JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Mechanism to increase the security using multimodal biometric with different approaches

Rajni,Suraj Pal
Department of Computer Science
Golden College of Engineering and Technology
Gurdaspur, India.

Abstract: In today's informative world, identifying a person's identity accurately and protecting the security is becoming important. Biometric recognition technology is becoming crucial and is widely being used. In today's world the most convenient and secured solution for the identification is multimodal biometric identification, which single biometric identification cannot achieve because of the complex identification situations. With multimodal system, accuracy and safety is achieved which may be lacked in single identification system. In this paper, biometric recognition system based on face, iris and fingerprints with CNN are evaluated. Multimodal biometric system based on deep learning algorithm is recommended for identifying humans based on face, iris and fingerprints. The whole structure of the system is based on convolutional neural networks (CNN). To find out the result of the accuracy on recognition system, CNN model is made for unimodal recognition system. Different fusion approaches are applied to carry out the recognition system. Then the CNN model for multimodal biometric system is developed based on two- layer fusion. In this paper Alex-Net and VGG-19 network models are evaluated in experimentation part for extracting iris, fingerprint and face image features as an input to the feature fusion module. Most of the empirical work is conducted using CMU PIE, CASIA and POLY-U datasets. Later based on both the studies it is concluded that multimodal biometric system is more accurate and reliable as compared to unimodal system. Furthermore, improvement to the multimodal biometric systems in terms of multi focal loss function for feature extraction was suggested.

Keywords: Multimodal Biometrics, Convolutional neural network, face recognition, iris recognition, and two-layer fusion.

1. INTRODUCTION

Biometric is made up of two words- Bio and Metrics which means measurement. Hence biometric is a branch of information technology which is used to identify any individual based on its traits[1]. Every person has his physical and behavioral characteristics which helps in identifying and make the person unique from other others[2]. Physical attributes includes finger prints, color of iris, face and behavioral characteristics includes its tone, speech, signature and many more features. This uniqueness of the person helps biometric system in-

- Identifying the person
- Authenticating the person
- And keeping them safe from unethical issues

Hence biometric system is defined as a technology which is used to take both physical and behavioral attributes as input [3]and then analyses them to find out whether the person is genuine or fake. Biometric is used in many fields such as in banking sector, security sign-ins, smartphone security, SIM cards, hospitals ,airports and many other sectors too[4]. Biometric system includes four basic components: Sensors, Processing Unit, database stores, and output interface.

In the figure 1 biometric system, the sample is collected from the user[5]. From the available sample all the important features are extracted and then it is compared with the samples that are stored in the database. The person is said to be the authenticated person if the input sample matches with the sample which is stored in the database[6]. In this way the whole biometric system works.

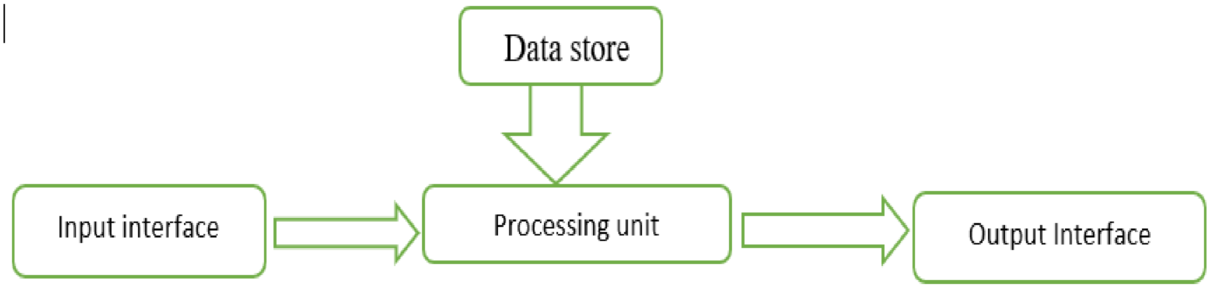

Figure1: Components of biometric system

Biometric recognition system is of two types- Unimodal biometric system and multimodal biometric system. Unimodal biometric system takes only single trait to identify and verify the individual while on the other hand multimodal biometric system includes two or more biometric technologies like fingerprints, facial recognition, iris scanning and many more[7]. Since unimodal biometric system is found to be proficient but still there exists many disadvantages:

- Sensitivity of the biometric sensor to noisy and bad data
- Biometric model may not be compatible with certain age group population especially with elderly and young children
- Unimodal biometric system may not work properly for twins as camera may not be able to detect similar faces
- Vulnerability to spoof attacks

A multimodal biometric system [8]comprises of following modules:

1. Sensor Modules
2. Feature Extraction Modules
3. Matching Module
4. Decision-Making Module

The process modeling corresponding to the sensors, feature extraction, matching and decision-making module is expressed within figure 2.

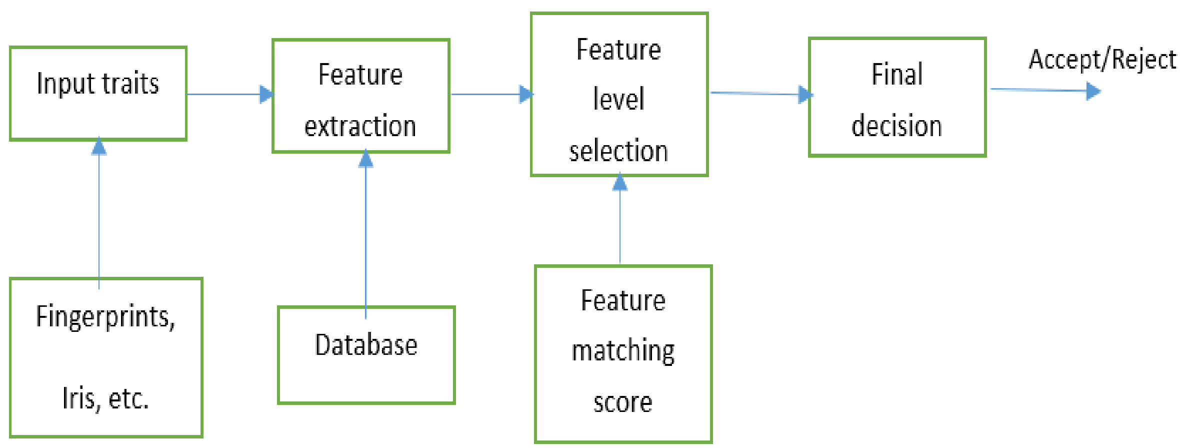

Figure 2: Block diagram of multimodal biometric system

The rest of the paper is organized into various sections. Section 2 provides insight into the related work. The methods used in the CNN are described in section 3. Section 4 examines the performance of various datasets. Finally, the conclusion is given in section 5.

