International Journal of Research in Advanced Engineering and Technology
ISSN: 2455-0876; Impact Factor: RJIF 5.44
Received: 28-07-2020; Accepted: 14-08-2020; Published: 29-08-2020
www.newengineeringjournal.in
Volume 6; Issue 3; 2020; Page No. 20-25

Multimodal biometric authentication system: A survey

Temitope Ayanladun Oyelakun[1], Taye Oladele Aro[2*], Kehinde Moses Aregbesola[3], Awe Yomi[4]
[1] Registry Department, Ladoke Akintola University of Technology, Ogbomoso (LAUTECH), Oyo State, Nigeria
[2, 3] Department of Mathematical and Computing Sciences, KolaDaisi University, Ibadan, Oyo State, Nigeria
[4] Department of Computer Science, University of Lagos, Lagos State, Nigeria

Abstract
Unimodal biometric system competes with several problems like noisy data, spoof attacks, changes in intra-class, restricted degrees of freedom, non-universality, and unacceptable error rates. Several of these limitations can be handled by the application of multimodal biometric systems that integrate multiple sources of information. Multimodal biometric systems involve the fusion of information from many biometrics. These biometric technologies are gaining great attention nowadays due to its possibility to overcome limitations in unimodal biometric systems. This paper presents an overview of multimodal biometrics used in multiple levels of security, it also includes modules of multimodal biometric system, different levels of fusion in multimodal biometrics and related work. The area to improve upon the fusion approach of multimodal technology is suggested as future work for researchers.

Keywords: authentication system, biometric, multi-modal, multi-level

1. Introduction
The necessity for a dependable user verification approach has brought concerns about security and fast advancements in networking, communication and mobility [1]. Biometrics is defined as the science of recognizing an individual based on her physiological or behavioural traits [2]. A Biometric system involves the recognition of an individual based on a feature vector derived from individual biological traits [3]. Biometrics has become the most recent promising technique of recognition [4]. The science of measuring personal Unimodal biometric system competes with several problems like noisy data, spoof attacks, changes in intra-class, restricted degrees of freedom, non-universality, and unacceptable error rates. Several of these limitations can be handled by the application of multimodal biometric systems that integrate multiple sources of information.
Multimodal biometric systems involve the fusion of information from many biometrics. These biometric technologies are gaining great attention nowadays due to its possibility to biometrics is an emerging technology in the identification and authentication of a human being with more reliable and accurate. There are several application domains of biometrics which include healthcare, time and attendance, e-commerce, banking and finance [5]. In biometric technologies, most biometric systems deployed in real-world applications are unimodal [6], which rely on the evidence of a single source of information for authentication such as a single fingerprint or face. These systems have to contend with a variety of problems like noise in sensed data: A fingerprint image with a scar or a voice sample altered by cold is examples of noisy data. Existing biometric systems have to deal with a variety of problems with the usage of single data such as a fingerprint image with a scar of poor illumination of the subject in face recognition [7].
The problem caused by the unimodal biometrics system can be overcome by applying multimodal biometric approaches [8]. Combining two or more biometric systems is a promising solution to provide more security [1]. It eliminates the disadvantages of unimodal biometric systems such as non-universality, noise in sensed data, intra-class variations, distinctiveness, spoof attacks and traditional method of authenticating a human and their identity. The multimodal biometric system has the prospective to be extensively accepted in a very wide range of real-life applications such as in banking security like check cashing, ATM security, credit card transactions and information system security like access to databases via login privileges [9].
In this paper, a general review of a multimodal biometric system for the authentication system was conducted. Different modules and modes involved in the technologies were mentioned and the further area of future research was discussed.

2. Literature Review
Multimodal biometrics can be referred to as the combination of two or more modalities of biometric in a verification or identification system. The features combination could be based on the multiple snapshots of a single fingerprint, faces or palm or any combination of choice [10]. However, the biometric traits of a particular person are normally a biological feature that can either be genetically implied possibly environmentally altered, feature acquired or learned over time that can be used for a verification system. The multi-modal technologies consider the constraint of non- universality since multiple traits ensure sufficient population coverage. Multimodal biometric systems also resolve the problem of spoofing as it concerns many traits or modalities, it would be very difficult for an imposter to spoof or attack multiple traits of the genuine user simultaneously. The schematic diagram of the multi-modal biometric system is shown in Figure 1.

