CHAPTER 7

CONCLUSION AND FUTURE WORK

7.1 CONCLUSION

With the advent of multimedia technologies, the information shared across the network are in various forms such as text, audio and video. Video sharing over Internet gains considerable importance with the increasing use of e-governance, e-business and social networking. Security, speed and resource requirement are some key factors that need to be considered during video transmission across networks. Various compression and encryption techniques have been proposed in the literature for secured video transmission. Over the years, it is observed that joint video compression and encryption techniques perform better than independent encryption techniques. Three joint compression and encryption algorithms, namely, Fast Random Bit Encryption (FRBE), Puzzle Fast Random Bit Encryption (PFRBE), and Enhanced Randomized Arithmetic Coding (ERAC) have been proposed in this thesis for secured video transmission. The proposed algorithms are efficient in terms of execution time, resource management and security. All three proposed techniques employ lossless compression. They provide additional security when compared to other video encryption algorithms and consume less resource during encryption.

The first method, Fast Random Bit Encryption (FRBE) technique, compresses the data using GZIP tool and then encrypts the compressed video with a four-step-procedure which provides multilevel security to the video
data. FRBE takes less execution time for encryption when compared to other traditional independent encryption algorithms. This is mainly due to compression before encryption. In PFRBE, Entropy Coding (EC), Puzzle Transform (PT) and RAC are used for compression and FRBE for encryption. ERAC integrates the interval splitting RAC with a simple bitwise XOR operation which prevents cryptanalytic attacks. From the analysis, it is observed that encryption of key along with video data mitigates various security threats. Experimental results obtained indicate that the proposed methods have the advantage of improved security and speed over existing algorithms such as AES, RSA, PGP, TEA, RC6, SECMPG, VEA, RVEA, Zigzag and RAC. FRBE consumes 27% and 13% less CPU overhead than RSA and AES algorithms respectively. PFRBE has 11.9% and 12% less CPU overhead when compared to VEA, SECMPG respectively. ERAC has 10.48% less CPU overhead when compared to RAC.

Among the three proposed techniques, ERAC has shown better performance than other two methods due to the following reasons: (i) less computational overhead, (ii) padding of encrypted key and video together. On the average, ERAC decreases 13.6%, PFRBE decreases 11.8% and FRBE decreases 5.8% of the file size during compression. ERAC has 4.1% and 18.9% less CPU overhead when compared to PFRBE, FRBE respectively.

7.2 SCOPE FOR FUTURE WORK

- Applying the proposed encryption techniques on audio data and combined video-audio data is an interesting open problem.
- The proposed methods are tested with recorded / saved video files. They may be tested on live video streams.

- Performance of the proposed techniques is analyzed based on CPU utilization, memory utilization and execution time. However, hardware (VLSI / FPGA) implementation of the proposed encryption algorithms using Electron Design Automation (EDA) tools is an open problem. The proposed methods can be further optimized to reduce the power and area requirements.