CHAPTER 9

SUMMARY AND CONCLUSIONS

9.1 SUMMARY

This chapter reviews the significance of the proposed voting protocol and proposed symmetric key algorithms in order to enable the voting requirements and makes suggestions for future research. Before proceeding with the review of the work done, the objectives of the thesis stated earlier in the introductory chapter are recalled.

The primary objective of this research is to propose alternative feasible high speed electronic voting system model. The essential requirements for electronic voting system have been analyzed. The electronic voting system with cryptographic technique in the past literature was found. In this regard, the limitations and the challenges of the existing voting system and the limitations of cryptographic techniques involved in the voting system have been examined. The scope and essential requirements for electronic voting systems such as fairness, privacy, uniqueness, eligibility, accuracy, authentication, anonymity, and uncoercibility have been identified.

The various existing protocols such as Two agency Protocol, Blind signature and Sensus protocols are based on the asymmetric key cryptosystem. Asymmetric key cryptosystem is much slower and more complex than symmetric cryptosystem. Moreover, these protocols are more difficult to implement and it is very difficult for the average user to follow it
correctly. It is proposed to incorporate the convenience of a public-key cryptosystem with the efficiency of a symmetric-key cryptosystem (also called hybrid cryptosystem). Hence, the present investigation was carried out to construct an alternative high speed, fool-proof and error less electronic voting system.

9.2 CONCLUSIONS

From this investigation the following conclusions are derived.

- New symmetric key algorithm proposed and developed based on the feistel cipher structure but using a new substitution technique and using different folding functions such as horizontal and vertical folding. In this investigation, the proposed symmetric key algorithm can be effectively used in the voting phase to encrypt the ballot.

- New voting protocol proposed and developed based on the hybrid cryptosystem. In this, the ballot is encrypted using the above mentioned proposed symmetric key algorithm and secret key information is encrypted using Tallier’s public key. Then, the Tallier decrypts the digital envelope using his own private key to get the secret key and then only the casted vote is decrypted using the received secret key. Once it is done, the confirmation message will be sent to the Validator to set the status bit of the voter. At the same time, the corresponding candidate’s count is updated in the same transaction.

- From the simulation results, it is easy to understand that the proposed symmetric key algorithm achieves better performance than the existing algorithms. The processing time is very less.
From the analysis, the proposed voting protocol satisfies eligibility, uniqueness, fairness, efficiency, authentication, security, anonymity and privacy issues as well.

The proposed voting protocol also increases the performance by 30% than the existing algorithms.

9.3 SUGGESTIONS FOR FUTURE WORK

Though the present investigation has brought out some important results and conclusions on electronic voting system, the research work can be extended further to address the following issues:

- To enhance the further speed and security, the cryptographic algorithms (i.e., Voting software) can be embedded in the smart card itself.

- This thesis makes use of VeriEye SDK to compare the iris pattern. To reduce the expenditure, one can implement new efficient iris pattern matching algorithm that can be embedded with this voting software.

- It is very difficult to achieve uncoercibility property in any remote voting system. One can incorporate this property in the next revision.

- Multimodal bio-metric techniques can be used for protocol development.

- World wide security mechanisms can be implemented for uniformity and quick voting results declaration.