Journal of Engineering and Applied Sciences 12 (9): 2367-2370, 2017
ISSN: 1816-949X

Design of Multimodal Biometric Framework for Distributed Personal Identification

[1]Jayakumar Vaithiyashankar, [1]Shohel Sayeed,
[1]Anang Hudaya Bin Muhamad Amin and [2]Andrews Samraj
[1]Faculty of Information Science and Technology, Multimedia University, Cyberjag, Malaysia
[2]Department of Information Technology, Mahendra Engineering College,
Anna University, Chennai, India

Abstract: In this study, we proposed a multi-modal biometric framework for the human identification based on the cloud computing platform. The proposed framework focuses on personal identification and the accuracy of the identification process. Additionally, it involves in discussing the advantages of multi-modal biometrics over the single modal methods. Also, the study elaborates about the improved method of combining the multi-modal biometrics with the parallel search method. This suggested design ensures the reliability and accuracy in the fast manner such that the validity of the system is confirmed.

Key words: Multimodal biometrics, cloud computing, parallel searching, personal identification, reliability

INTRODUCTION

The biometric system utilizes the measured physical features of particular person like the fingerprint, palm-print, face, ear pattern, hand-vein pattern, iris, retina, DNA sequence, etc. and also uses the behavioral characteristics as gait, signature, voice , etc. to verify and authenticate his/her identity (Calik *et al*., 2004).

At present, the personal identification gaining momentum with a lot of attention and the application like criminal identification needs the more elaborate and sophisticated methodology (Ross *et al*., 2006; Ross and Govindarajan, 2005). Solving the personal identification problems at Internet level is the hot topic in now a days biometric applications.

Prior to the multi-modal, the uni-modal was used for the identification and verification but hugely affected by the various issues as noise over the data and error rate which is not tolerable (Hong and Jain, 1998). The multi-modal biometrics came into the light to override the problems existed in the uni-modal systems (Barrero *et al*., 2013).

The biometric identification getting matured day-by-day with a lot of improvements. Due to the today's integrated environment, the data sprawled all over the network. Thus the solution for the single point and standalone solution are more and more ambiguous (Chang *et al*., 2003). The biometric solution also should be widespread and distributed over the network to meet the current demand.

In this study, we going to discuss the multi-modal biometrics framework architecture and summarize the various frameworks scope up to the implementation in the distributed manner.

The multi-modal biometrics has several advantages over the uni-modal biometrics. It is hard to spoof the multi-modal biometrics, the noise in the data can be tackled due to multiple pieces of evidence, the system is reliable because it's not depended on over a single input hence the fault tolerance is relatively higher (Zhang *et al*., 2008). We can target and follow the person without any hindrance due to the multiple biometric traits.

The major steps in biometric identification involve with the data acquisition, preprocessing, feature extraction, post processing, template generation. But these process are suitable for the stand alone system. In the case of the distributed identification over the cloud. The given input need to match with the already existing database.

Literature review: Snelick *et al*. (2005) analysed the performance of multimodal biometrics using the fingerprint details and biometric face templates over thousand persons. They used newly devised normalization concept and the fusion method in order to achieve the score level fusion for matching biometric templates.

Ben-Yacoub *et al*. (1999) combined various fusion techniques like SVM, tree classifiers and multilayer perceptron for matching both face and voice data. The best method is identified by comparing the bayes with other classifiers.

Corresponding Author: Jayakumar Vaithiyashankar, Faculty of Information Science and Technology, Multimedia University, Cyberjag, Malaysia

Ross *et al.* (2006) confirmed that sum rule gives more and perfect score than the decision tree and linear discriminant based classifier over the different biometric data such as the face, fingerprint and hand geometry.

Richiardi *et al.* (2005) presented the distributed framework for multimodal biometric authentication. The design consists of the transparency in network system, end-to-end encryption and biometric data management services in the overall architecture.

Raghavendra *et al.* (2011) designed the fusion schemes for the various multimodal biometrics such as face and palm print used the log-gabor transformations yields high dimensional feature spaces. They also infused the particle swarm optimization to identify the dominant subspace in the high dimensional feature space without degradation of the system performance.

Volner and Bores (2006) discusses the framework for the multi-modal biometrics to process and record data. It functions based on the biometric fusion type, each process is taken place through the respective API to obtain the optimized performance. The framework designed particularly for the airport authentication system.

MATERIALS AND METHODS

Proposed framework: The framework becomes the necessary part for integrating and coordinating the data acquisition, multi-modal biometric fusion techniques and biometric match algorithms. Hence, it is important to assemble all these above-mentioned functionalities within a single framework. In our proposed framework, we have several building blocks such as:

- Amalgamation of multi-modal biometrics
- Super unique key
- Query generator
- Customized search engine
- Search result report
- Biometric templates
- Application server
- User application framework
- User cloud

Amalgamation of multi-modal biometrics: In this part, the various biometrics inputs are given by the user to identify the particular person. Thus the multiple biometrics inputs are combined together to ensure more accuracy in identification. The biometric fusion can be implemented based on the ranking subjects. The integration of the various multimodal biometrics explored in the discriminant correlation analysis (Haghighat *et al.*, 2016).