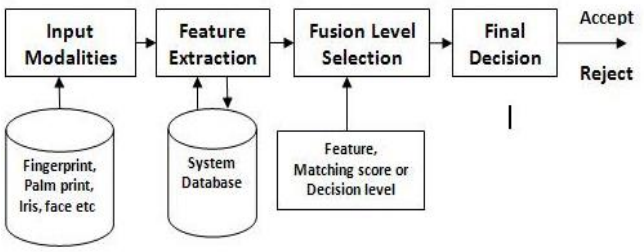

Fig 1: Multimodal Biometric System [9]

2.1 Modules of Multimodal Biometrics

There are four modules in a multi-modal system: sensor module, feature extraction module, matching module and decision-making module respectively [6].

1. **Feature Extraction Module:** At feature extraction, the features are extracted from different modalities after the preprocessing phase to obtain a feature set [9]. These features yield a compact representation of these traits or modalities. These extracted features are then further given to the matching module for comparison.
2. **Matching Module: -** In the matching phase of multi-modal the extracted features from the biological traits are compared against the templates stored in the database [11].
3. **Decision-Making Module:** In this phase, a user is either accepted or rejected based on the matching criteria set in the matching module.
4. **Sensor Module:** At the sensor module, the biometric modalities (biometric data or traits) are first captured and these modalities are provided as inputs for the next phase which is feature extraction [10].

2.2 Multi-Modal Operation Modes

A multimodal biometric system can work in three modes [12]:

1. **Serial Mode:** In serial mode, the biometrics (modals) are considered one after another. The output of one biometric characteristic is used to reduce the number of possible identities before the next characteristic is used. The final decision is accepted depends upon the acceptance of any one of the modal otherwise it is rejected. Figure 1 shows the serial mode in the decision of fusion. A fingerprint modal is considered as an input. If fingerprint accepts the person then a person is treated as genuine otherwise next modal i.e. palmprint is serially taken as an input. If palmprint accepts the person then the person is treated as genuine otherwise final modal. For instance, iris is taken as an input serially. If iris accepts the person then the person is treated as genuine otherwise treated as an imposter.

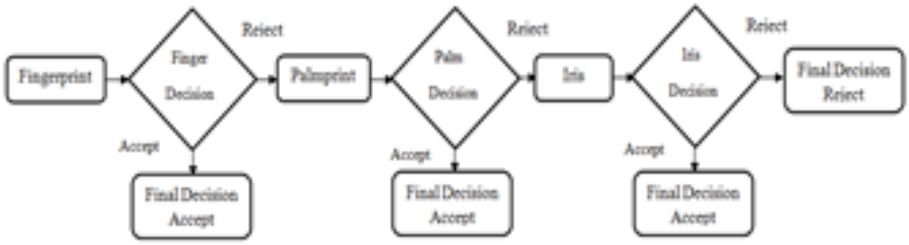

Fig 2: Multimodal in Serial mode [12]

2. **Parallel mode:** In parallel mode, the decisions from individual unimodal verification systems i.e. fingerprint, palmprint and iris are fused using the majority voting rule. In the majority voting rule, the final decision is based on the majority of the decision given by different traits and it works in parallel mode. In parallel mode, all the traits are processed concurrently to produce the final decision of the system. Figure 3 shows a schematic diagram of the parallel mode.

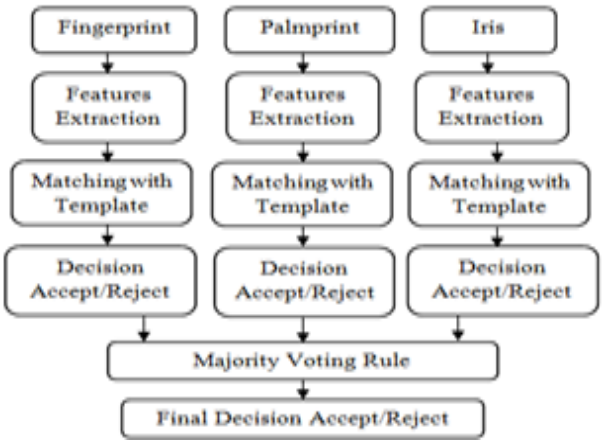

Fig 3: Multimodal in Parallel Mode [13]

3. **Hierarchical Model:** In hierarchical mode, some traits work in parallel mode and some in serial modes of operation as shown in Figure 4. First fingerprint and palmprint verification systems work in parallel mode of operation. The individual decision given by fingerprint and palmprint system is combined using AND fusion rule. In AND rule, a person is accepted if both systems accept the person. If in the parallel mode of fingerprint

and palmprint the person is rejected then the third modal i.e. iris is processed serially. Finally, the decision given by the iris is considered as a final decision. This mode is well suited where a large number of classifiers are applicable.

