Advances in Parallel Computing Technologies and Applications
D.J. Hemanth et al. (Eds.)

doi:10.3233/APC210155

Automatic Biometric System for Finger Knuckle Using Sparse Encoder Approaches

Suganthi Devi S [a,1]

[a] *Lecturer, Department of Computer Engineering, Srinivasa Subbaraya Polytechnic College, Puthur, Sirkali (T.K.) Nagapatinam District, Tamil Nadu, India. [Deputed from Department of Computer Science and Engineering, Annamalai University]*

Abstract. Biometric recognition is one of the effective authentication techniques which is utilized in various applications for making the individual identification process. During the verification and authentication process different biometric features such as signature, ear, iris, face, palm, finger knuckle details are used to perform this process. Due to the easy acceptance of the palm surface, fine textures and stable features characteristics are helps to choose the finger knuckle feature for biometric process in this work. First the finger biometric features are collected from PolyU finger knuckle database. After that, the noise present in the images are eliminated using weighted median filter and the knuckle region is located with the help of the variational approach. After that key point descriptors are extracted using sparse autoencoder approach. Finally, the specific features are trained using compositional networks and features matching is performed by Chebyshev distance. The matching process authenticate the user whether they are authorized person or not. At last efficiency of the system is evaluated using MATLAB based experimental results such as false acceptance rate, equal error rate and false rejection rate.

Keywords. Biometric recognition, individual identification, finger knuckle features, PolyU finger knuckle database, variational approach, Chebyshev distance.

1. Introduction

Biometric [1] is the process of identifying and authenticating the person according to their recognizable data. During the biometric authentication process, user personal characteristics and identifies are used to authenticate the user to access the application or data. The authenticated characteristics [2] are their physiological information such as retina, hand geometry, DNA, signature, face, palm veins, face features, hand print, finger knuckle information, voice, gait, rhythm and so on. These biometric features are providing the access permission and control the unauthorized activities.In solving these real-time problems, [3] the impact of soft computing techniques which employ cognitive skills is very high. Although this system has been commercialized, the scope for improvement is still plenty. In many scenarios, [4] this authentication is provided by

[1] Suganthi Devi S, Department of Computer Engineering, Srinivasa Subbaraya Polytechnic College, Puthur. E-mail: ssuganthidevi@gmail.com

biometric systems. Moreover, the threat of pandemic has made the people to think of hygienic systems which are non-invasive.

These biometric authentication-based security [5] processes are utilized in different application [6] such as schools, college, office, bank transaction, hospital, attendance maintenance system and so on. As discussed earlier, each biometric feature having specific characteristics among that, finger knuckle biometric feature [7] have several advantages such as fine texture information, stable features, contact less, acceptance easy, easy capturing also it does not change according to personal feelings and other aspects. Due to these reasons, in this work finger knuckle biometric features are used to create the effective authentication [8] system. In addition to this, the finger knuckle biometric feature establishes the higher security collated with the other biometric features. Here the sample finger knuckle biometric graphical representation is depicted in Figure 1. With the help of the knuckle biometric feature [9] different automatic biometric system is created by applying the machine learning and image processing techniques [10]. There are several researchers uses the machine learning techniques to analyze the captured biometric image. Here few authors works are analyzed to get the knowledge about how the biometric images are processed. In [11] creating the multi model biometric system using deep learning techniques. Initially, finger knuckle print images are collected from user because, it is one of the effective, low cost and user-friendly biometric features. In [12] identifying and authenticating the user information using scale invariant feature transform and wavelet analysis. In this work fingerprint biometric features are getting from user which are decomposed into wavelet examination process. The wavelet approach decomposes the images into different sub image. After that scale invariant features are applied to extract the various descriptors. In [13] introducing parallel thinning approach to analyze the fingerprint approach. Initially, the fingerprint approach is captured, noise present in the images are removed with the help of median value. Then the thinning algorithm is applied to binarize the images. Then the thinning algorithm attains minimum execution time to authenticate the user effectively.In [14] creating the person authentication

