International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 05 | May 2019 www.irjet.net p-ISSN: 2395-0072

Confidential Data Access through Deep Learning Iris Biometrics

M. Preethi[1], K. Sathish[2]

[1]*Student, M.E, Computer Science and Engineering, Gojan School of Business and Technology, Tamil Nadu, India*
[2]*Assistant Professor, Computer Science and Engineering, Gojan School of Business and Technology, Tamil Nadu, India*

---***---

Abstract - *This paper explores automated iris recognition as a biometrically based technology for personal identification and verification. Because of the Fast growing mobile technology, when it comes to sensitive transactions, such as financial or payment applications, it is required to follow the security in all kinds of transactions made through mobile devices. Image based biometric authentication creates good impact on security. In the Existing System We develop a deep feature fusion network that exploits the complementary information presented in iris and periocular regions. The proposed method initially applies maxout units into the convolution neural networks (CNNs) to produce a compact description for each modality, and then combines the discriminative features of two modalities through a weighted concatenation. In the proposed system a deep neural network based classification algorithm is used, edge detection with adaptive contour segmentation is used to segment the iris from the given image. The quality of the image is enhanced through color equalization etc. The proposed system authenticates for a particular website access and which can be implemented in MATLAB software.*

Keywords - **Iris recognition, periocular recognition, deep feature fusion, adaptive weights, mobile devices.**

1. Introduction

"Biometrics is an attempt to imitate the elegant sensor fusion network of humans in identifying and verifying other humans by their behavioral and physiological characteristics" (a self-quote from Lisa Kalyan).

The first modern commercial biometric device was introduced over 25 years ago when a machine that measured finger length was installed for maintaining employee time records at Shearson Hamil on Wall Street. In the emerging years, hundreds of these hand geometry devices have been fixed for security purposes at facilities run by Western Electric and Naval Intelligence. In the US today, biometric security systems may be found in the Oakland International Airport (face recognition), Chicago O'Hare International (fingerprint), and the Navy Consolidated Building (iris recognition). With an increasing demand for better security technology in public and private buildings since September 11, 2001, a variety of pilot projects have been completed in the area of access control. These projects highlight the need to improve biometric verification accuracy, universality, and ease of use.

Identification methods can be grouped into three classes: something you possess as in an ID card, something you know, and something unique about you. Ownership (e.g., keys) can be easily lost, found, or duplicated. Knowledge can be forgotten as well as shared, stolen, or guessed. The value of forgotten passwords is excessive and accounts for 40%–80% of all the IT help desk calls. Resetting the forgotten or compromised passwords costs as much as $340/user/year. Biometrics, which is something unique about you, is inherently secure since they are unique features the person has. The science of biometrics is a solution to identifying an individual and avoids the problems faced by possession-based and knowledge-based security approaches. The aggregate security level of a system increases as these three identification approaches are combined in various ways. The least secure approach is one based solely on Personal Identification Numbers (PINs). This is because a very small PIN consisting of four characters can be easily guessed by an imposter, while a 200-character PIN is difficult for users to remember. This frequently leads to PINs getting compromised in many ways, such as a second possession. The biometrics system's security level can be improved by adding some possession such as an identification card.

2. Methodologies

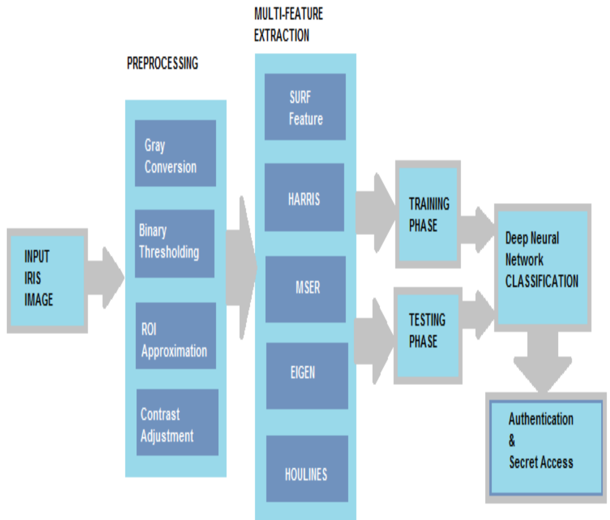

Fig 1: Block Diagram

2.1 Preprocessing: This module consists of MATLAB executable commands useful for extracting the image frames from the input database video. RGB panel is used to view the red, green and blue components of the image separately. It has previously been referred that an RGB image is overlap of three two dimensional matrix. The discrete cosine transform (DCT) is closely associated to the discrete Fourier transform.