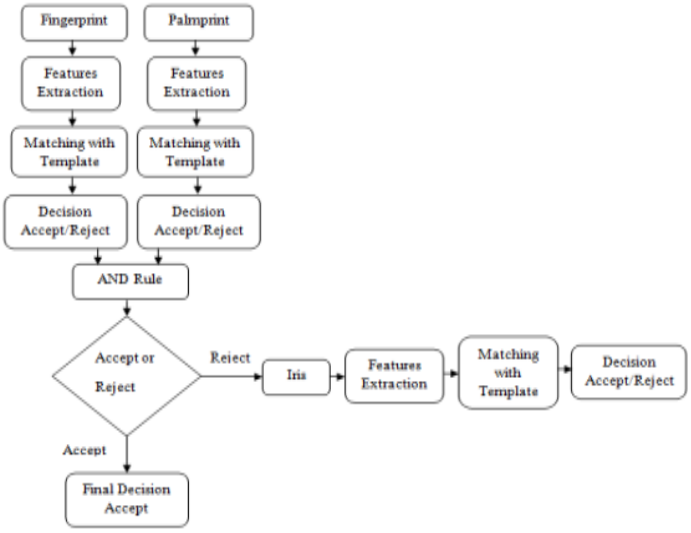

Fig 4: Multimodal in Hierarchical Mode [12]

2.4 Fusion of Feature in Multi-Modal Biometrics

Feature fusion is the process of combining two feature vectors to obtain a single feature vector, which is more discriminative than any of the input feature vectors [14]. The technique involves the combination of the specific extracted features which are stored in a dictionary to obtain a single feature file, which is very informative [15]. The relative analysis of feature fusion approaches determines that different metrics support different user needs. Fusion at the feature level involves the integration of feature sets corresponding to multiple modalities. Different fusion techniques include:

1. **Sensor Level:** Raw data acquired from multiple sensors can be processed and integrated to generate new data from which features can be extracted [16]. For instance, in the case of face biometrics, both 2D texture information and 3D depth (range) information (obtained using two different sensors) may be combined to produce a 3D texture face image which may be subjected to feature extraction and matching.
2. **Feature Level:** The feature sets extracted from multiple data sources can be fused to create a new feature set to represent the individual [17]. The geometric features of the hand, for example, maybe augmented with the eigen-coefficients of the face to construct a new high-dimension feature vector. A feature selection/transformation procedure may be adopted to elicit a minimal feature set from the high-dimensional feature vector.
3. **Match Score Level:** In this case, multiple classifiers output a set of match scores that are combined to produce a single scalar score [18]. As an example, the match scores generated by the face and hand modalities of a user may be combined through the simple sum rule to obtain a new match score which is then used to make the final decision.
4. **Rank Level:** This type of fusion is relevant in identification systems where each classifier associates a rank with every enrolled identity (a higher rank indicating a good match) [11]. Thus, fusion entails consolidating the multiple ranks associated with an identity and determining a new rank that would aid in establishing the final decision. Techniques such as the Borda count may be used to make the final decision.
5. **Decision Level:** When each matcher outputs its class label (accept or reject in a verification system, or the identity of a user in an identification system), a single class label can be obtained by employing techniques like majority voting and behaviour knowledge space [19].

3. Related Work

Shaikh and Kolekar [20] designed a multimodal biometric system using matching score level fusion of palm print and fingerprint. A feature of palm print was extracted with gray level co-occurrence based Harlick features and a feature of the fingerprint was extracted with minutiae-based methods. The matching score with weighted sum rule-based fusion was used to combine the score of a palm print and fingerprint traits. The multimodal system was evaluated employing the publically available IIT Delhi Touchless Palmprint database and FVC 2002 database for fingerprint. The recognition accuracy was improved and when compared with a recognition accuracy of individual traits. The multimodal system outperformed the unimodal with the following results; the accuracy of 99.93 %, and an Equal Error Rate (EER) of 0.0006.