2. RELATED WORK

Data and corresponding information are critical for any organization for success. Security of information thus becomes critical. Design of multimodal biometric system generally consists of phases as described in [9] .The first phase is pre-processing. This phase is critical in achieving high classification accuracy. The classification accuracy is the degree of true results obtained. The pre-processing phase remove the noise that can introduced due to issues with capturing mechanisms as discussed in[10]. The Delunay Quadrangle was proposed by [11]to deal with non-linear distortion within facial and fingerprint images. Distortion generally is caused due to inappropriate feature extraction mechanisms or problem with capturing mechanisms. To overcome the issue, [12] proposed eye tracking feature extraction for biometrics. Eye tracking based system gives accurate information about human actions and environment considering the mean shift filtering.

Second phase in the multimodal biometric recognition is segmentation. Segmentation is used to divide the image that could be biometric image into critical and noncritical sections[13]. Segmentation phase is critical in biometric image correlation analysis. Effective segmentation process leads to the correct and quick classification phase[14]. Segmentation phase can be accomplished in multiple ways including thresholding[15], region-based segmentation[16], edge detection[17] and clustering[18]. The edge detection and thresholding-based approach is useful in biometric image segmentation as fingerprint images have number of associated edges whose recognition is effective with edge detection. Furthermore, thresholding mechanism with Otsue mechanism give minimum and maximum values corresponding to the edge of the finger images[19].

After the segmentation phase, classification is performed. Classification phase is used to test the biometric image for authentication. Authentication as proposed in [20]. The degree of classification accuracy will enhance in case degree of misclassification is limited. The classification accuracy depends upon degree of true positive and true negative values achieved. Degree of true positive and negative values corresponding to support vector machine is better as discussed in [21]. Furthermore, KNN based classification model also provides better classification accuracy however static values corresponding to K is required[22]. Large datasets classification models thus are difficult to prepare using KNN. Ensemble based classification model appears to be best as discussed in [23].

Unimodal and multimodal security models are considered most appropriate for securing assets in the form of information[24]. [25]proposed secured user identification model using deep neural network-based approach. The layered based approach provides highest form of security using focal loss function at output layer. To provide the highest form of security, multimodal biometric security system integrated fingerprint, face, iris, signature, and voice. Hand vein, ear, speech and many more as proposed in [26]using CNN. Feature selection and extraction for biometric systems becomes critical for high classification accuracy. This was achieved using feature selection model through support vector machine as proposed in [27]. [28] proposed fusion of ECG and fingerprint model at the relocation layer within CNN. The validation of result in the form of classification accuracy in range of 90% was achieved. [29]proposed fusion of fingerprint, finger veins and face images as multimodal authentication system where the CNN and Delunay Quadrangle method was used for authentication and unique topology code for security and enhancement and local registrations.

Two methods were employed in eye tracking authentication system including texture-based methods and minutiae-based methods. The issues exist within traditional biometric systems as discussed in [30] and to overcome the issues, modification in existing models [31], [32], [33] and in [34]. The changes in terms of special function at output layer of CNN was useful as suggested by [35]. To achieving better security, [36] proposed multimodal biometric authentication system with the integration of artificial neural network for capturing and identification of dorsal hand vein patterns and palmar vein patterns to achieve better security in the form of authentication security system. Advanced security system using vein pattern recognition with segmentation mechanism proposed by [37]. This model was applied to view the entire vein features which is a dimension reduction technique.

The security of information with biometrics as explained in [38] with the different performance measurement parameters such as false acceptance rate (FAR), false reject rate (FRR), and equal error rate (ERR). Metric for classification required for validation of result includes classification accuracy, specificity, sensitivity and F-score as discussed in [39]

Unimodal as well as multimodal security systems presets security and both systems can perform well depending upon the environment in which they were used[40]. Unimodal biometric security system as proposed by [41] was useful for security against the cyberattack within cloud environment. [42] proposed a unimodal and multimodal based model using CNN for person identification. Optimal feature set extraction mechanism was integrated within both unimodal and multimodal based person identification system. [43]self-attention mechanism was used to achieve the weights of both the biometrics and then combined with RESENT residual structure. In the experimental phase, AlexNet[44] and VGG-16[45] network models were used to extract the finger vein and face features which was used as an input in fusion model. Effective results in the form of classification accuracy were achieved with these mechanisms.

The comparative analysis of different models employed for achieving security is presented within table 1.

Table1: Techniques used in previous research work

Author name and year	Biometric	Techniques and algorithms used
Supreetha Gowda, Imran, et al., 2019 [46]	Palm print, iris, signature, voice, face	Multi spectral palm print verification with deep neural network
Nahar et al., 2022[47]	Fingerprint	Delunay Quadrangle method and unique topology code
Benaouda et al., 2022[48]	Hand vein	Independent component analysis (ICA)

Xie & Kumar, 2017[49]	Finger vein	convolutional neural network (CNN), fusion model
Jalilian & Uhl, 2020[50]	Finger vein	convolutional neural network (CNN) and softmax and random forest (RF)
Brown et al., 2021[51]	face, iris, and palm prints	CNN and two layer fusion mechanism
Patil & Agarwal, 2021[52]	Mouse dynamics	fusion techniques, threshold settings, score boosting techniques and static versus dynamic trust models
[53]	Face and fingerprint	Particle Swarm Optimization (PSO)
Abinaya et al., 2022[54]	Speech and key stroke	Fisher Linear Discriminant analysis

3. DISCUSSION

Various machine learning algorithms are used for biometric recognition system. Machine learning algorithms use extraction techniques so that features can be extracted from the biometric data and then using that data to create it into proper format so that it can be classified. Some of the extraction techniques used in machine learning algorithms does not always work well in extracting biometric data, so deep learning techniques are used which gives excellent results in biometric recognition system. In this paper, the recommended deep learning methods is CNN algorithm for identifying person based on face, fingerprints, and iris traits. The most natural trait chosen to identify any person is face and the most accurate and precision nature of identifying human is iris. And the third trait is fingerprints which is added to increase the security, accuracy and reliability of the recommended model.

To carry out the recognition system two fusion levels are one is feature level fusion and the second is score level fusion. The structure of the recommended work is as shown in the figure 3.

Due to the limitations of unimodal biometric authentication system[55], multimodal biometric system for iris, face and fingerprint work was proposed in[56] based on the fusion of matching score level. Using multimodal fusion framework for iris, face and fingerprint images the middle layer semantic features are extracted as semantic features are characterized in a better way[57]. All the previous papers [58][59] and [60]focused on fusion models like decision level, feature level and pixel level fusion. In the traditional ways with these methods extraction of features was easy[61]. But with complex images, and data, these models were not appropriate[62]. In deep learning techniques, CNN has emerged out to show better results [63]. Fusion levels within CNN can be a great asset to enhance the security of multimodal biometric further.

