Semiconductor Optoelectronics, *Vol. 42 No. 1 (2023), 1288-1295*
https://bdtgd.cn/

Semiconductor Optoelectronics ISSN: 1001-5868

SECURED BIOMETRICS AUTHENTICATION THROUGH EXTREME MACHINE LEARNING CLASSIFICATION ON RESIDUAL NEURAL NETWORK EXTRACTED FEATURES

Dr. N. Susitha[1*]
Associate Professor, Dept. of Computer Science,
School of Arts and Science, Vinayaka Mission's Research Foundation DU, Paiyanur, OMR, Chennai.

Dr. Monika G[2]
HOD i/c & Assistant Professor, Dept. of Computer Science & Applications,
Jeppiaar College of arts and Science, Padur, Chennai

Abstract – Iris detection and recognition systems are commonly used by several security based applications and the present literature contains numerous solutions for the same. Due to the increased usage of iris recognition systems, several attacks are launched to compromise the security of the application. One of the most harmful attacks is the presentation attack, which aims to mess up the system or to impersonate as the legitimate user. Both these scenarios are equally serious and this work attempts to present a presentation attack detection scheme for iris images by employing deep 150 layers of Residual Network(RESNET-150) and Extreme Learning Machine (ELM) classifier. When the classifier sniffs some abnormality, then the access is denied to the malicious user. Finally, the performance of the system is tested in terms of attack detection accuracy, false positive and negative alarms.
Keywords – Iris detection, Machine Learning classifier, security.

1. Introduction

Today's digital world handles most of the data online, which makes it prone to security attacks easily. In order to deal with this serious issue, several applications ensuring security are on the market. These applications follow different mechanisms for security achievement to handle security threats. Inspired by the uniqueness and stability of biometric features, this work intends to present a solution for presentation attacks in iris based security systems.

Biometric features define the biological aspects of an entity, which remain stable and cannot be stolen. The biometric feature can be chosen from the unique biological traits, based on the nature of the security application. Biological traits like speech, retina, iris, finger print etc. can be utilized in security systems. Among them Iris can be considered as reliable and stable trait [1, 2].

The iris recognition system has phases for gathering input picture, partitioning candidate segments, extracting eligible iris features and pattern cataloguing. The presentation attacks intend to mess up the recognition system by the act of masquerading as the legitimate user. This act of impersonation results in presenting access to the unintended users, which is a serious issue. This kind of presentation attacks can be avoided by tightening the feature extraction process. Taking this into account, this work extracts the textural features of the iris images by Deep Residual Network 150 (RESNET-150) and Extreme Learning Machine (ELM) classifier. Some of the highlighting points of the article are as follows.

- The reliability of the iris recognition system is improved, as the proposed approach combats against presentation attacks.
- The feature extraction of the proposed approach is focussed more, such that the intricate details of images help in improving the security of the system.
- As ResNet adds more and more attractiveness in the field of exploration, its structural design is getting studied profoundly.
- The metrics accuracy, sensitivity, specificity and optimum time utilization are satisfactorily met by the proposed method.

Further, the related review of literature with respect to iris recognition system is discussed in section 2. The proposed approach that withstands presentation attacks is presented in section 3. The performance of the proposed approach is analysed and discussed in section 4. Sections 5 brings to a close look at merits and the points to be analysed further.

2. Review of Literature

A brief literature review is undertaken to focus the analysis towards correct track in a more precise way.

In [3], 2D Gabor along with Particle Swarm Optimization (PSO) builds iris based security application. This work trains the system by neural network specifically multi-layer perceptron and PSO and the combination of these techniques is employed as classifier. A robust scheme to detect iris presentation attack by multi-scale binarized statistical features is presented in [8]. The PSO algorithm is utilized for training the neural network in performing classification. In [14], a technique to detect pupil and segment iris is presented. This work detects the pupil and eyelids of human eye, followed by which the iris is segmented. The performance of this work is tested over four different datasets and this work shows consistent performance.

An iris recognition system based on contouret and gabor features is proposed in [15]. This work segments the iris by means of integro-differential operator and the image contrast is improved by histogram equalization technique. The image is normalized by Daugman’s rubber sheet model and the combination of contourlet and gabor features are extracted. The Extreme Learning Machine (ELM) classifier is employed to classify and recognize the iris. In [16], a novel iris based security policy using LDP and ensemble classification is proposed. This work segments the iris and the LDP features are extracted. Classification by ensemble classifiers is then carried out by k Nearest Neighbour (k-NN), SVM and ELM.

