Convolutional Neural Network Based Face Verification System for User Authentication

Harish H.R., Bhumika K, Pallavi Gowdoor.

Department of Information science & Engineering, SKIT College, India
Department of Information science & Engineering, SKIT College, India
Department of Information science & Engineering, SKIT College, India

Abstract–*The face recognition has become a common means of identity authentication because of the advantages of uniqueness, non-invasive and not easy to be stolen. In modern times, face recognition has become one of the key aspects of computer vision. The outsourcing of face recognition to the service provider is a typical manner nowadays. There are many biometric processes, in that face recognition is the best method. In this paper we are using Convolutional Neural Network (CNN) for face feature extraction and for the authentication purpose we make use of k- nearest neighbor algorithm.*

Key Words: Face Recognition, Convolutional Neural Network (CNN), Face Verification, k-Nearest Neighbor[1].

1. INTRODUCTION

In recent years, biometrics identification such as face, iris, fingerprints and DNA receive a significant attention, especially in the field of human identification and authentication. Compared with the traditional password-based authentication, biometrics has the advantages of uniqueness, distinctive, mobility, user friendliness and not being transferable. Face verification, as the most popular technology in biometrics, is widely used in authentication systems because its non-invasive and not needing the cooperation of users when scanning face images compared with the identification technology of fingerprint and iris. However, in addition to the advantages mentioned above, there are also many challenges about the technology of biometrics identification such as privacy and security. It is a very typical choice to perform face verification by the cloud service providers such as face++, but in this situation, one must upload the face image to the cloud server of service providers. Face image is extremely sensitive information, for it contains much privacy. In this paper, we propose a frame of identity authentication based on technology of face recognition in which k-nearest neighbor scheme is used for face recognition and convolutional neural network (CNN) is used for face feature extraction.

2. RELATED WORK

2.1 A Secure Protocol for Biometric Identification

In recent years, many privacy-preserving methods for biometric data recognition were proposed. The combination of cryptographic primitives such as homomorphic encryption and garbled circuits are mostly used for protect the biometric data in these methods. A secure protocol for privacy preserving biometric identification was proposed in [2] that can achieve security against semi-honest adversaries. The security model is designed by the scheme of homomorphic encryption, oblivious transfer and garbled circuit. Hamming distance and Euclidean distance are used for measuring the similarity of biometric information.

2.2 A Protocol for Outsourcing Identification of Encrypted Biometric Data

In [3], a protocol for outsourcing identification of encrypted biometric data to untrusted server was proposed, a new method of oblivious RAM was adopted for iris recognition and proved to be effective. The proposal only relies on standard symmetric encryption technology. The result shows that it is the only one that can deal with large databases and utilize all the opportunities of cloud computing

2.3 Finger and Iris-Recognition Based User Authentication

A privacy-preserving fingerprint recognition scheme was given in [4] that improved the performance of computation and communication efficiency. In [5], the privacy-preserving computation method was further improved that can be used for computing Euclidean distance, Hamming distance, Mahalanobis distance and scalar product of different biometric traits such as iris, face and fingerprint.

3. PROPOSED WORK

System design is the process of defining the architecture, components, modules, interfaces, and data for a system to satisfy specified requirements. System design could be seen as the application of systems theory to product development. The proposed user authentication system can be divided into four main modules. The modules and their functions are defined in this section. The four modules into which the proposed system is divided are:

3.1 Image Capture

We make use of WEB camera to capture the frontal images of the user and further process goes for face detection.

3.2 Face Identification

Face verification is the task of determine whether two face images belong to the same person. Face feature extraction is the first step of face verification. In early researches, many classical methods appeared, such as SIFTs, LBPs, and Gabor features. In recent years, CNNs-based methods have proven to be more efficient for face feature extraction. The structure of network in DeepID is shown in Figure 1. The network contains four convolutional layers and four max-pooling layers. Through this network, a 160-dimensional feature vectors can be extracted from a face image. In this paper, method of DeepID is used to extract facial feature vector.

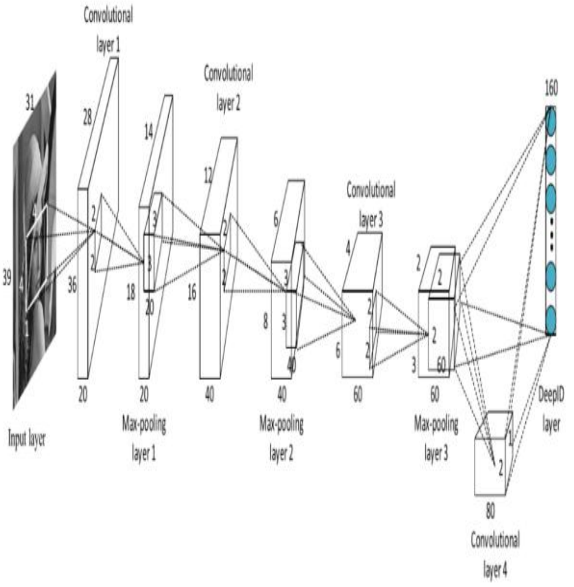

Figure 1: Overview of Proposed Method

3.3. Storing the Extracted Image Data in Database

As we chose biometric based system, enrolment of every individual is required. This database development phase consists of image capture of every individual and extracting the bio-metric feature, in our case it is face, and later it is enhanced using DeepID techniques and stored in the database.