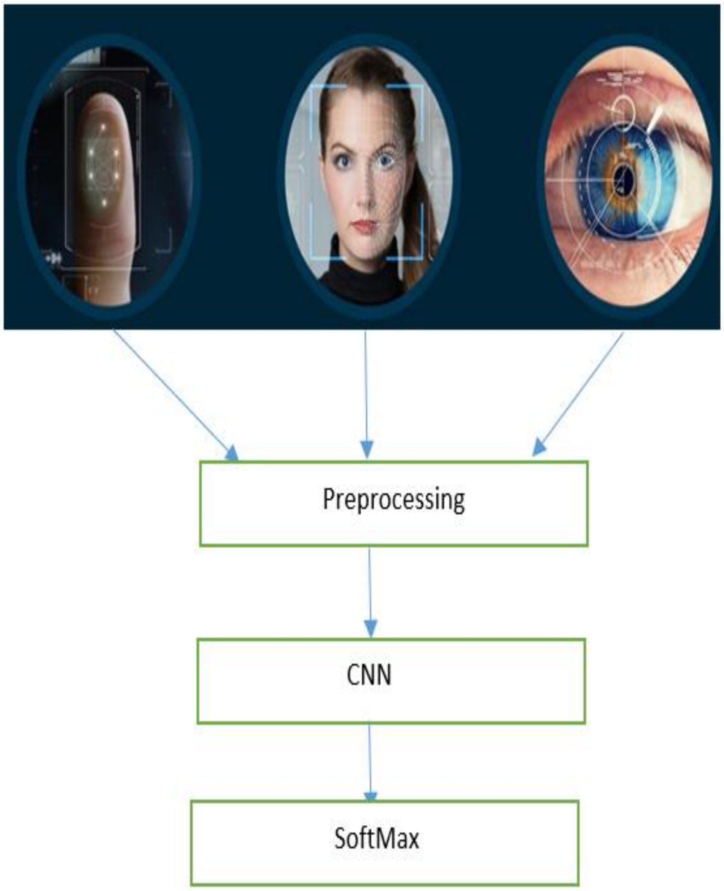

Figure3: Structure of CNN model

We propose a two-layer fusion mechanism where the first fusion happens in convolutional layer and the second fusion happens after pooling. Thus, we can employ two-layer fusion to better extract the features to be used for person identification. The proposed model, four distinct modes will be used that are discussed as under

- The features of face and iris images after convolution are fused which are used as an input for the next layer of iris.
- The features of fingerprints and iris images after convolution are fused which are used as an input for the next layer of finger prints.
- The features of face and fingerprints images after convolution are fused which are used as an input for the next layer of iris.
- The features of iris and iris images after convolution are fused which are used as an input for the next layer of face.

The model for validation that can be used is Alex –Net. For better performance, work can be done on different layers of CNN by naming them as Input-1, conv2d, max_pooling2d, batch normalization, dense. This can be termed as 5-layer network model. In this model input is given for unimodal biometric recognition and respective model is chosen for multimodal biometric recognition system.

The parameters for 5-layer network are shown in table 2.

Layer name	Input	Output
Input-1	16 feature map(32x32)	32 feature maps(32x32)
Conv2d	64x64 gray image	16 feature maps(64x64)
Max_pooling2d	16 feature map(64x64)	16 feature map(32x32)
Batch normalization	32 feature map(16x16)	256x1 vector
Dense	256x1 vector	68x1 vector

Table 2: parameters of 5 layer network model

Feature level fusion is used for fusing the features of face, iris and fingerprints traits and score level fusion is used to calculate the similarity between the three traits. The different datasets are used which is explained in the next section to evaluate the performance of the multimodal biometric system.

Furthermore, multi focal loss function can be integrated at the output layer of CNN for reducing degree of misclassification. [64]explained the concept of focal loss function which had few limitations. For simple images the value of entropy increases and the extraction from complex images become complex[65]. Complex images have low weight factor compared to simple images. This means that in case dataset contains both simple and complex images, only simple images will be used for feature extraction[66]. To overcome the issue, multifocal loss function containing multiple phases of feature extraction can be integrated along with output layer of CNN.

4. Experimental results and analysis

For carrying the experimentation to show whether unimodal or multimodal biometric system is efficient, literature analysis is carried out by working with different set of research [67],[68] and [69]. CMU PIE database is a facial database which contains 1630 images of 65 people with left, right-side image of face. Each image is stored in GIF format of (320x240) pixels. CASIA database is iris database having almost 600 iris images of 110 people. Poly-U database is fingerprint database having fingerprints of 150 people. For carrying out the unimodal biometric recognition system, randomly 8 samples are collected out of which 4 are given for training and 4 are used for testing[70].

In unimodal biometric system, these three datasets were used to perform experiment with different CNN frameworks like AlexNet and VGG-19[71]. The accuracy of unimodal system is shown within table 3.

	Accuracy rates		
Model	**CMU PIE**	**CASIA**	**Poly-U**
AlexNet[72]	0.7102	0.4213	0.5145
VGG-19[73]	0.8543	0.6231	0.5322

Table 3: Results of unimodal biometric system

The accuracy corresponding to all the datasets including CMU PEI, CASIA and Poly-U is minimal for unimodal system. Thus, some modification to existing unimodal system is desired.