2.2 Segmentation: The median filter is used in order to remove the noise from the merged RGB panel. The image features like color, weight, and depth and pixel information to apply before the classifier Here we used the adaptive hierarchical motion segmentation algorithm is used in order to segment the portion of defected areas.

2.3 Classification: This module is used to establish the concept for training the image and testing the image with the help of weight estimating classifier. With the help of metric value, the resultant image will be compared with the dataset images and it will display the analysis result of Iris image whether it is access granted or denied.

2.4 Neural Network: A Neural Network (NN) is a statistics processing paradigm that buck up by the way biological nervous systems, such as the brain, process information. The pointer element of this paradigm is the novel structure of the information processing system. It is composed of a huge number of highly interconnected processing elements (neurons) functioning in unison to decode particular problems. NNs, like people, learn by example. An NN is configured for a specific application, such as pattern recognition or data classification, through a learning process. Learning in biological systems requires adjustments to the synaptic connections that exist between the neurons. Neural networks are typically organized in layers. Layers are made up of a number of interconnected 'nodes' which contain an 'activation function'. Patterns are presented to the network via the 'input layer', which communicates to one or more 'hidden layers' where the actual processing is done via a system of weighted 'connections'. The hidden layers then link to an 'output layer' where the answer is output as shown in the graphic below.

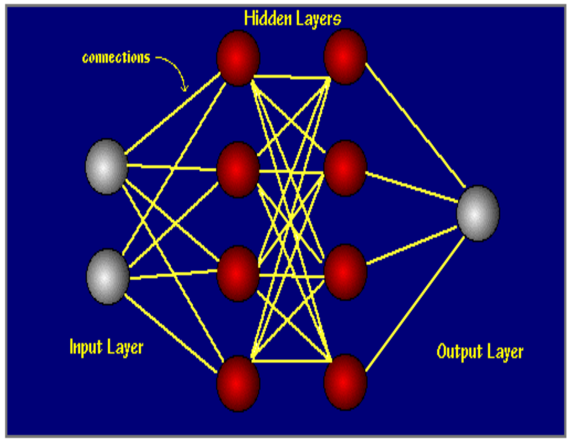

Fig 2: Hidden layer links to an output layer

2.5 Train the Network: Once the network weights and biases are loaded, the network is prepared for training. The training process involves a set of examples of proper network behavior of network inputs p and target outputs t. The process of training a neural network includes adjusting the values of the weights and biases of the network to optimize network performance, as explicate by the network performance function net.performFcn. The standard performance function for feed forward networks is mean square error (mse)—the average squared error between the network outputs a and the target outputs t. It is defined as follows:

There are two ways in which training can be executed: They are incremental mode and batch mode. In incremental mode, the gradient is computed and the weights are updated after each input is registered to the network. In batch mode, all the inputs in the training set are applied to the network before the weights are modernize. This topic narrates batch mode training with the train command. Incremental training with the adapt command is examined in Incremental Training with adapt. For most problems, when using the Neural Network Toolbox™ software, batch training is significantly faster and produces smaller errors than incremental training. For training multilayer feed forward networks, any standard numerical optimization algorithm can be applied to optimize the performance function, but there are a few key ones that have shown excellent performance for neural network training. These optimization methods utilize either the gradient of the network performance with respect to the network weights, or the Jacobian of the network errors with respect to the weights. The gradient and the Jacobian are evaluated using a technique called the back propagation algorithm, which includes performing computations backward through the network.

3. Result and Discussion

(I) Reduction in Computation Time

Type of Segmentation	Average Computation time
Region based Active Contour Segmentation	44.42s
Edge based Active Contour Segmentation	27.73s

Table 1: Output comparison with Region based Segmentation

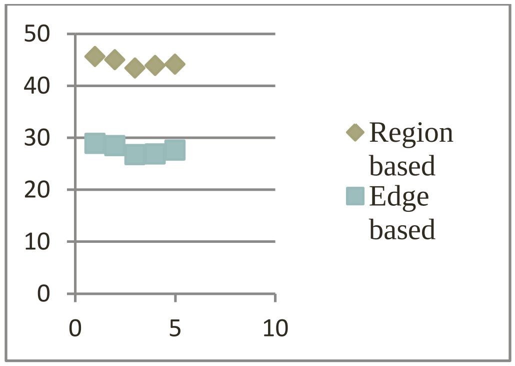

Chart 1: Decrease in Computational Time

(II) Specificity, Sensitivity and Accuracy

Method	Sensitivity	Specificity	Accuracy
Proposed-Edge based Active Contour	100%	92.308%	96.67%
Existing-Region based Active Contour	79.93%	99.10%	84.83%