Super unique key: After the amalgamation part, the unique key is generated and includes the details of multi-modal biometric inputs. The unique key is encrypted for the security purpose. So, it avoids the security flaws.

The super unique key is sent to the destination along the unsecured channel. Thus, we going to enable the cryptography algorithm such as RSA and AES for encryption purpose and to ensure the security of the super unique key.

Sura developed a model which deals with the cloud security by enabling mixed cryptographic algorithms while transferring data between service centre and the end-user. The researchers also suggest the AES method rather than other cryptographic techniques due to its low key size, faster performance and more immune to vulnerable attack.

Query generator: According to the contents in the unique key, the query is generated to search the database. The number of inputs in the unique key is replicated in the query parameters. The query is dynamically created based upon the argument given in the search string. Thus, query is used for searching the database in a meaningful context.

Customized search engine: The customized search engine is able to store the queries and designed for the biometric search purpose. The verification and identification can be done in the simplified textual environment easily. But in the case of the multimodal biometric system. The available data differs in the various format. When, there is a massive comparison, it's necessary for the search engine in order to perform this Hercules task.

Search result report: The search result is compiled into the report which consists all the information about the search operations with timestamps details and the number of resources used. The report consists of the time taken for the search process and the calculation of resources utilized during the time period also. The search result report is useful to identify the efficiency of the system for the analytical comparison with the traditional system.

Biometric templates: The biometric templates consist the various biometrics inputs combined together. It serves as the biometric dictionary for a particular person. The biometric templates are indexed periodically depending upon the system updates about the biometric databases.

Application server: The application server monitors and maintains every operation taken place in the whole architecture. It interacts with the application database, consists the unique key generator, query generator,

customized search engine, report generator, template generator, amalgamation unit. The application server lies the basic foundation for the entire framework. It serves the basic data interaction through each and every part of the system.

User application framework: The user application consists the user's input and output model, all the graphical unit interfaces, interaction with the application server. The user application enables the user to give the input of the particular subject's details as a face, fingerprint, palm print, iris, etc. It also permits the user to narrow down the search entity and redirect the search process. User application framework also provides the access to the application database and cloud connectivity. Finally, the search output collected as the report with the timestamp.

User cloud: The data stored in all the private and public cloud storages are accessed through the user cloud part of the system. The access of public cloud is as usual and the user can normally search through the search process. But, the access of private cloud should have prior permission such that only data can be searched in that cloud. The user cloud is the cloud area encompasses the private cloud, public cloud, community cloud and hybrid cloud. The user cloud can interact with another cloud by interfaces. Such that, it can transfer data efficiently with proper planning.

RESULTS AND DISCUSSION

Design of the framework: The design of the proposed framework is illustrated in Fig. 1. The user inputs are collected over the amalgamation unit, there we can combine the user biometric inputs together. The fusion technique may be applied for the multimodal biometrics. Then the super unique key is generated by using the user inputs. To maintain the secrecy of search this super unique is encrypted using AES algorithm.

The encrypted super unique key is passed over the application server, according to the user input the appropriate query is generated for the searching purpose. The customized search engine take care of the search process and keep on track over the search.

Initially, the search took place over the application database, if the data no matches then it transfer the control to the cloud search. The additional user input can be given to the system such that it reinitiate search process by updating the super unique key.

Dynamically, the search process updates with the new additional information and remaining process taken place as previously mentioned. The cloud services can be increased or decreased based upon the user request and demand.

The biometric template generated after the search process to easy the future search operations. Finally, the search result is generated as the report with elaborate