The outstanding AlexNet, the high-tech CNN architecture is available deeper and deeper. While AlexNet had only 5 convolutional layers, the VGG network [23] had 19 layers and GoogleNet [24] had 22 layers in the network.

3. Protected Iris Recognition

This phase elaborately narrates the projected iris recognition approach along with the general outline of the work.

3.1 General Flow of the Research

Though there are numerous works in literature for recognizing iris, most of the systems do not consider the masquerading attacks. This work intends to tighten the security of the system by extracting better feature set and recognizes the iris accurately.

Additionally, this work considers the human eye images with contact lens. The classification part of this work is achieved by ELM as in [15]. The false acceptance and false rejection rates of the system access must be as minimal as possible. Hence, this work strives hard to achieve lease false acceptance and false rejection rates.

3.2 Proposed Secure Iris Recognition Approach

The proposed approach is divided into three major phases, which are iris segmentation, feature extraction and recognition.

3.2.1 Iris Segmentation and Normalization

This is the most crucial step of any iris recognition algorithm. The more accurate the iris segmentation, the better is the accuracy of the iris recognition system. This work utilises the iris segmentation algorithm in [14] and the segmented iris is normalised by Daugman's rubber sheet model as in [15].

3.2.2 Iris Feature Extraction

The most popular feature extraction model is to supply the image to a classical pre-trained neural network, and apply the version for that specific image in the in-between layers consisted in the neural network.

3.2.2.1 RESNET-150

ResNet-150 is a neural network which has deeper 150 neural convolution layers. The vector size of the extracted output feature set relies on the deployed depth of layer in the network. The residual block is set as proposed network's building block, therefore, during training, when a particular residual block is enable, its input flows through both the identity shortcut and the weight layers, otherwise the input only flows only through the identity shortcut. In training time, each layer has a "survival probability" and is randomly dropped. In testing time, all blocks are kept active and re-calibrated according to its survival probability during training.

ResNet Depth	Output Vector Size
18	512
34	640
50	890
101	1024
150	2048

3.2.2.3 ELM classifier

ELM is one of the promising classifiers with quicker learning capability [19] and the classifier is utilized as in [15]. The classifier can perform its function, when it undergoes two significant phases such as training and testing.

Let there be A_{TS} training samples as denoted by (s_i, t_i), where $s_i = [s_{i1}, s_{i2}, s_{i3}, \dots, s_{in}]^T \in D^n$, where s_i is the i^{th} training entity having n dimensions. $tk_i = [tk_{i1}, tk_{i2}, tk_{i3}, \dots, tk_{im}]^T \in D^m$, that represents the i^{th} training label with m dimensions. Here, 'm' denotes classes count. Neural Network based on Feed Forward technique particularly using Single layer (SLFN) is built up that deploys an activation method $act(x)$ with NR neurons.

$$\sum_{i=1}^{NR} \mu_i (wt_i . s_i + c) = r_j; j = 1,2, \dots, n \tag{1}$$

Where, $wt_i = [wt_{i1}, wt_{i2}, \dots, wt_{in}]^T$ and it interrelates the input neurons and i^{th} hidden neuron, here i value can be from $[i1, i2, \dots, im]^T$. The i^{th} hidden neuron is linked with the assistance of weight factor to the output neurons via the bias $(bias_i)$ of the i^{th} hidden neuron. The SLFN equation,

$$\sum_{i=1}^{NR} \mu_i act(wt_i . s_i + bias_i) = tk_i; i = 1,2, \dots, n \tag{2}$$

As the classifier has a hidden layer output matrix (HDL), the column i of HDL includes the output vector related to i^{th} concealed neurons, for the input ranges from$s_{i1}, \dots, s_{in}$.