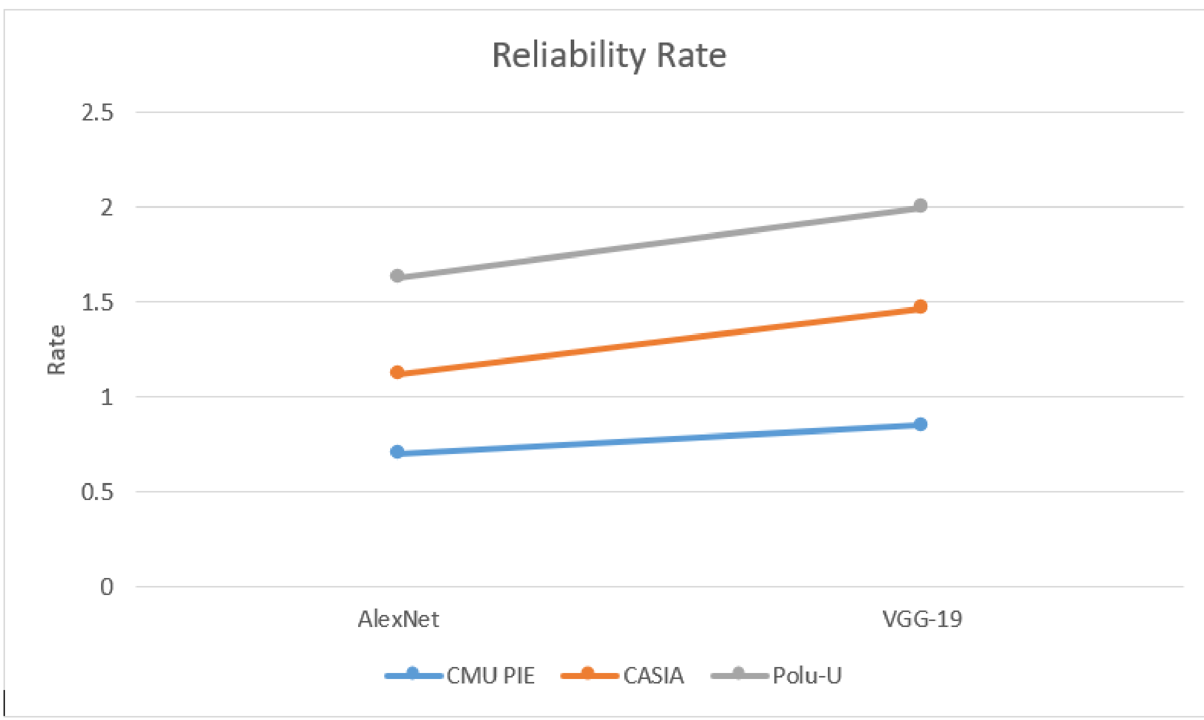

Figure 4: Reliability rate corresponding to VGG-19 and Alex Net on Unimodal systems

The variation of result in terms of AlexNet Model and and VGG-19 for CMU, CASIA and Poly-U is high. The VGG-19 performs better in almost all the cases. The reliability prediction generated through ALexNet and VGG 19 is given within figure 4. It was observed that with Poly-U dataset highest reliability rate was observed. Thus, VGG-19 can be implemented for larger and complex datasets.

The same dataset tested on the multimodal biometric system resulted in higher accuracy as shown in table 4

	Accuracy rates		
Model	**CMU PIE**	**CASIA**	**Poly-U**
AlexNet[74]	0.996	0.9745	0.9644
VGG-19[75]	0.9577	0.9986	0.9994

Table 4: Results of multimodal biometric system

From the above two tables of unimodal and multimodal system for the three datasets it is shown that the lowest accuracy of unimodal system is 85% and the lowest value is 42%. In multimodal system the accuracy rate of AlexNet fusion is 99.6% and VGG-19 is 99.94%. Hence it is shown that by working with three different datasets the multimodal biometric recognition system turned out to be more effective as compared to unimodal biometric system.

The comparative analysis in terms of Multimodal system is presented in figure 5. The reliability in terms of detection rate is better for multimodal system as compared to the unimodal system.

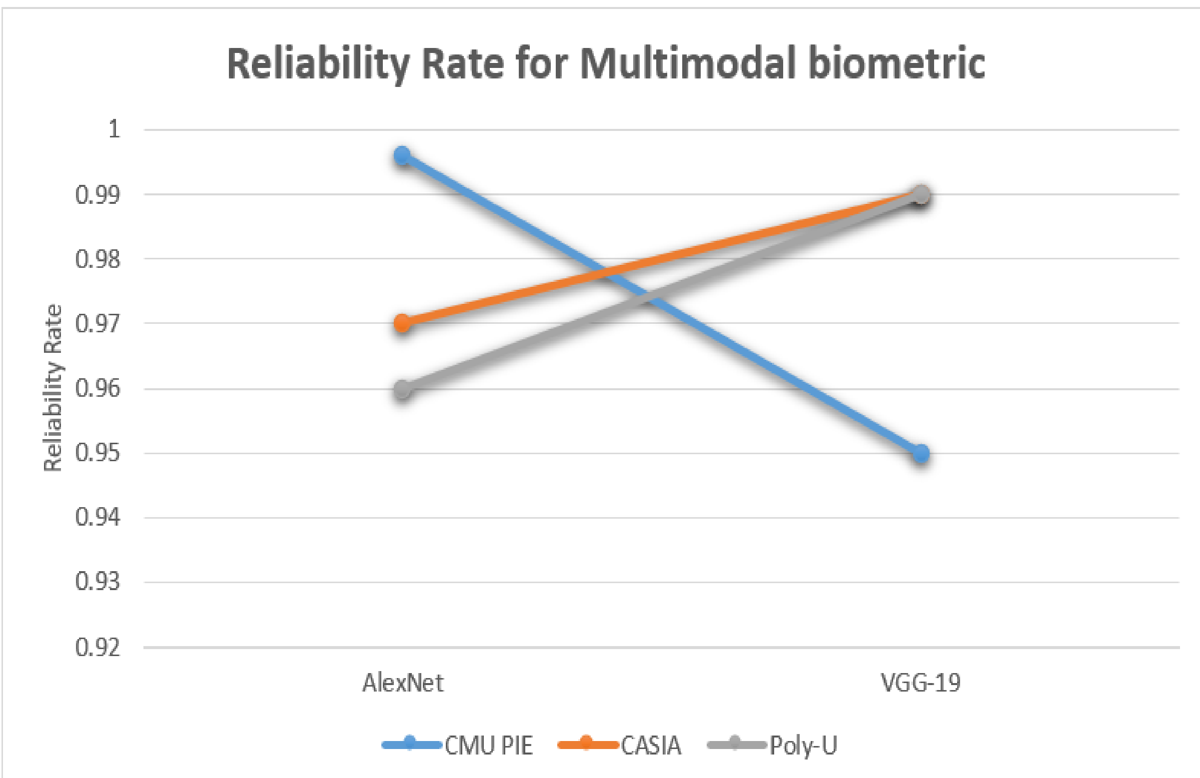

Figure 5: Reliability rate corresponding to Multimodal biometric

The analysis of the reliability rate suggests that for, smaller dataset Alexnet in multimodal biometric performs better but as the size of the dataset increases, VGG 19 performs slightly better as compared to AlexNet. Thus, it is recommended that VGG 19 model should be employed with CNN for multimodal biometric authentication process.

The validation of the result in terms of unimodal and multimodal is given within figure 6. The unimodal and multimodal comparison suggests that the overall result of multimodal biometric is better. However, multimodal biometric is suitable only if size of the dataset is large. CNN model can be accommodated with the VGG model to tackle the complexities of the dataset.

