Chapter 11
Conclusion

ABSTRACT

This chapter summarizes the book's contribution to the domain of information security and biometric research, and points out future directions of this dynamic field of studies. The book is the first to link the concepts of security, biometric and computational intelligence, and show how intricately they are woven with one another.

1. BOOK SUMMARY

This book is the first to link the concepts of security, biometric and computational intelligence and show how intricately they are woven with one another. It starts off by looking at the history of computational intelligence and relates it to current security research. Biometric systems, and their functionalities, performances issues and challenges are reviewed next. Based on known issues with single biometrics, a concept of multimodal biometric system is presented. Pros and cons of multimodal biometric systems along with various development issues have been studied in literature. They are further discussed and illustrated in this book.

Among the fusion approaches, pre-matching fusion approaches, such as sensor level fusion and feature level fusion, are discussed. Match score level fusion methods which are very popular with developers are presented and decision level fusion approaches used in many commercial biometric systems are discussed next. The focus then moves onto rank level fusion methods. Novel rank fusion approaches based on fuzzy logic and Markov Chain method have been introduced. For rank level fusion, comparison with highest rank, Borda count, logistic regression methods have been performed.

Outcomes of the practical multi-modal system implementation and experimentations have been presented and discussed further. Aside from increased accuracy, enrolment and response times

DOI: 10.4018/978-1-4666-3646-0.ch011

which are very essential in time critical security systems have been computed and analyzed for different scenarios.

Novel alternative approaches based on computational intelligence paradigm are presented next. These include chaotic neural network and dimension-reduction concepts for multi-biometric system design, robotic biometric and avatar recognition for intelligent software security systems, and a concept of application of soft biometric, social networks and social trends for improved performance of multi-modal biometric system.

2. CONCLUSION

The world where we are living is more complex and yet arguably less secure than ever. There is tremendous pressure on government and public organizations to increase the security, with increased investments to both research and development in this field. However, at the same time, the security breaches become more frequent, more costly and more severe, with potential to negatively impact all spheres of personal life of an individual, a large corporations, stock markets, and even political structure of a country.

Multimodal biometric system emerged as one of the solutions which provides a significant advantages over unimodal biometric system, such as increased and reliable recognition performance, fewer enrolment problems and suitability of the final system to be used in real world security crucial applications. The design of a multimodal biometric system is a challenging task due to heterogeneity of the biometric sources in terms of the type of information, the magnitude of information content, correlation among the different sources and conflicting performance requirements of the practical applications.

Researchers are still trying to find a good combination of biometric traits and various fusion methods to find the optimum recognition performance. As recent results has shown, a multimodal biometric system developed using fuzzy fusion approaches along with soft biometric information is a powerful tool to achieve this. A novel rank fusion approach, Markov chain based rank fusion, has been introduced which satisfies the Condorcet criteria essential for any fair rank aggregation process and can enhance the performance by a significant margin even in the presence of some low quality data. It significantly improves the response time as well as the recognition performance of any multimodal biometric system.

Furthermore, utilizing neural networks and social traits can lead to increased system reliability and recognition rates. A combination of such intelligent approaches with formal topological neighborhood relationship and rigorous mathematical measures of closeness seem to result in highly reliable systems.

3. FUTURE RESEARCH DIRECTIONS

There are many interesting questions left for future research enquiry. Many of them were identified in concluding chapter discussions. Some key observations are summarized here.

A true multimodal database can be quite useful for developing a reliable and efficient security application. True multimodal database with the identical conditions can be employed for further performance analysis. In most cases, biometric based security systems need to operate in real-time mode. Proper instruments for capturing real-time data and peripheral communications are needed for this purpose. Special concentration is needed to automatically acquire soft biometric information in real-time setup.

Dual or tri-level (different fusion in different levels of the system) fusion scenarios can be implemented to make the system faster and sig-