniques simultaneously is a very tough challenge due to the fact that we need to optimize the compression ratio, time complexity, security and the quality simultaneously.

There are different available image/video compression schemes that provide reasonable compression while attempting to maintain image quality, such as JPEG, MPEG and JPEG2000. The main approach to video compression is based on detecting and removing spatial correlation within the video frames as well as temporal correlations across the video frames. Temporal correlations are expected to be more evident across sequences of frames captured within a short period of time (often a fraction of a second). Correlation can be measured in terms of similarity between blocks of pixels. Frequency domain transforms such as the Discrete Cosine Transform (DCT) and the Discrete Wavelet Transform (DWT) have both been used to restructure the frequency content (coefficients) to become amenable for efficient detection. JPEG and MPEG use DCT while JPEG2000 uses DWT. Removing spatial/temporal correlation encodes only one block from each class of equivalent (i.e. similar) blocks and remembering the position of all other block within the equivalence class. JPEG2000 compressed images

achieve higher image quality than JPEG for the same compression ratios, while DCT-based coding suffer from noticeable distortion at high compression ratio but when applied to any block it is easy to isolate the significant coefficients from the non-significant ones.

Efficient video encryption in computationally constrained applications is another challenge on its own. It has long been recognised that selective encryption is the only viable approach to deal with the overwhelming file size. Selection can be made in the spatial or frequency domain. Efficiency of simultaneous compression and encryption is a good reason for us to apply selective encryption in the frequency domain.

In this thesis we develop a hybrid of DWT and DCT for improved image/video compression in terms of image quality, compression ratio, bandwidth, and efficiency. We shall also investigate other techniques that have similar properties to the DCT in terms of representation of significant wavelet coefficients. The statistical properties of wavelet transform high frequency sub-bands provide one such approach, and we also propose phase sensing as another alternative but very efficient scheme.

Simultaneous compression and encryption, in our investigations, were aimed at finding the best way of applying these two tasks in parallel by selecting some wavelet sub-bands for encryptions and applying compression on the other sub-bands. Since most spatial/temporal correlation appears in the high frequency wavelet sub-bands and the low-low (LL) sub-bands of wavelet transformed images approximate the original images then we select the LL-sub-band data for encryption and the non-LL high frequency sub-band coefficients for compression. We also follow the common practice of using stream ciphers to meet efficiency requirements of real-time transmission. For key stream generation we investigated a number of schemes and the ultimate choice will depend on robustness to attacks.

The still image (i.e. Reference frames) is compressed with a modified Embedded Zero tree of Wavelet (EZW) wavelet scheme by applying the DCT on the blocks of the wavelet sub-bands, selecting appropriate thresholds for determining significance of coefficients, and encrypting the EZW thresholds only with a simple 10-bit LFSR cipher. This scheme is reasonably efficient in terms of processing time, compression ratio, image quality, as well as security robustness against statistical and frequency attack. However, many areas for improvements were identified as necessary to achieve the objectives of the thesis.

Through a process of refinement we developed and tested 3 different secure and efficient video compression schemes, whereby at each step we improve the performance of the scheme in the previous step. Extensive experiments are conducted to test performance of the new scheme, at each refined stage, in terms of efficiency, compression ratio, image quality, and security robustness.

Depending on the aspects of compression that needs improvement at each refinement step, we replaced the previous block coding scheme with a more appropriate one from among the 3 above mentioned schemes (i.e. DCT, Edge sensing and phase sensing) for the reference frames or the non-reference ones. In subsequent refinement steps we apply encryption to a slightly expanded LL-sub-band using successively more secure stream ciphers, but with different approaches to key stream generation. In the first refinement step, encryption utilised two Linear Feedback Shift Registers (LFSR) seeded with three secret keys to scramble the significant wavelet Low-Low (LL) -coefficients multiple times. In the second approach, the encryption algorithm utilises LFSR to scramble the wavelet coefficients of the edges extracted from the low frequency sub-band. These edges are mapped from the high frequency sub-bands using different thresholds. Finally, a version of the A5 cipher combined with chaotic logistic map is used to encrypt the significant parameters of the LL sub-band.

Our empirical results show that the refinement process achieves the ultimate objectives of the thesis, i.e. an efficient secure video compression scheme that is scalable in terms of the frame size at about 100 fps and satisfying the following features; high compression, acceptable quality, and resistance to the statistical, frequency and the brute force attack with low computational processing. Although image quality fluctuates depending on video complexity, in the conclusion we recommend an adaptive implementation of our scheme.

Although this thesis does not deal with transmission tasks, the efficiency achieved in terms of video encryption and compression time as well as in compression ratios will be sufficient for real-time secure transmission of video using commercially available mobile computing devices.