The size of Poly-U dataset is larger as compared CMU and CASIA dataset. Although performance of the CNN with VGG model is high however execution time is significantly higher. To rectify the issue, layers can be combined to form a complex network in the form of deep neural network to handle larger sized images and datasets.

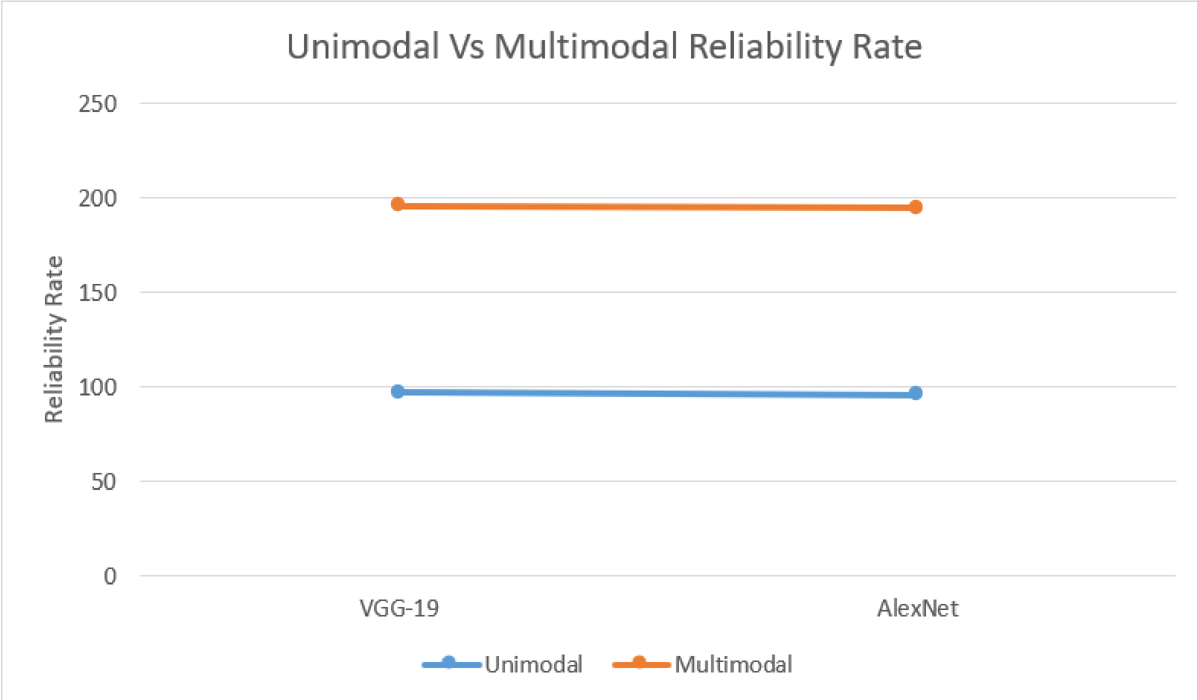

Figure 6: Reliability Rate for Poly U dataset

From the empirical analysis, it is concluded that some modifications to the CNN model integrated with VGG 19 can be accommodated to generate better model for larger as well as smaller datasets. The primary issue with the reliability rate corresponding to CNN is extraction of features that are not significant at the classification layer. This means, degree of misclassification at the output layer is high. For multiple image types within dataset, model in terms of feature shifting is required. Thus, images that are complex can be classified in two different phases. The model of such sought can extract the features from the dataset by skipping complex images and in case, degree of misclassification is high, second phase can be performed to extract features from the complex images.

5. Conclusion

Biometric security systems provide highest form of security as compared to any encryption system. Furthermore, Information and data security against unauthorized access is critical. To this end, this paper discussed the unimodal and multimodal security systems. Both the systems operate well under certain conditions. In less secure environment, multimodal security mechanism will be useful and in more secure regions, unimodal can serve the purpose. Determining the environmental security is difficult, so we need a system suitable for both complex as well as simple environment. Unimodal systems are less secure as discussed within experiment result analysis section. Multimodal security systems are more secured. Both the models however can be modified by the integration of multi focal loss function at the output layer. It was discovered that the CNN model may not perform well in terms of execution time in case, size of the dataset is increased. The deep neural network-based mechanism can be used in that case. Deep neural network-based approach is nothing but the combination of multiple interconnected input, processing, and output layers of CNN. Thus, within deep neural network, multiple CNN model operates. DNN can be used for person identification but the process can be complex. To overcome the issue, multiple phases of feature extraction with the CNN model can be accommodated

Thus, we proposed a two-layer fusion mechanism that can be used on face, iris and fingerprint using CNN. At the output layer, multifocal loss function can be applied to extract the features from both complex as well as simple images. Thus, in future work, multi focal loss function at the output layer of CNN can be applied to reduce degree of misclassification in person identification. The empirical study can be conducted using MATLAB for validation of result. The metrics that can be used for evaluation includes classification accuracy, specificity , sensitivity and F-score.

References

[1] S. Y. Chiou, "Secure method for biometric-based recognition with integrated cryptographic functions," *Biomed Res Int*, vol. 2013, 2013, doi: 10.1155/2013/623815.

[2] G. Bhatnagar, Q. M. J. Wu, and B. Raman, "Biometric Template Security based on Watermarking," *Procedia Comput Sci*, vol. 2, pp. 227–235, 2010, doi: 10.1016/j.procs.2010.11.029.

[3] L. C. O. Tiong, S. T. Kim, and Y. M. Ro, "Multimodal Face Biometrics by Using Convolutional Neural Networks," *Journal of Korea Multimedia Society*, vol. 20, no. 2, pp. 170–178, Feb. 2017, doi: 10.9717/KMMS.2017.20.2.170.

[4] A. Castiglione, K. K. R. Choo, M. Nappi, and F. Narducci, "Biometrics in the Cloud: Challenges and Research Opportunities," *IEEE Cloud Computing*, vol. 4, no. 4, pp. 12–17, 2017, doi: 10.1109/MCC.2017.3791012.

[5] A. Natarajan and N. Shanthi, "A survey on multimodal biometrics authentication and template protection," *Proceedings of IEEE International Conference on Intelligent Computing and Communication for Smart World, I2C2SW 2018*, pp. 64–71, Dec. 2018, doi: 10.1109/I2C2SW45816.2018.8997125.

[6] P. Anitha, K. N. Rao, V. Rajasekhar, and C. H. Krishna, "Security for Biometrics Protection between Watermarking and Visual Cryptography," no. March, pp. 64–71, 2017.