Jagadiswary and Saraswady [21] proposed a fused multimodal system that showed some advantages over unimodal biometric systems like enhanced recognition accuracy, larger feature space to accommodate more subjects and higher security against spoofing. The enhanced multimodal authentication system through feature extraction (fingerprint, retina and finger-vein) and key generation (RSA). The experimental results reveal the performance of multimodal biometrics with RSA recorded the GAR of 95.3% and FAR of 0.01%.

Sasidhar *et al* [22] came up with a framework that assessed the performance of multimodal biometric systems. The study examined relatively large face and fingerprint datasets over a spectrum of normalization and fusion techniques. The

results showed that multimodal biometric systems performed better than uni-modal biometric systems.

Garg, Vig, and Gupta [23] analyzed several techniques of score-level missions in multimodal biometrics. Two modalities were combined to form a single authentication factor so the selection of fusion method. A score level fusion was used to examine the performance of the multimodal biometric system. Two datasets; CASIA and IITD were applied to extract texture features of iris and fingerprint. The texture feature was used to calculate a score for the two modalities and fused using SUM, PRODUCT and MAX methods. The performance evaluation of all three methods was analyzed in terms of FAR, FRR and accuracy.

Sireesha and Reddy [24] developed a multimodal biometric authentication approach. The input image was pre-processed and then offered to feature extraction. A modified Local Binary Pattern (LBP) was effectively utilized, in which the extracted features were furnished to the feature level and score level fusions. In feature level fusion, extracted features were offered to the GSO where the optimal features were shortlisted, and furnished to the optimized neural network which effectively detected the iris and fingerprint image. In score level fusion, extracted features from the iris image were offered to the PSO and the Naive Bayes classifier achieved one score value. The extracted features from the fingerprint image were applied to the AGFS and then one score value was attained. Finally, both the score values were combined. The evaluation was achieved in terms of precision, FAR and FRR.

Devi [25] studied the performance of different fusion techniques and fusion rules in the context of a multimodal biometric system based on the fingerprint, hand geometry, knuckle extraction and speech traits of a user. The experiment result showed that these fusion techniques showed a marked performance, which the serial rule showed comparatively better performance.

Mezai and Hachouf [26] proposed an adaptive multimodal biometric fusion technique. It was based on belief functions and Particle Swarm Optimization (PSO). The fusion was achieved at the score level using belief functions such as Dempster Shafer, Yager, Proportional Conflict Redistribution and Dezert-Smarandache hybrid rules. A hybrid PSO was applied to obtain the best belief function and estimate its parameters. Several experiments were conducted on the BANCA dataset and a comparison between the well-established methods.

Rajagopal and Palaniswamy [28] presented a multimodal multi-feature biometric system for human recognition using palmprint and iris. The features at the feature level fusion were raw biometric data which contains rich information when compared to the decision and matching score level fusion. The dimensionality of information fused at the feature level was reduced by applying Principal Component Analysis (PCA). The developed multimodal system was tested using a created virtual multimodal database using the UPOL iris database and PolyU palmprint database. The results were compared with other multimodal and unimodal approaches. Out of these comparisons, the multimodal multi-feature palmprint iris fusion offers significant improvements in the accuracy of the suggested multimodal biometric system.

Fathima *et al*. [30] developed a multi-modal, multi-sensor-based Person Authentication System (PAS) using the Joint Directors of Laboratories (JDL) fusion model. The study investigated the need for multiple sensors, multiple recognition algorithms and multiple fusion levels and their efficiency for a Person Authentication System (PAS) with face, fingerprint and iris biometrics. The system considered several environmental factors in the design. If one sensor is not functional, others contribute to the system making it fault-tolerant. A multitude of decisions was fused locally to decide the weight for a particular modality. Algorithms were tagged with weights based on their recognition accuracy. Weights are assigned to sensors based on their identification accuracy. Adaptability was incorporated by modifying the weights based on the environmental conditions. All local decisions were then combined to result in a global decision about the person.

Vishi and Yayilgan [31] proposed a new multimodal biometric authentication approach fusing iris and fingerprint traits at a score-level. The study principally explored the fusion of iris and fingerprint biometrics and their potential application as biometric identifiers. The individual comparison scores obtained from the iris and fingerprints were combined at score-level using three score normalization techniques (Min-Max, Z-Score, Hyperbolic Tangent) and fourscore fusion approaches (Minimum Score, Maximum Score Simple Sum and User Weighting). The fused-score was utilized to classify an unknown user into the genuine or impostor.