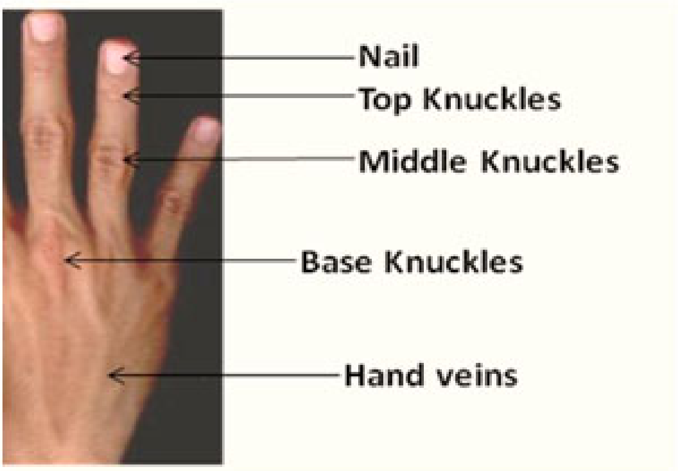

Figure 1. Sample Finger Knuckle Biometric Representation

system using biometric features. During this process, knuckle print imaging information is collected which are processed using effectively machine learning techniques.

2. Variational and Sparse Autoencoder Approaches Based Biometric Authentication System

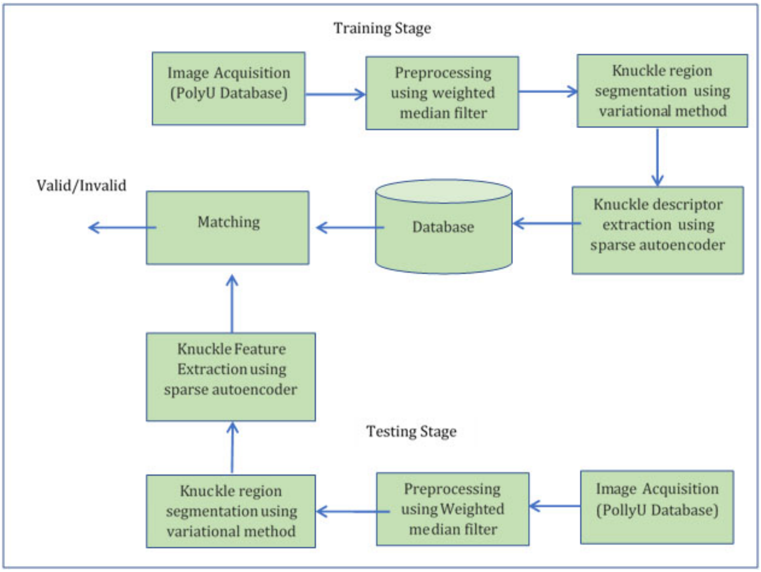
Training Stage
Image Acquisition (PolyU Database)
Preprocessing using weighted median filter
Knuckle region segmentation using variational method
Knuckle descriptor extraction using sparse autoencoder
Database
Matching
Valid/Invalid
Knuckle Feature Extraction using sparse autoencoder
Testing Stage
Knuckle region segmentation using variational method
Preprocessing using Weighted median filter
Image Acquisition (PollyU Database)

Figure 2. Automatic biometric authentication system structure

This section discuss about the variational and sparse autoencoder approach-based authentication system. The created system ability to recognize the users according to the personal traits for authenticating the credential and user information. For achieving the above discussed goal finger knuckle print biometric features [15] are used to authenticate each user while accessing the data from the application. In this work, polyU finger knuckle database images are used to process the introduced steps and methodologies. The system consists of different steps such as image collection, noise removal, knuckle region location, descriptor extraction and feature matching process which used to authenticate the user identifies. According to the list, the automatic biometric authentication system structure is depicted in Figure 2.

2.1. Finger Knuckler print image preprocessing

The first step of the work is to eliminate the noise from the image. The collected finger knuckle images having different type of noises due to the capturing process, name, image shake and so on. The inconsistent pixel details are reducing the authentications system and reduces the entire system security. So, the noise [16] present in the finger knuckle image must be removed by applying the weighted median filter. Initially, the pixels are checked against the threshold value. The threshold value is determined by analyzing the pixel range from the image. If the pixel value is deviated from the threshold value, it should be replaced by the weighted median value.