[7] P. P. Paul, M. Gavrilova, and R. Alhajj, "Social Network Analysis for Biometric Template Protection," pp. 217–233, 2015, doi: 10.1007/978-3-319-19003-7_12.

[8] P. Bedi, R. Bansal, and P. Sehgal, "Multimodal Biometric Authentication using PSO based Watermarking," *Procedia Technology*, vol. 4, pp. 612–618, Jan. 2012, doi: 10.1016/J.PROTCY.2012.05.098.

[9] R. H. Farouk, H. Mohsen, · Yasser, and M. Abd El-Latif, "A Proposed Biometric Technique for Improving Iris Recognition," *International Journal of Computational Intelligence Systems 2022 15:1*, vol. 15, no. 1, pp. 1–11, Sep. 2022, doi: 10.1007/S44196-022-00135-Z.

[10] O. Alpar and O. Krejcar, "Biometric keystroke signal preprocessing part I: Signalization, digitization and alteration," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 10350 LNCS, pp. 267–276, 2017, doi: 10.1007/978-3-319-60042-0_31/COVER.

[11] W. Yang, J. Hu, and S. Wang, "A Delaunay Quadrangle-Based Fingerprint Authentication System With Template Protection Using Topology Code for Local Registration and Security Enhancement," *undefined*, vol. 9, no. 7, pp. 1179–1192, 2014, doi: 10.1109/TIFS.2014.2328095.

[12] J. Z. Lim, J. Mountstephens, and J. Teo, "Eye-Tracking Feature Extraction for Biometric Machine Learning," *Front Neurorobot*, vol. 15, Feb. 2022, doi: 10.3389/FNBOT.2021.796895.

[13] Y. Prajna and M. K. Nath, "A Survey of Semantic Segmentation on Biomedical Images Using Deep Learning," *Lecture Notes in Electrical Engineering*, vol. 683, pp. 347–357, 2021, doi: 10.1007/978-981-15-6840-4_27/COVER.

[14] S. Jayanthi Sree and C. Vasanthanayaki, "Texture-Based Fuzzy Connectedness Algorithm for Fetal Ultrasound Image Segmentation for Biometric Measurements," *Advances in Intelligent Systems and Computing*, vol. 1048, pp. 91–103, 2020, doi: 10.1007/978-981-15-0035-0_8/COVER.

[15] Singaraju Jyothi and K.Bhargavi, "A Survey on Threshold Based Segmentation Technique in Image Processing," *Research Gate*, 2014. https://www.researchgate.net/publication/309209325_A_Survey_on_Threshold_Based_Segmentation_Technique_in_Image_Processing (accessed Sep. 22, 2022).

[16] T. Adamek and N. E. O'Connor, "Stopping region-based image segmentation at meaningful partitions," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 4816 LNCS, pp. 15–27, 2007, doi: 10.1007/978-3-540-77051-0_2/COVER.

[17] A. Khwairakpam, R. A. Hazarika, and D. Kandar, "Image Segmentation by Fuzzy Edge Detection and Region Growing Technique," *Lecture Notes in Electrical Engineering*, vol. 556, pp. 51–64, 2019, doi: 10.1007/978-981-13-7091-5_5/COVER.

[18] F. U. Siddiqui and A. Yahya, "Clustering Techniques for Image Segmentation," *Clustering Techniques for Image Segmentation*, 2022, doi: 10.1007/978-3-030-81230-0.

[19] Duaa Hamed AlSaeed, Ahmed Bouridane, and Ali El-Zaart, "(PDF) A novel fast Otsu digital image segmentation method," *Research Gate*, 2016. https://www.researchgate.net/publication/306147920_A_novel_fast_Otsu_digital_image_segmentation_method (accessed Sep. 22, 2022).

[20] S. Vegad and Z. Shah, "Fingerprint Image Classification," *Lecture Notes on Data Engineering and Communications Technologies*, vol. 52, pp. 545–552, 2021, doi: 10.1007/978-981-15-4474-3_59/COVER.

[21] H. Li, F. L. Chung, and S. Wang, "A SVM based classification method for homogeneous data," *Appl Soft Comput*, vol. 36, pp. 228–235, Nov. 2015, doi: 10.1016/J.ASOC.2015.07.027.

[22] G. Guo, H. Wang, D. Bell, Y. Bi, and K. Greer, "KNN model-based approach in classification," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 2888, pp. 986–996, 2003, doi: 10.1007/978-3-540-39964-3_62/COVER.

[23] A. Azri, C. Favre, N. Harbi, J. Darmont, and C. Noûs, "Rumor Classification through a Multimodal Fusion Framework and Ensemble Learning," *Information Systems Frontiers*, vol. 1, pp. 1–16, Aug. 2022, doi: 10.1007/S10796-022-10315-Z/FIGURES/13.

[24] M. O. Oloyede and G. P. Hancke, "Unimodal and Multimodal Biometric Sensing Systems: A Review," *IEEE Access*, vol. 4, pp. 7532–7555, 2016, doi: 10.1109/ACCESS.2016.2614720.

[25] S. Arora, M. P. S. Bhatia, and H. Kukreja, "A Multimodal Biometric System for Secure User Identification Based on Deep Learning," *Advances in Intelligent Systems and Computing*, vol. 1183, pp. 95–103, 2021, doi: 10.1007/978-981-15-5856-6_8/COVER.

[26] P. Shende and Y. Dandawate, "Convolutional neural network-based feature extraction using multimodal for high security application," *Evol Intell*, vol. 14, no. 2, pp. 1023–1033, Jun. 2021, doi: 10.1007/s12065-020-00522-5.

[27] G. A. Fofanov, "On Selection and Extraction of Biometric Features of Human Motor Activity from Data Obtained from Inertial Measurement Units," *Advances in Science, Technology and Innovation*, pp. 369–377, 2021, doi: 10.1007/978-3-030-66218-9_43/COVER.

[28] M. Hammad, Y. Liu, and K. Wang, "Multimodal biometric authentication systems using convolution neural network based on different level fusion of ECG and fingerprint," *IEEE Access*, vol. 7, pp. 25527–25542, 2019, doi: 10.1109/ACCESS.2018.2886573.

[29] E. Cherrat, R. Alaoui, and H. Bouzahir, "Convolutional neural networks approach for multimodal biometric identification system using the fusion of fingerprint, finger-vein and face images," *PeerJ Comput Sci*, vol. 6, no. 1, pp. 1–15, 2020, doi: 10.7717/PEERJ-CS.248.

[30] Z. Sun, Q. Li, Y. Liu, and Y. Zhu, "Opportunities and Challenges for Biometrics," *China's e-Science Blue Book 2020*, pp. 101–125, 2021, doi: 10.1007/978-981-15-8342-1_6.