3.4. User Authentication

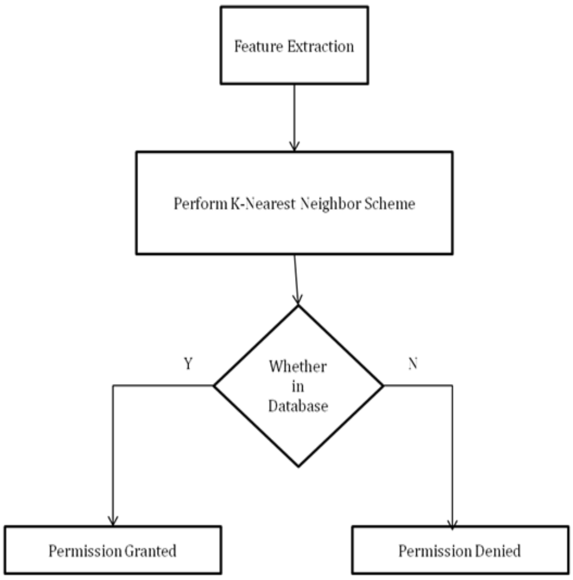

Figure 2: Flow Chart of Proposed Method

Face feature vector can reveal some information of face image content. Therefore, the plain text of the face feature vector cannot be stored without protecting, effective encryption method must be employed to protect the plaintext of face feature vector from being stolen by adversary. In this paper, the k- nearest neighbor algorithm is used as our encryption method that can not only protect the privacy of face feature vector, but also guarantee the ciphertext of the feature vectors can be used for face recognition. The most obvious advantage of k-nearest neighbor algorithm is that it doesn't need high computation complexities or communication burden compared with the homomorphic encryption algorithm. On getting the face image, the CNN will firstly extract a feature vector from it, then perform the k-nearest neighbor algorithm to encrypt the feature and store the ciphertext in its database. The database of each computing system is used for storing the face information of the users who registered on it. For the identity authentication, the system searches in its database using the method of k- nearest neighbor to find whether the user is registered on it, if so, we can get his permission immediately. Identity authentication can be completed if the user's feature vector is found in the database of the system. If the feature vector does not match then the user authentication fails.

4. EFFICIENCY EVALUATION

We compare the time consumption of face recognition achieved by the plaintext of face data with the ciphertext that encrypted by the privacy-preserving method we proposed above. The time consumption on the method of k-nearest neighbor contains the time of feature vectors extraction, encryption and recognition. The results about time consumption of these two situations are recorded according to considerable experiments. We can find that the time consumption of these two methods are almost linear to the number of face images in database from our experimental results. Notice that, the time consumption of face recognition with the face feature vectors protected by the k-nearest neighbor is almost equal to that with the plain text of face feature vectors. Thus, performing k-nearest neighbor scheme on the system can protect the face data of the users registered on it from being stolen by the adversary and won't waste too much time at the same time.

5. CONCLUSION

A convolutional neural network-based face verification system for user authentication is proposed in this paper. Face feature vectors are extracted by the method of convolutional neural network. K-Nearest Neighbor Method is introduced in our system to perform face verification. All operations in the system is performed on the encrypted feature vectors to prevent privacy leaks. How to ameliorate the encryption algorithm to further reduce the time consumption of authentication is still an open problem and will continue to be studied in our future work.

ACKNOWLEDGEMENT

With all respect and gratitude, we would like to thank all the people who have helped us directly or indirectly for the completion of the paper " A Convolutional Neural Network-Based Face Verification System for User Authentication ". We express our heartily gratitude towards Prof. Pallavi Gowdoor for guiding us to understand the work conceptually and also for her constant encouragement to complete this paper. Our association with her as a student has been extremely inspiring. We would like to give our sincere thanks to Dr. Hemalatha K.L. Head of the Department of Information Science and Engineering for her technical support and constant encouragement. We would also like to extend our sincere thanks to our Principal Dr. Manjunatha A. for his help and support in all respects. We would also like to thank all our staff members and collagues who helped us directly or indirectly throughout our dissertation work.

REFERENCES

[1] W. K. Wong, D. W.-L. Cheung, B. Kao, and N. Mamoulis, ‘‘Secure knn computation on encrypted databases,’’ presented at the ACM SIGMOD Int. Conf. Manage. Data, New York, NY, USA, Jun./Jul. 2009.

[2] M. Blanton and P. Gasti, ‘‘Secure and efficient protocols for iris and fingerprint identification,’’ presented at the Eur. Symp. Res. Comput. Secur., Leuven, Belgium, Sep. 2011.

[3] J. Bringer, H. Chabanne, and A. Patey, ‘‘Practical identification with encrypted biometric data using oblivious ram,’’ presented at the Int. Conf. Biometrics (ICB), Madrid, Spain, Jun. 2013.

[4] A.-R. Sadeghi, T. Schneider, and I. Wehrenberg, ‘‘Efficient privacypreserving face recognition,’’ presented at the Int. Conf. Inf. Secur. Cryptol., Seoul, South Korea, Dec. 2009.

[5] J.Bringer,H. Chabanne, M.Favre, A.Patey, T.Schneider, and M.Zohner, ‘‘GSHADE: Faster privacy-preserving distance computation and biometric identification,’’ presented at the 2nd ACM WorkshopInf. Hiding Multimedia Secur., Salzburg, Austria, Jun. 2014.