Table 2: Comparison with Specificity, Sensitivity and Accuracy

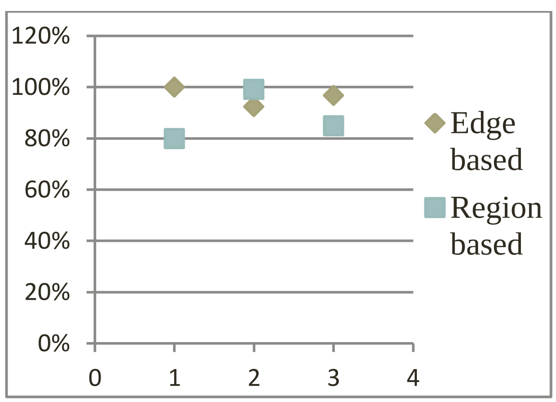

Chart 2: Edge based Vs Region based Segmentation

Conclusion

In this paper, we have proposed a deep feature fusion network that exploits the complementary information presented in iris and periocular regions to enhance the performance of mobile identification. Firstly, a CNNs model with maxout units has been exploited to extract robust, compact and discriminative features for the iris as well as the periocular region. Extensive experiments have been conducted and results have showed that the used CNNs model is effective and efficient. It has achieved state-of-the-art performance for both iris and periocular recognition on mobile devices. Afterwards, iris and periocular deep features have been fused through a weighted concatenation. The parameters of convolutional filters and fusion weights can be learned simultaneously to optimize the joint representation of iris and periocular biometrics. We have released the CASIA-Iris-Mobile-V1.0 database to the public, comprising of 11,000 images from 630 Asians. It is the largest NIR mobile iris database as far as we know and is valuable to promote the iris recognition research on mobile devices. Experiments have been conducted on the newly built CASIA-Iris-M1-S3 dataset which containing 3600 NIR iris images of both eyes from 360 Asians. Experimental results have showed that although periocular recognition gets much worse performance than iris recognition, bimodal fusion can still achieve significantly better results than unimodal recognition. The proposed deep feature fusion with adaptive weights approach has obtained promising results that the EER is 0.60% and FNMR@FMR=10^{-5} is 2.32%. The value of FNMR@FMR=10^{-5} drops by 52.0% and 81.7% compared with that of iris and periocular recognition, respectively. The value of EER drops by 37.5% and 54.2% compared with that of iris and periocular recognition, respectively. The results are also obviously better than directly concatenating various feature vectors. In addition, we have achieved significant improvements compared with the pervious study. By using the deep feature fusion with adaptive weights, the value of FNMR@FMR=10^{-4} has dropped by 70.6% compared with the previous best result. Moreover, the proposed model has required much less storage space and computational resources than general CNNs. Exploring complementary features of various modalities can take full advantage of different information, which will be beneficial for future multimodal fusion research. For the issue of mobile identification, we will focus on tackling the cross sensor recognition problem, matching images obtained from mobile devices and those from specialized equipment, which has practical significance. In the future, we will also try to use non-square filters and irregular kernel shapes in the CNNs model for processing rectangle iris images to avoid the image distortion problem.

Reference

[1] A. Joshi, A. K. Gangwar, and Z. Saquib, “Person recognition based on fusion of iris and periocular biometrics,” in International Conference on Hybrid Intelligent Systems, 2012, pp. 57–62.

[2] Q. Zhang, H. Li, M. Zhang, Z. He, Z. Sun, and T. Tan, “Fusion of face and iris biometrics on mobile devices using near-infrared images,” in Chinese Conference on Biometric Recognition, 2015, pp. 569–578.

[3] Q. Zhang, H. Li, Z. Sun, Z. He, and T. Tan, “Exploring complementary features for iris recognition on mobile devices,” in International Conference on Biometrics, 2016, pp. 1–8.

[4] R. P. Wildes, “Iris recognition: an emerging biometric technology,” Proceedings of the IEEE, vol. 85, no. 9, pp. 1348–1363, 1997.

[5] D. M. Monro, S. Rakshit, and D. Zhang, “DCT-based iris recognition,” IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 29, no. 4, pp. 586–595, 2007.

[6] Y.-h. Li, M. Savvides, J. Thornton, and B. Vijaya Kumar, “Iris recognition using correlation filters,” Encyclopedia of Biometrics, pp. 1015–1023, 2015.

[7] H. Proenca and L. A. Alexandre, “Toward covert iris biometric recognition: Experimental results from the nice contests,” IEEE Transactions on Information Forensics and Security, vol. 7, no. 2, pp. 798–808, 2012.

[8] K. W. Bowyer, “The results of the nice. ii iris biometrics competition,” Pattern Recognition Letters, vol. 33, no. 8, pp. 965–969, 2012.