[31] N. Hezil and A. Boukrouche, "Multimodal biometric recognition using human ear and palmprint," *IET Biom*, vol. 6, no. 5, pp. 351–359, Sep. 2017, doi: 10.1049/IET-BMT.2016.0072.

[32] M. Cheniti, N. E. Boukezzoula, and Z. Akhtar, "Symmetric sum-based biometric score fusion," *IET Biom*, vol. 7, no. 5, pp. 391–395, Sep. 2018, doi: 10.1049/IET-BMT.2017.0015.

[33] B. Ammour, T. Bouden, and L. Boubchir, "Face–iris multi-modal biometric system using multi-resolution Log-Gabor filter with spectral regression kernel discriminant analysis," *IET Biom*, vol. 7, no. 5, pp. 482–489, Sep. 2018, doi: 10.1049/IET-BMT.2017.0251.

[34] Atanda Oladayo, Adeolu Olabode Afolabi, and Falohun A.s, "Development of a Multimodal Biometric Security System using Modified Convolutional Neural Network," *Lautech Journal of Computing and Informatics*, May 2021. https://www.researchgate.net/publication/353558637_Development_of_a_Multimodal_Biometric_Security_System_using_Modified_Convolutional_Neural_Network (accessed Sep. 18, 2022).

[35] T. Y. Lin, P. Goyal, R. Girshick, K. He, and P. Dollar, "Focal Loss for Dense Object Detection," *Proceedings of the IEEE International Conference on Computer Vision*, vol. 2017-October, pp. 2999–3007, Dec. 2017, doi: 10.1109/ICCV.2017.324.

[36] S. K. S. Modak and V. K. Jha, "A Novel Multimodal Biometric Authentication Framework Using Rule-Based ANFIS Based on Hybrid Level Fusion," *Wireless Personal Communications 2022*, pp. 1–21, Sep. 2022, doi: 10.1007/S11277-022-09949-8.

[37] G. Rajakumar and T. Ananth Kumar, "Design of Advanced Security System Using Vein Pattern Recognition and Image Segmentation Techniques," pp. 213–225, 2022, doi: 10.1007/978-981-16-9324-3_12.

[38] L. R. Haddada, B. Dorizzi, and N. Essoukri Ben Amara, "Watermarking signal fusion in multimodal biometrics," *International Image Processing, Applications and Systems Conference, IPAS 2014*, 2019, doi: 10.1109/IPAS.2014.7043280.

[39] S. Barde and A. Agrawal, "Classification of biometrics and implementation strategies," *Advances in Biometrics: Modern Methods and Implementation Strategies*, pp. 307–332, Jan. 2019, doi: 10.1007/978-3-030-30436-2_15/COVER.

[40] A. S. Raju and V. Udayashankara, "A Survey on Unimodal, Multimodal Biometrics and Its Fusion Techniques," *International Journal of Engineering & Technology*, vol. 7, no. 4.36, p. 689, Dec. 2018, doi: 10.14419/IJET.V7I4.36.24224.

[41] J. Dave and M. Gayathri, "Hybrid Encryption Algorithm for Storing Unimodal Biometric Templates in Cloud," *Lecture Notes in Networks and Systems*, vol. 311, pp. 251–266, 2022, doi: 10.1007/978-981-16-5529-6_21/COVER.

[42] G. Sarker and S. Ghosh, "Biometric-based unimodal and multimodal person identification with CNN using optimal filter set," *Innovations in Systems and Software Engineering 2021 17:2*, vol. 17, no. 2, pp. 157–166, Jan. 2021, doi: 10.1007/S11334-020-00381-4.

[43] C. Lu, H. N. Dai, J. Zhou, and H. Wang, "Exploring Self-attention Mechanism of Deep Learning in Cloud Intrusion Detection," *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, vol. 363, pp. 57–73, 2021, doi: 10.1007/978-3-030-69992-5_5/COVER.

[44] F. N. Iandola, S. Han, M. W. Moskewicz, K. Ashraf, W. J. Dally, and K. Keutzer, "SqueezeNet: AlexNet-level accuracy with 50x fewer parameters and <0.5MB model size," Feb. 2016, Accessed: May 18, 2022. [Online]. Available: http://arxiv.org/abs/1602.07360

[45] O. K. Sikha and B. Bharath, "VGG16-random fourier hybrid model for masked face recognition," *Soft comput*, pp. 1–16, Jul. 2022, doi: 10.1007/S00500-022-07289-0/FIGURES/18.

[46] H. D. Supreetha Gowda, M. Imran, and G. H. Kumar, "Multispectral Palmprint Biometric Verification System Using Deep CNN," *Communications in Computer and Information Science*, vol. 1036, pp. 505–513, 2019, doi: 10.1007/978-981-13-9184-2_45/COVER.

[47] P. Nahar, N. S. Chaudhari, and S. K. Tanwani, "Fingerprint classification system using CNN," *Multimedia Tools and Applications 2022 81:17*, vol. 81, no. 17, pp. 24515–24527, Mar. 2022, doi: 10.1007/S11042-022-12294-4.

[48] A. Benaouda, A. H. Mustapha, and S. Benziane, "A CNN Approach for the Identification of Dorsal Veins of the Hand," *Lecture Notes in Networks and Systems*, vol. 413 LNNS, pp. 574–587, 2022, doi: 10.1007/978-3-030-96311-8_54/COVER.

[49] C. Xie and A. Kumar, "Finger vein identification using convolutional neural network and supervised discrete hashing," *Advances in Computer Vision and Pattern Recognition*, vol. PartF1, pp. 109–132, 2017, doi: 10.1007/978-3-319-61657-5_5/COVER.

[50] E. Jalilian and A. Uhl, "Improved CNN-Segmentation-Based Finger Vein Recognition Using Automatically Generated and Fused Training Labels," *Advances in Computer Vision and Pattern Recognition*, pp. 201–223, 2020, doi: 10.1007/978-3-030-27731-4_8/FIGURES/6.

[51] R. Brown, G. Bendiab, S. Shiaeles, and B. Ghita, "A Novel Multimodal Biometric Authentication System Using Machine Learning and Blockchain," *Lecture Notes in Networks and Systems*, vol. 180, pp. 31–46, 2021, doi: 10.1007/978-3-030-64758-2_3/COVER.

[52] P. Patil and S. Agarwal, "Dynamic Multimodal Biometric System," *Communications in Computer and Information Science*, vol. 1376 CCIS, pp. 12–19, 2021, doi: 10.1007/978-981-16-1086-8_2/COVER.