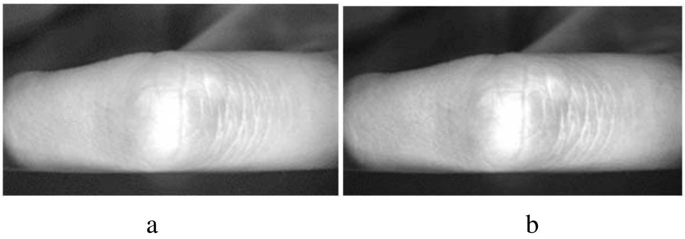

Figure 3. a) original finger knuckle image, b) noise free knuckle image

During this process, the weighted value is allocated depending on the user choice. When the highest value is chosen, the image has been smoothened effectively. Then the median value [17] is computed to replace the noise pixel value. This process is repeated until to eliminate the noise present in the image completely and the sample result is depicted in Figure 3.

2.2. Knuckle Region Segmentation

The second step of the work is to extract the knuckle region which is done by using the variational approach. It selects the optimal pixels while performing grouping process also consume minimum deviation and resolve the non-convexity problem. Due to this reason, in this work variational approach [18] is used for segmentation. During the segmentation process pixel energy function is used to predict the exact location. The energy function includes the pixel fitness criteria and regularizing terms. Then the pixel energy function is computed using Eq. (1)

$$argmin_{uy}||\nabla\mu||_{\int(\mu-f)^2dx} \tag{1}$$

In Eq. (1),μ represented as the piecewise constant image. The image energy function is relative between eh Chanvase and Mumford shah model that is written as follows.

$$argmin_u, Ky|K| + \int|\nabla\mu|^2dx + \int(\mu-f)^2dx \tag{2}$$

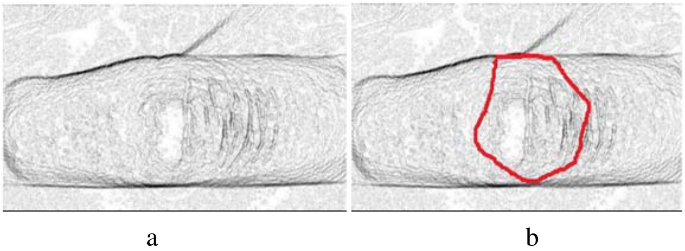

Figure 4. a) edge detected finger knuckle image b) knuckle region located finger knuckle image

The computed energy function value is addition of total length of the segmentation curve K,μ is represented as the smoothness f. So, the segmentation process includes the computation of the curve information, smoothness details and link between the curves are continuously examined. The identified similar smoothness related curves are grouped together. This process is repeated continuously until to locate the knuckle region from the noise removed image. According to the discussion, the sample knuckle segmented region is depicted in Figure 4.

2.3. Knuckle feature descriptor extraction

The third step of the work is to derive the descriptors [19] from the knuckle located image because, the key descriptors are used to match each person identities. The autoencoder utilizes the different layers such as input, hidden and output which helps to derive the features from located images unlike the autoencoder, sparse encoder [20] uses the greater number of hidden units compare to the input unit but minimum units are activated while extracting the features from the image. The feature extraction process includes the sparsity penalty concept in hidden layer h. The penalty process in layer h is mentioned as using Eq. (3).

$$L(x,x') + \Omega(h) \tag{3}$$

In eqn (3), h is computed using the pixel input, weight value and bias values that is represented as follows.

$$h = f(Wx + b) \tag{4}$$

The computed penalty value helps to determine the features in the knuckle image. During this process, each feature is extracted according to the activation function which is computed using the kullback-leiblerdivergence process. The activation function is computed using Eq. (5).

$$\rho_j - \frac{1}{m}\sum_{i-1}^{m}[h_j(x_i)] \tag{5}$$

According to the computed activation function each feature is analyzed continuously, then the minimum and maximum value of the located region is computed using Eq. (6).

$$D(x,y,\sigma) = L(x,y,K_i\sigma) - L(x,y,K_j\sigma) \tag{6}$$

in Eq. (6), knuckle region gaussian value is denoted as $D(x,y,\sigma)$, convolution of the knuckle region is represented as the $L(x,y,K\sigma)$ and the blur image is represented as the $I(x,y)$. By using these image details, key points are identified from the segmented region and the location of the key descriptors are identified with the help of the Taylor series that is computed using Eq. (7).

$$D(x) = D + \frac{\partial D^T}{\partial x}x + \frac{1}{2}x^T + \frac{\partial^2 D}{\partial x^2}x \tag{7}$$

After that, key point orientation is identified according to the various orientation and magnitude which is done as using Eq. (8).

$$m(x,y) = \sqrt{(L(x+1,y)-L(x-1,y))^2+(L(x,y+1)-L(x,y-1))^2} \tag{8}$$

in Eq. (8), magnitude of the key point is denoted as m (x, y) and orientation of the key point is determined as $\theta(x,y)$.