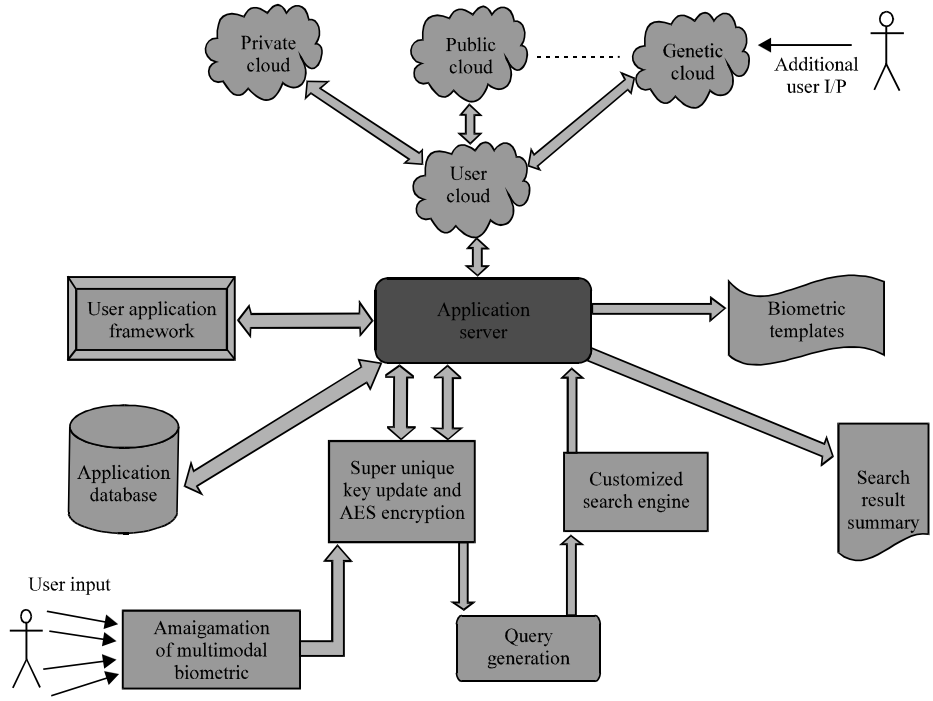

Fig. 1: Proposed framework of multimodal biometrics

details such as the information about the given input and the search process involved including the geographical location of the servers.

CONCLUSION

In this study, we proposed the new multi-modal biometric identification framework which supports the cloud-based personal identification. The first approach to the framework to start with a simple design with few biometric elements along the small data set. It ensures the secrecy of the search process all over the entire transaction. The framework provides the better solution than traditional search process and we can get hyper accuracy due to the multi-modal biometric identification system. The researchers are working on the platform for the practical implementation of the proposed framework.

ACKNOWLEDEGEMENTS

The researchers would like to thank Multimedia University, Malaysia. This work is supported in part by Ministry of Education Malaysia under the FRGS Research grant no: MMUE/140013.

REFERENCES

Barrero, G.M., J. Galbally, J. Fierrez and G.J. Ortega, 2013. Multimodal Biometric Fusion: A Study on Vulnerabilities to Indirect Attacks. In: Iberoamerican Congress on Pattern Recognition, Shulcloper, R.J. and D.B.G. Sanniti (Eds.). Springer, Berlin, Germany, pp: 358-365.

Ben-Yacoub, S., Y. Abdeljaoued and E. Mayoraz, 1999. Fusion of face and speech data for person identity verification. IEEE Trans. Neural Networks, 10: 1065-1074.

Calik, P., P. Yilgor, P. Ayhan and A.S. Demir, 2004. Oxygen transfer effects on recombinant benzaldehyde lyase production. Chem. Eng. Sci., 59: 5075-5083.

Chang, K., K.W. Bowyer, S. Sarkar and B. Victor, 2003. Comparison and combination of ear and face images in appearance-based biometrics. IEEE. Trans. Patt. Anal. Mach. Intel., 25: 1160-1165.

Haghighat, M., A.M. Mottaleb and W. Alhalabi, 2016. Discriminant correlation analysis: Real-time feature level fusion for multimodal biometric recognition. IEEE. Trans. Inf. Forensics Secur., 11: 1984-1996.

Hong, L. and A. Jain, 1998. Integrating faces and fingerprints for personal identification. IEEE. Trans. Pattern Anal. Mach. Intell., 20: 1295-1307.

Raghavendra, R., B. Dorizzi, A. Rao and G.H. Kumar, 2011. Designing efficient fusion schemes for multimodal biometric systems using face and palmprint. Pattern Recognit., 44: 1076-1088.

Richiardi, J., A. Drygajlo, V.A. Palacios, R. Ludvig and O. Genton *et al*., 2005. A distributed multimodal biometric authentication framework. Proceedings of the 3rd Cost 275 Workshop on Biometrics on the Internet, October 27-28, 2005, University of Hertfordshire, Hatfield, England, pp: 85-88.

Ross, A. and R. Govindarajan, 2005. Feature level fusion using hand and face biometrics. Proc. SPIE Conf. Biometric Technol. Hum. Identificat., 5779: 196-204.

Ross, A.A., K. Nandakumar and A. Jain, 2006. Handbook of Multibiometrics. Vol. 6, Springer, Berlin, Germany, ISBN:13:978-0-387-22296-7, Pages:

Snelick, R., U. Uludag, A. Mink, M. Indovina and A. Jain, 2005. Large-scale evaluation of multimodal biometric authentication using state-of-the-art systems. IEEE Trans. Pattern Anal. Machine Intellig., 27: 450-455.

Volner, R. and P. Bores, 2006. Multi-biometric techniques, standards activities and experimenting. Proceedings of the 2006 International Conference on Electronics Baltic, October 2-4, 2006, IEEE, Prague, Czech Republic, ISBN:1-4244-0414-2, pp: 1-4.

Zhang, T., X. Li, D. Tao and J. Yang, 2008. Multimodal biometrics using geometry preserving projections. Pattern Recognit., 41: 805-813.