[53] M. Sivarathinabala, S. Abirami, M. Deivamani, and M. Sudharsan, "A Smart Security System Using Multimodal Features from Videos," *Pattern Recognition and Image Analysis 2019 29:1*, vol. 29, no. 1, pp. 89–98, Apr. 2019, doi: 10.1134/S1054661819010218.

[54] R. Abinaya, D. N. V. S. L. S. Indira, and J. N. V. R. Swarup Kumar, "Multimodal Biometric Person Identification System Based on Speech and Keystroke Dynamics," *EAI/Springer Innovations in Communication and Computing*, pp. 285–299, 2022, doi: 10.1007/978-3-030-86165-0_24/COVER.

[55] P. Akulwar and N. A. Vijapur, "Secured Multi Modal Biometric System : A Review," *Proceedings of the 3rd International Conference on I-SMAC IoT in Social, Mobile, Analytics and Cloud, I-SMAC 2019*, pp. 396–403, Dec. 2019, doi: 10.1109/I-SMAC47947.2019.9032628.

[56] Y. Wang, D. Shi, and W. Zhou, "Convolutional Neural Network Approach Based on Multimodal Biometric System with Fusion of Face and Finger Vein Features," *Sensors*, vol. 22, no. 16, p. 6039, Aug. 2022, doi: 10.3390/s22166039.

[57] F. Liang and P. Yu, "The Sensitive Data Feature Extraction Based on Low-Rank Multimodal Fusion," *ACM International Conference Proceeding Series*, pp. 504–511, Oct. 2021, doi: 10.1145/3501409.3501501.

[58] O. Russakovsky *et al.*, "ImageNet Large Scale Visual Recognition Challenge," *Int J Comput Vis*, vol. 115, no. 3, pp. 211–252, Dec. 2015, doi: 10.1007/S11263-015-0816-Y.

[59] S. Veluchamy and L. R. Karlmarx, "System for multimodal biometric recognition based on finger knuckle and finger vein using feature-level fusion and k-support vector machine classifier," *IET Biom*, vol. 6, no. 3, pp. 232–242, May 2017, doi: 10.1049/IET-BMT.2016.0112.

[60] B. Ammour, T. Bouden, and L. Boubchir, "Face–iris multi-modal biometric system using multi-resolution Log-Gabor filter with spectral regression kernel discriminant analysis," *IET Biom*, vol. 7, no. 5, pp. 482–489, Sep. 2018, doi: 10.1049/IET-BMT.2017.0251.

[61] F. Z. el Biach, I. Iala, H. Laanaya, and K. Minaoui, "Efficient balanced focal loss function for manipulated images detection," *5th International Conference on Intelligent Computing in Data Sciences, ICDS 2021*, 2021, doi: 10.1109/ICDS53782.2021.9626750.

[62] Z. Wang and P. Shi, "CAPTCHA Recognition Method Based on CNN with Focal Loss," *Complexity*, vol. 2021, 2021, doi: 10.1155/2021/6641329.

[63] H. Mehraj and A. H. Mir, "Robust Multimodal Biometric System Based on Feature Level Fusion of Optimiseddeepnet Features," *Wireless Personal Communications 2021*, pp. 1–22, Sep. 2021, doi: 10.1007/S11277-021-09075-X.

[64] Z. Wang and P. Shi, "CAPTCHA Recognition Method Based on CNN with Focal Loss," *Complexity*, vol. 2021, 2021, doi: 10.1155/2021/6641329.

[65] I. Kovacs, A. Iosub, M. Topa, A. Buzo, and G. Pelz, "A novel entropy-based sensitivity analysis approach for complex systems," *2016 IEEE Symposium Series on Computational Intelligence, SSCI 2016*, Feb. 2017, doi: 10.1109/SSCI.2016.7849980.

[66] X. Zhao, L. Gao, Z. Chen, B. Zhang, W. Liao, and X. Yang, "An Entropy and MRF Model-Based CNN for Large-Scale Landsat Image Classification," *IEEE Geoscience and Remote Sensing Letters*, vol. 16, no. 7, pp. 1145–1149, Jul. 2019, doi: 10.1109/LGRS.2019.2890996.

[67] H. D. Supreetha Gowda, G. Hemantha Kumar, and M. Imran, "Multimodal biometric recognition system based on nonparametric classifiers," *Lecture Notes in Networks and Systems*, vol. 43, pp. 269–278, 2019, doi: 10.1007/978-981-13-2514-4_23/COVER.

[68] Mahesh, R. Kumar, and K. Sharma, "Biometric System: Unimodal Versus Multibiometric Fusion and Its Current Applications: Review," *Lecture Notes on Data Engineering and Communications Technologies*, vol. 58, pp. 145–152, 2021, doi: 10.1007/978-981-15-9647-6_11/COVER.

[69] M. Pathak and N. Srinivasu, "Performance of multimodal biometric system based on level and method of fusion," *Advances in Computing Applications*, pp. 137–152, Jan. 2017, doi: 10.1007/978-981-10-2630-0_9/COVER.

[70] S. A. El_Rahman, "Multimodal biometric systems based on different fusion levels of ECG and fingerprint using different classifiers," *Soft Computing 2020 24:16*, vol. 24, no. 16, pp. 12599–12632, Jan. 2020, doi: 10.1007/S00500-020-04700-6.

[71] A. Gholami *et al.*, "SqueezeNext: Hardware-aware neural network design," *IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*, vol. 2018-June, pp. 1719–1728, Dec. 2018, doi: 10.1109/CVPRW.2018.00215.

[72] S. C. Yow and A. N. Ali, "Iris Recognition System (IRS) Using Deep Learning Technique," *Journal of Engineering Science*, vol. 15, no. 2, pp. 125–144, 2019, doi: 10.21315/jes2019.15.2.9.

[73] S. Anton, T. Artem, P. Andrey, and K. Igor, “Modification of VGG Neural Network Architecture for Unimodal and Multimodal Biometrics,” *2020 IEEE East-West Design and Test Symposium, EWDTS 2020 - Proceedings*, Sep. 2020, doi: 10.1109/EWDTS50664.2020.9224924.

[74] H. B. Alwan and K. R. Ku-Mahamud, “Cancellable Face Biometrics Template Using AlexNet,” *Communications in Computer and Information Science*, vol. 1174 CCIS, pp. 336–348, 2020, doi: 10.1007/978-3-030-38752-5_27/COVER.

[75] A. Arunraja, V. Mahendran, C. Mukesh, and M. Mahinesh, “Development of Novel Face Recognition Techniques for VGG Model by Using Deep Learning,” pp. 849–861, 2022, doi: 10.1007/978-981-16-9573-5_61.