2.4. Matching process

The extracted features are trained by applying the compositional neural network [21] because it helps to improve the overall matching process. The network consists of multiple layers, which are trained based on activation function. In additionit also contains weight and bias values to improve the training process.

$$Netoutput = \sum_{i=1}^{N} x_i * w_i + b \tag{9}$$

In Eq. (9) x represented as the extracted features (input), w is weight value of the node and b is the bias values. This valueis processed according to eqn (9) and the net output value is computed. At the time of this process, following learning function is applied to train the features.

$$X_(k+1) = X_k + \left[J^T J + \mu I]\right]^{-1} J^T e \tag{10}$$

This process is applied to entire features in the feature list and the respective output value is computed. The resultant output is stored in the database as template which is used to matching process. When the incoming new user finger knuckle print is entered into the authentication system. The input image is processed is compared with the template features. The matching process is done by applying the Chebyshev distance [22] metric which detect the different between the two vectors. If the computed distance value is maximum, then it considered as the authorized or valid person else they are treated as unauthorized person. Then the Chebyshev distance value is computed using Eq. (11).

$$D_{chebyshev}(x,y) = max_i(|x_i - y_i|) \tag{11}$$

In Eq. (11) x is represented as the template feature and y is the testing finger knuckle features. According to the distance measure, the maximum relevant features are compared and identified effectively. In addition to this, once the feature similarity is identified, the feature value is further compared with the threshold value (0.3). If the computed feature value is maximum then the users are considered as the valid user else, they are terminated from access.

3. Results and Discussions

In this section discusses about the variational and sparse autoencoder based automatic biometric authentication system efficiency. During this process system uses the polyU finger knuckle print image database. The database consists of 7920 images which are collected from 165 volunteers that includes 40 females and 125 male information. During the data collection process, index finger, right middle finger, left middle finger, right index finger and 660 different finger information is analyzed and recorded. Based on the discussion, the collected finger knuckle print image is depicted in Figure 5.

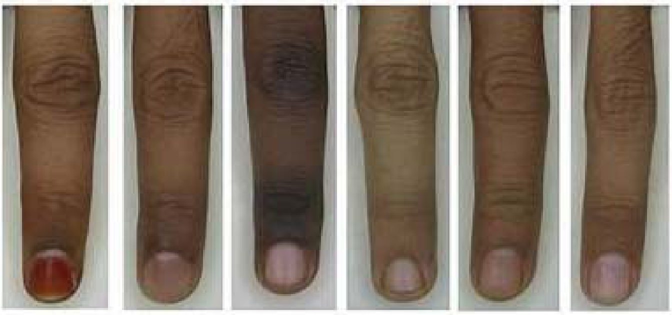

Figure 5. sample PolyU finger knuckle print images

After collecting the images, the above discussed steps are utilized to extract the knuckle region from the image. Once the region is extracted, respective features are derived which are trained and stored in database as template. Finally, the comparison process is performed according to the Chebyshev distance computation process. This discussed process is implemented using the MATLAB tool and the excellence of the system is determined using various performance metrics such as false acceptance rate, false rejection rate, equal error rate and authentication accuracy. False acceptance rate [17]- It is the important metrics, whether introduced system reject the false feature or false person into the system while analyzing the extracted features. The false acceptance rate is computed using Eq. (12).

$$FAR = \frac{Numberoffeaturesaccepted}{Numberoffeaturestested} * 100 \tag{12}$$

Based on the FAR computation process, the different finger knuckle print biometric images related false acceptance value is computed and the value is depicted in Table 1.