$$HDL = \begin{bmatrix} act(wt_1 . s_1 + bias_i) & \dots & act(wt_{NR} . s_1 + bias_G) \\ \vdots & \vdots & \vdots \\ act(wt_1 . s_n + bias_i) & \dots & act(wt_{NR} . s_n + bias_G) \end{bmatrix} \tag{3}$$

$$\mu = \begin{bmatrix} \mu_1^T \\ \vdots \\ \mu_{NR}^T \end{bmatrix} \tag{4}$$

$$TK = \begin{bmatrix} tk_1^T \\ \vdots \\ tk_n^T \end{bmatrix} \tag{5}$$

The same format can be expressed in matrix notation as,

$$HDL\mu = TK \tag{6}$$

The least-square approach yields the output weights as below,

$$\mu = HDL^{\dagger} TK \tag{7}$$

In the above equation, the Moore-Penrose generalized inverse of HDL is represented by $HDL^{\dagger}$. The pre-requirements of ELM training includes class count m, activation function $act(x)$, NR hidden neurons. During the knowledge gaining phase, the ELM is provided with a training set $Tr_{set} = \{(s_i, t_i) | s_i \in D^n, t_i \in D^m; i = 1,2, \dots, N\}$. The training process is done by performing the operation as in equation 7.

4. Results and Discussion

Matlab 2013B software package has been deployed in order to simulate the proposed work, on an individual system with 16 GB RAM. The robust nature of the proposed system is established in terms of performance metrics. The existing approaches such as Multi Layer Perceptron (MLP) [3] and statistical features [8] are compared with the proposed approach. The main merit of the proposed approach is that the system recognizes the iris well, even when the candidate is wearing contact lens. This work utilizes the images available in the dataset [20].

(a) (b)

Fig.2. (a,b) Sample eye images from the dataset

4.1 Assessment of fitness w.r.t feature extraction methods

The unfathomable act of the deep feature extractor RES-150 is verified and compared with the traditional feature extractors such as GLVP and LVP.

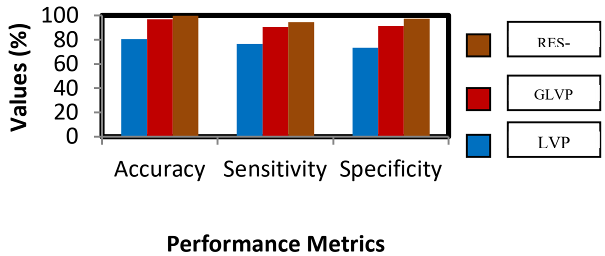

Fig.3. Robustness comparison w.r.t feature extraction methods

From the figure, it is apparent that a RES-150 deep neural layer performs well than the other two feature extraction techniques. The reason is that the pre trained deeper layers yield fine tuned extraction of features.

4.2 Assessment of fitness by varying classifiers

The classifier consumes some time for the learning process and during the process of testing; the classifier compares the query image with the images enrolled in the database for providing access to the system. The experimental outcome of this investigation is as follows.

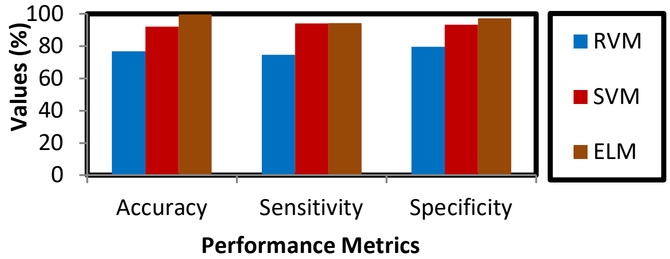

Fig.4. Fitness analysis by varying classifiers

Experimental results show that demonstrated ELM can be deployed as an improved classifier rather than RVM [21] and SVM [22]. The deeper RES-150 features are used in the training phase for the three classifiers and the results are recorded. ELM outweighs the other two classifiers in performance.

4.3 Assessment of fitness w.r.t existing approaches

The assessment of fitness of the proposed approach is undertaken by overall work with the state-of-art approaches in terms of accuracy, sensitivity and specificity as follows,

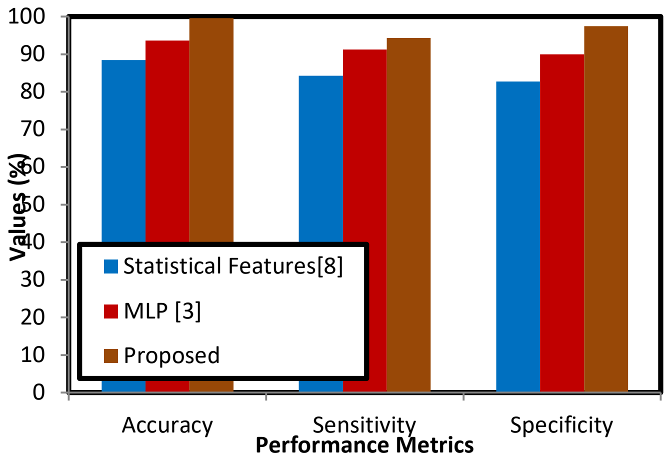

Fig.5. Fitness analysis w.r.t existing approaches

The performance of the proposed approach outperforms the existing approaches, owing to the efficiency of the feature extractor and the classifier.