4. Summary and Discussion

Unimodal biometric techniques contend with various challenges such as noisy data, intra-class variations, restricted degrees of freedom, non-universality, spoof attacks, and unacceptable error rate [32]. Some of these limitations can be addressed by deploying multimodal biometric systems that integrate the evidence presented by multiple sources of information. Different level of fusions such as sensor level, feature level, match level and decision level have been used by researchers in multimodal biometrics. In feature level fusion, the main idea is consolidating the obtained feature set of multiple biometric algorithms into a single feature trait. After the process of normalization and transformation, a reduction is performed. In feature level fusion, features are obtained from different sensors are in the form of dimensions and types. It has a limitation that it is very difficult to fuse an image with a higher dimension feature [33].

There is a need for a feature selection approach to obtain the most relevant features before the fusion process. With the feature selection, the complexity and computational cost of the classifier can be reduced by minimizing the number of features to be used into measurable forms while still maintaining acceptable recognition accuracy [34][35]. Researchers in the past have applied many selection techniques such as subspace techniques like Principal Component Analysis (PCA), Linear Discriminant Analysis (LDA) and Independent Component Analysis (ICA), but the resultant features are not the optimal features [36] [37]. Therefore, it is necessary to introduce a robust feature selection algorithm, a meta-heuristic optimization algorithm is a good candidate for the feature selection method [38].

5. Conclusion

Multimodal biometric systems that involve the combination of information from several biometrics (multiple modalities) are getting more considerations recently due to its ability to

overcome limitations in unimodal biometric systems. These systems are appropriate for high-security applications, most of the developed multi-biometric technologies offer one level of security. This paper presented a literature review on a multimodal biometric system. Some modules and modes involved in the multi-modal techniques were mentioned and also the further area of future work was suggested.