From the Table 1, it clearly depicted that the Autoencoder compositional network with Chebyshev distance (CAN+CD) approach having the minimum false acceptance rate compared to other classifiers such as Artificial Neural Network (ANN)[5], Multilayer Neural Network (MLP) [23], Back propagation Neural Network (BPNN)[24] and Deep Learning Neural Network (DNN)[25]. So, the false features are restricted to enter the system that is shown via the minimum false acceptance rate. Then the respective graphical analysis is depicted in Figure 6. The false acceptance rate of the Autoencoder compositional network with Chebyshev distance (CAN+CD) approach. From the analysis it clearly shows that CAN_CD (0.25%) of false acceptance rate compared to other ap-

Table 1. False Acceptance Rate

S. No	Classifier Methods	FAR (%),Number of Images						
		100	**200**	**300**	**400**	**500**	**600**	**700**
1	Artificial Neural Network (ANN)	0.59	0.63	0.79	0.62	0.793	0.634	0.65
2	Multi-layer Neural Network (MLP)	0.45	0.59	0.64	0.76	0.63	0.693	0.7
3	Back propagation Neural Network (BPNN)	0.38	0.44	0.59	0.64	0.66	0.59	0.53
4	Deep Learning Neural Network (DNN)	0.26	0.36	0.34	0.41	0.38	0.424	0.431
5	Autoencoder compositional network with Chebyshev distance (CAN+CD)	0.189	0.249	0.254	0.275	0.289	0.21	0.29

proaches such as ANN(0.67%), MLP(0.63%), BPNN (0.54%) and DNN(0.372%). The effective computation of the knuckle print features, link between the features and matching process helps to reduces the false feature acceptance while accessing the data in the system.

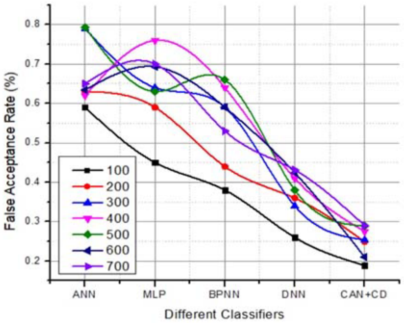

Figure 6. False Acceptance Rate (CAN+CD)

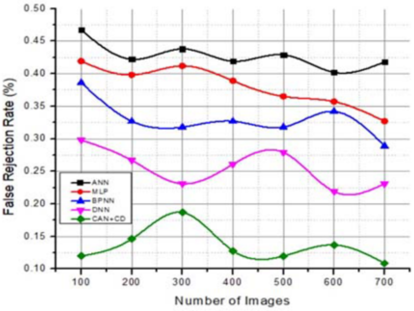

Figure 7. False Rejection Rate -CAN+CD

In addition to this, the system needs to reject only the false feature when it comes to access the data in the system. Then the false rejection rate [26] is estimated using Eq. (13).

$$FRR = \frac{Number of original features rejected}{Number of original features tested} * 100 \tag{13}$$

According to the Eq. (13), the system efficiency is analyzed how effectively the system access the authorized user and incorrectly reject the authorized users in the list. Based on the computation, the estimated false rejection rate is depicted in Table 2.

From the Table 2, it clearly depicted that the Autoencoder compositional network with Chebyshev distance (CAN+CD) approach attains low false rejection rate compared to other classifiers such as Artificial Neural Network (ANN), Multi-layer Neural Network (MLP), Back propagation Neural Network (BPNN) and Deep Learning Neural Network (DNN). Then the respective graphical analysis is depicted in Figure 7.

Table 2. False Rejection Rate

S.	Classifier Methods	FAR (%),Number of Images						
No		100	200	300	400	500	600	700
1	Artificial Neural Network (ANN)	0.467	0.422	0.438	0.419	0.429	0.402	0.418
2	Multi-layer Neural Network (MLP)	0.419	0.398	0.412	0.389	0.365	0.357	0.327
3	Back propagation Neural Network (BPNN)	0.386	0.327	0.318	0.327	0.318	0.342	0.289
4	Deep Learning Neural Network (DNN)	0.298	0.267	0.231	0.261	0.279	0.219	0.231
5	Autoencoder compositional network with Chebyshev distance (CAN+CD)	0.12	0.146	0.187	0.128	0.12	0.137	0.109