Table 1: Time consumption analysis

Technique	Time consumption (ms)
Statistical features [8]	2967
MLP [3]	2138
Proposed	2079

With optimum time consumption, the targeted system outweighs in robustness. The prime cause behind this achievement is the quicker learning skill of the ELM classifier and the efficiency of the deployed deeper RES-150 feature extractor.

5. Conclusion

The iris of the human eye is segmented by the previously proposed algorithm and the deeper RES-150 convolution neural network extracts and generates feature vector. The trained ELM is engaged to recognize the iris. The metrics such as accuracy, sensitivity and specificity clearly states that the proposed approach outperforms the other comparative approaches, The less time consumption yields best possible iris detection rate. Processing images can be enhanced with different lighting conditions and 3D images can be utilized for recognition as an extension of this work in future.

References

[1] Akhtar, Z. & Kale, S., 2011. Security analysis of multimodal biometric systems against spoof attacks. Advances in Computing and Communications, Springer Berlin Heidelberg, pp. 604–611.

[2] I. Nigam, M. Vatsa, and R. Singh. Ocular biometrics: A survey of modalities and fusion approaches. Information Fusion, 26:1 – 35, 2015.

[3] Neda Ahmadi ; Gholamreza Akbarizadeh, "Hybrid robust iris recognition approach using iris image pre-processing, two-dimensional gabor features and multi-layer perceptron neural network/PSO", IET Biometrics, Vol.7, No.2, pp.153-162, 2018.

[8] R. Raghavendra ; Christoph Busch, "Robust Scheme for Iris Presentation Attack Detection Using Multiscale Binarized Statistical Image Features", IEEE Transactions on Information Forensics and Security, Vol.10, No.4, pp.703-715, 2015.

[14] N.Susitha, Ravi Subban, "Reliable Pupil Detection and Iris Segmentation Algorithm based on SPS", Cognitive Systems Research, Available Online, 2018. DoI: https://doi.org/10.1016/j.cogsys.2018.09.029

[15] Susitha N., Ravi Subban, "EFFICIENT IRIS RECOGNITION SYSTEM BASED ON CONTOURLET AND GABOR FEATURES", International Journal of Current Advanced Research, Vol.7, No.3, pp.10736-10742, 2018.

[16] N. Susitha & Dr. Ravi Subban, “A Novel Iris Based Security Policy Using LDP and Ensemble Classification”, International Journal of Current Research and Modern Education, Volume 3, Issue 1, Page Number 325-333, 2018.

[17] Fan K.C., Hung T.Y., “A Novel Local Pattern Descriptor—Local Vector Pattern in High-Order Derivative Space for Face Recognition,” IEEE Transactions on Image Processing, vol.23, no.7, pp.2877-2891, 2014.

[18] Zhang B., Gao Y., Zhao S., Liu J., “Local derivative pattern versus local binary pattern: Face recognition with higher-order local pattern descriptor,” IEEE Transactions on Image Processing, vol. 19, no. 2, pp. 533–544, 2010.

[19] Guang-Bin Huang, Hongming Zhou, Xiaojian Ding, and Rui Zhang, Extreme Learning Machine for Regression and Multiclass Classification, IEEE Transactions on systems, Man and Cybernetics - Part B, Vol.42, No.2, pp.513-529, 2012.

[20] http://iab-rubric.org/resources.html#iris

[21] Tipping, M. E. (2000). The relevance vector machine. In Advances in neural information processing systems (pp. 652-658).

[22] Adankon, M. M., & Cheriet, M. (2009). Support vector machine. In Encyclopedia of biometrics (pp. 1303-1308). Springer, Boston, MA.

[23] K. Simonyan and A. Zisserman. Very deep convolutional networks for large-scale image recognition. arXiv preprint arXiv:1409.1556,2014.

[24] C. Szegedy, W. Liu, Y. Jia, P. Sermanet, S. Reed, D. Anguelov, D. Erhan, V. Vanhoucke, and A. Rabinovich. Going deeper with convolutions. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition,pages 1–9,2015.