References

1. Nil ES, Chilambuchelvan A. "Multimodal biometric authentication algorithm at score level fusion using hybrid optimization," Wirel. Commun. Technol. 2018; 2(1):1-12.
2. Hamdani OA. "Multimodal Biometrics Based on Identification and Verification System," J. Biom. Biostat. 2013; 04(02):1-8.
3. Kadry S, Smaili M. "Wireless attendance management system based on iris recognition," Sci. Res. Essays. 2010; 5(12):1428-1435.
4. Parmar DN, Mehta BB. "Face Recognition Methods & Applications," Int. J Comput. Technol. Appl. 2013; 4(1):84-86.
5. Kavitha A, Vanaja A. "Analysis of Authentication System in Different," Int. J Latest Trends Eng. Technol, 2017, 13-17.
6. Ross A, Jain AK. "Multimodal Biometrics: An Overview," in European Signal Processing Conference (EUSIPO), 2004, 1221-1224.
7. Yahya F, Nasir H, Kadir K. "Multimodal Biometric Algorithm: A Survey," Biotechnology. 2016; 15(5):119-124.
8. Lathika D, Devaraj BA. "Artificial Neural Network Based Multimodal Biometrics Recognition System," in International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), 2014, 973-978.
9. Arulalan V, Premanand V, Balamurugan G. "An overview on multimodal biometrics," Int. J Appl. Eng. Res. 2015; 10(17):37534-37538.
10. Obed-Emeribe C. "Multimodal Biometric Technology System Framework and E-Commerce in Emerging Markets," Int. J Adv. Comput. Sci. Appl. 2013; 4(7):192-196.
11. Taleb N, Abbes SB. "A Robust Multi-Biometric System with Compact Code for Iris and Face," Int. J Ectrical Eng. Informatics. 2018; 10(1):1-13.
12. Sanjekar PS, Patil JB. "Multimodal biometrics with serial, parallel and hierarchical mode at decision level fusion," Indones. J Electr. Eng. Comput. Sci. 2019; 16(3):1303-1310.
13. Zhang Q, Yin Y, Zhan DC, Peng J. "A novel serial multimodal biometrics framework based on semisupervised learning techniques," IEEE Trans. Inf. Forensics Secur. 2014; 9(10):1681-1694.
14. Sudha D, Ramakrishna M. "Comparative Study of Features Fusion Techniques," in Internavances itional Conference on Recent Advances in Electronics and Communication Technology, 2017, 235-239.
15. Samanta S, Das S. "Technical Review," IETE Tech. Rev. 2010; 27(4):293-307.
16. Al-allaf ONA. "Improving the Performance of Particle Swarm Optimization for Iris Recognition System Using Independent Component Analysis," in International Conference of Artificial Intelligence, 2015, 111-117.
17. Aly OM, Mahmoud TA. "An Adaptive Multimodal Biometrics System using PSO," Int. J Adv. Comput. Sci. Appl. 2013; 4(7):158-165.
18. Muthukumar A, Kasthuri C, Kannan S. "Multimodal Biometric Authentication Using Particle Swarm Optimization Algorithm with Fingerprint and Iris," ICTACT J. Image Video Process. 2012; 2(3):369-374.
19. Kulkarni MM. "Study of Multimodal Biometric System: A Score," Int. J Eng. Res. Technol. 2014; 3(6):1890-1893.
20. Shaikh JA, Kolekar PUD. "Multimodal biometric system based on Matching Score Level Fusion of Palm print And Finger print.," IOSR J Electr. Electron. Eng. 2017; 12(3):27-31.
21. Jagadiswary D, Saraswady D. "Biometric Authentication using Fused Multimodal Biometric," in Procedia - Procedia Computer Science. 2016; 85:109-116.
22. Kakulapati V, Kolikipogu R. "Multimodal Biometric Systems- Study to Improve Accuracy and Performance," Int. J Comput. Sci. Eng. Surv. 2010; 1(2):54-61.
23. Garg SN, Vig R, Gupta S. "Analysis of Different Techniques for Score Level Fusion in Multimodal Biometrics," Int. J Recent Technol. Eng. 2019; 7(6):1233-1238.
24. Sireesha SR, Reddy V. "Two Levels Fusion Based Multimodal Biometric Authentication Using Iris and Fingerprint Modalities," Int. J Intell. Eng. Syst. 2016; 9(3):21-35.
25. Devi NK. "Authentication Using Multimodal Biometric Features," Int. J Comput. Mob. Comput. 2018; 7(1):1-8.
26. Mezai F, Hachouf L. "Adaptive Multimodal Biometric Fusion Algorithm Using Particle Swarm Optimization and Belief Function," in IEEE, 2016, 0-5.
27. Rajagopal G, Palaniswamy R. "Performance Evaluation of Multimodal Multifeature Authentication System Using K NN Classification," Sci. World J, 2015, 1-9.
28. Rajagopal G, Manoharan SK. "Personal Authentication Using Multifeatures Multispectral Palm Print Traits," Sci. World J, 2015.
29. Fathima AA, Vasuhi S, Babu NTN, Vaidehi V, Treesa TM. "Fusion Framework for Multimodal Biometric Person Authentication System," IAENG Int. J. Comput. Sci. 2014; 41(1):1-14.
30. Fathima AA, Vasuhi S, Babu NTN, Vaidehi V, Treesa TM. "Fusion framework for multimodal biometric person authentication system," IAENG Int. J Comput. Sci. 2014; 41(1):18-31.
31. Vishi Y, Yayilgan K. "Multimodal Biometric Authentication using Fingerprint and Iris Recognition in Identity Management," in 9th IEEE International Conference on Intelligent Information Hiding and MultimediaSignal Processing, 2013, 1-8.
32. Dahea HS, Fadewar W. "Multimodal biometric system: A review Multimodal biometric system: A review," Int. J Res. Adv. Eng. Technol. 2018; 4(1):25-31.
33. Prakash SM, Betty P, Sivanarulselvan K. "Fusion of Multimodal Biometrics using Feature and Score Level Fusion," Iinternational J Appl. Inf. Commun. Engineeering. 2016; 2(4):52-56.
34. Miche Y, Bas P, Lendasse A, Jutten C, Simula O. "Advantages of Using Feature Selection Techniques on Steganalysis Schemes," 9th Int. Work. Artif. Neural

Networks, IWANN', 2007, 606-613.
35. Hira ZM, Gillies DF. "A Review of Feature Selection and Feature Extraction Methods Applied on Microarray Data.," Adv. Bioinformatics, 2015, 198-363.
36. Deniz O, Castrillon M, Hernandez M. "Face recognition using independent component analysis and support vector machines," Pattern Recognit. Lett. 2003; 24(13):2153-2157.
37. Bhuiyan A, Liu CH. "On Face Recognition using Gabor Filters," Eng. Technol. 2007; 2(1):51-56.
38. Aghdam MH, Ghasem-Aghaee N, Basiri ME. "Text feature selection using ant colony optimization," Expert Syst. Appl. 2009; (36):6843-6853.