Figure 7 illustrated that the false rejection rate of the Autoencoder compositional network with Chebyshev distance (CAN+CD) approach. From the analysis it clearly shows that CAN_CD(0.134%) of false acceptance rate compared to other approaches such as ANN(0.42%), MLP(0.38%), BPNN (0.32%) and DNN(0.25%). The introduced CAN+CD approach examines the testing and training features using the effective distance measure, in addition to this, threshold-based comparison process also improves the overall authentication process. The effective computation process reduces the false rejection rate. Further efficiency of the system determined using the equal error rate [27] which is computed from the common value with the FAR and FRR. Then the computed equal error rate value is depicted in Figure 8. According to the above figure it clearly depicted that the (CAN+CD) approach attains minimum equal error rate value compared to other classifiers such as Artificial Neural Network (ANN), Multi-layer Neural Network (MLP), Back propagation Neural Network (BPNN) and Deep Learning Neural Network (DNN). The minimum error rate, false rejection value, false acceptance value directly indicates that the introduced CAN+CD system provide the security, authentication to the data while accessing the data. so, the overall recognition or matching rate is depicted in Figure 9. The (CAN+CD) approach ensures maximum authentication accuracy (99.52%) value compared to other classifiers such as Artificial Neural Network (ANN)(93.2%), Multi-layer Neural Network (MLP)(94.52%), Back propagation Neural Network (BPNN) (96.8%) and Deep Learning Neural Network (DNN)(98.7%). Thus the introduced Autoencoder compositional network with Chebyshev distance (CAN+CD)

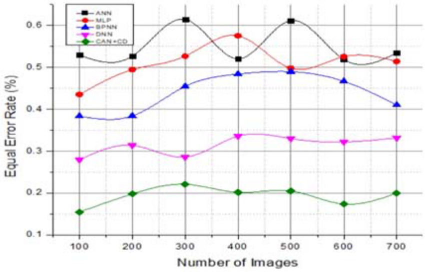

Figure 8. Equal Error Rate- CAN+CD

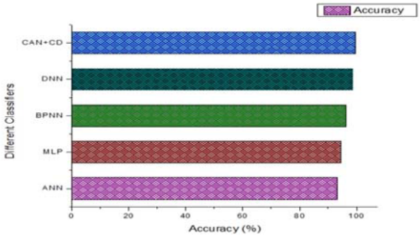

Figure 9. Authentication Accuracy

approach successfully ensure the security to the data by authenticating the users compared to other methods.

4. Conclusion

Thus, in this work creating the automatic biometric authentication system using the variationalAutoencoder compositional network with Chebyshev distance (CAN+CD) approach. Initially, finger knuckle print image is collected from the polyU finger knuckle image dataset. The collected images noise has been removed by computing the weighted median value. The method removes and smoothen the image effectively. Then the knuckle region is located by computing the pixel energy functionality value. Based on that information, region is located with the help of pixel link. After extracting the knuckle location, respective features are extracted by considering the sparse penalty value. Based on that information, autoencoder identify the features point, then the respective magnitude and key point orientation is derived. The derived features are trained and stored in the database as template. At last the matching process is performed by Chebyshev distance measure, in which maximum relevant features are considered as authenticated user else they are restricted to access the data. The efficiency of the system is evaluated using MATLAB based results in which system maintain the authentication up to 99.52% of accuracy with minimum error rate. In future, optimization techniques are used to select the best key point and improve the matching process using meta-heuristic techniques.

References

[1] Nagaraja S, Prabhakar CJ, Kumar PP. Extraction of texture based features of underwater images using RLBP descriptor. In Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014 2015 (pp. 263-272). Springer, Cham.

[2] Rabiul Islam M. Feature and score fusion based multiple classifier selection for iris recognition. Computational intelligence and neuroscience. 2014 Jul 10;2014:1-11.

[3] Winston JJ, Hemanth DJ. A comprehensive review on iris image-based biometric system. Soft Computing. 2019 Oct;23(19):9361-84.

[4] Jenkin Winston J, Turker GF, Kose U, Jude Hemanth D. Novel optimization based hybrid self-organizing map classifiers for Iris image recognition. International Journal of Computational Intelligence Systems. 2020 Aug;13(1):1048-58.

[5] Abiyev RH, Altunkaya K. Iris recognition for biometric personal identification using neural networks. In International Conference on Artificial Neural Networks 2007 Sep 9 (pp. 554-563). Springer, Berlin, Heidelberg.

[6] Kumar A, Ravikanth C. Personal authentication using finger knuckle surface. IEEE Transactions on Information Forensics and Security. 2009 Feb 10;4(1):98-110.

[7] He K, Zhang X, Ren S, Sun J. Deep residual learning for image recognition. In Proceedings of the IEEE conference on computer vision and pattern recognition 2016 (pp. 770-778).

[8] Maheshan CM, Kumar HP. Performance of image pre-processing filters for noise removal in transformer oil images at different temperatures. SN Applied Sciences. 2020 Jan;2(67):1-7.

[9] Krig S. Image Pre-Processing. Computer Vision Metrics. Apress, Berkeley, CA; 2014.

[10] Kuncheva LI, Faithfull WJ. Pca feature extraction for change detection in multidimensional unlabelled streaming data. InProceedings of the 21st International Conference on Pattern Recognition (ICPR2012) 2012 Nov 11 (pp. 1140-1143). IEEE.

[11] Faundez-Zanuy M. Biometric security technology. InEncyclopedia of Artificial Intelligence 2009 (pp. 262-269). IGI Global.

[12] Obaidat MS, Rana SP, Maitra T, Giri D, Dutta S. Biometric security and internet of things (IoT). InBiometric-Based Physical and Cybersecurity Systems 2019 (pp. 477-509). Springer, Cham.

[13] Inan Y, Sekeroglu B. Signature Recognition Using Backpropagation Neural Network. In International Conference on Theory and Applications of Fuzzy Systems and Soft Computing 2018 Aug 26 (pp. 256-261). Springer, Cham.

[14] Dey A, Pal A, Mukherjee A, Bhattacharjee KG. An approach for identification using knuckle and fingerprint biometrics employing wavelet based image fusion and SIFT feature detection. In Advancements of Medical Electronics 2015 (pp. 149-159). Springer, New Delhi.

[15] Gogna A, Majumdar A. Discriminative autoencoder for feature extraction: Application to character recognition. Neural Processing Letters. 2019 Jun;49(3):1723-35.

[16] Chantaf S, Hilal A, Elsaleh R. Palm vein biometric authentication using convolutional neural networks. InInternational conference on the Sciences of Electronics, Technologies of Information and Telecommunications 2018 Dec 18 (pp. 352-363). Springer, Cham.

[17] Arulalan V, Balamurugan G, Premanand V. Multi Modal Biometric Recognition System using Palm print and Inner-Knuckle Print. International Journal of Applied Engineering Research. 2015;10(14):34748-51.

[18] Chlaoua R, Meraoumia A, Aiadi KE, Korichi M. Deep learning for finger-knuckle-print identification system based on PCANet and SVM classifier. Evolving Systems. 2019 Jun;10(2):261-72.

[19] Kumar A, Ravikanth C. Personal authentication using finger knuckle surface. IEEE Transactions on Information Forensics and Security. 2009 Feb 10;4(1):98-110.

[20] Zhai Y, Cao H, Cao L, Ma H, Gan J, Zeng J, Piuri V, Scotti F, Deng W, Zhi Y, Wang J. A novel finger-knuckle-print recognition based on batch-normalized CNN. InChinese conference on biometric recognition 2018 Aug 11 (pp. 11-21). Springer, Cham.

[21] Anand J, Sivachandar K. An edge vector and edge map based boundary detection in medical images. International Journal of Innovative Research in Computer and Communication Engineering. 2013 Jun;1(4):1050-55.

[22] Karczmarek P, Kiersztyn A, Pedrycz W. An application of graphic tools and analytic hierarchy process to the description of biometric features. In International Conference on Artificial Intelligence and Soft Computing 2018 Jun 3 (pp. 137-147). Springer, Cham.

[23] Belgacem N, Fournier R, Nait-Ali A, Bereksi-Reguig F. A novel biometric authentication approach using ECG and EMG signals. Journal of medical engineering & technology. 2015 May 19;39(4):226-38.

[24] Kwon JS. Improved parallel thinning algorithm to obtain unit-width skeleton. The International Journal of Multimedia & Its Applications. 2013 Apr 1;5(2):1-14.

[25] Ioffe S, Szegedy C. Batch normalization: Accelerating deep network training by reducing internal covariate shift. In International conference on machine learning 2015 Jun 1 (pp. 448-456). PMLR.

[26] Anand J, Sivachandar K, Yaseen MM. Contour-based Target Detection in Real-time Videos. International Journal of Computer Trends and Technology. 2013;4(8):2615-18.

[27] Sibia EV, Mareena G, Anand J. Content Based Image Retrieval Technique on Texture and Shape Analysis using Wavelet Feature and Clustering Model. International Journal of Enhanced Research in Science Technology & Engineering. 2014;3(8):224-9.