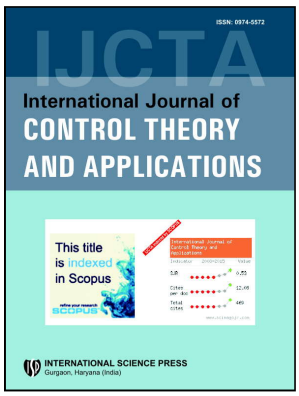

International Journal of Control Theory and Applications

ISSN : 0974-5572

Volume 10 • Number 13 • 2017

Multimodal Authentication System: An Overview

Suneet Narula Garg[1], Renu Vig[2] and Savita Gupta[3]

[1,2] Department of Electronics and Communication Engineering UIET,Punjab University, Chandigarh, Punjab, India, Emails: suneetgarg1979@gmail.com, renuvig@hotmail.com
[3] Department of Computer Science and Engineering UIET,Punjab University, Chandigarh, Punjab, India, Email: savita2k8@yahoo.com

Abstract: The Biometric systems are successfully being used in many diverse fields like identification, forensic, authorization and security systems. A brief overview of various biometric modalities is presented in this survey. Earlier uni-modal biometric systems were used which depended up on the use of a single human characteristic. Such systems had many disadvantages which led to the development of a multimodal biometric system. The multi modal biometric system uses two or more human body characteristics which results in a much higher security and authentication level. The aim of this paper is to think about different methods utilized for execution improvement, security and level of combination in multimodal biometric alongside different difficulties.

Keywords: Biometric system, Multimodal biometrics, fingerprint, Iris, Fusion

1. INTRODUCTION

The requirement for reliable techniques for user authentication has enhanced within the wake of heightened considerations regarding security and fast advancements in communication, quality and networking. A large kind of applications need reliable verification schemes to verify the identity of a person requesting their service. The common ways of authentication is through passwords (knowledge-based security) and ID cards (token based security) which are normally accustomed limit access to a variety of systems. But these systems are liable to be attacked and security is often simply broken. The emergence of bioscience technologies is the replacement of the standard ways because it has addressed the issues that plague these systems. Biometrics is a kind of authentication techniques which place confidence in measurable individual and physiological characteristics which will be mechanically verified. Counting on the appliance context, a biometric system could operate the necessity of technologies for extremely secure identification and private verification is changing into apparent. Biometric-based solutions are providing the data privacy and confidential transactions.

1.1. Biometric System

The biometric system is constitutes of the following main modules as shown in figure 1 [4] - feature extraction module, sensor module, decision making module and matching module. Every module has been described below:

- *Sensor Module*→In this module, interface can incorporate the biometric user sensor which is required to notice the biometric information of user. The biometric data can be transferred and captured into next one module for the feature extraction. The sensor module design influences the several factors like size and cost [5].
- *Module of Feature Extraction*→In this module quality of the biometric information from sensor can be assessed at initial step for more processing. Therefore, generate synoptic but the indicative digital representation of underlying modalities or traits. [9] After the extraction of features which is given as input to match the module for comparison.
- *Matching Module*→In this Matching Module, extracted features compare with in database templates to create the matched score. The matched score can control by quality of provided biometric data. [15] The matched module is used the module of decision making in the created match score that can be deployed to verify the claimed identity.
- *Decision Making Module*→This module can be identified where impostor or real user based on matched scores. It can be used to authenticate the identification of person or offers the rank of entered identity to identify person. The main two mode of the operation in the multi-modal systems comes in parallel mode or serial mode. [11] In the operation of serial mode, several sources of data have not used which the real user goes via stage of authentication process. Therefore recognition time can be increased in the decision of serial mode which is created before taking all the assets. But in terms of the parallel mode recognition has been well performed to acquire the several sources of the information simultaneously [12]. It can be reduced the efficiency of system which causes inconvenience to user. Therefore, these operations modes have their disadvantages and advantages. In this, Study reveals are combined the use of result modes system that offers user convenience and high efficiency.

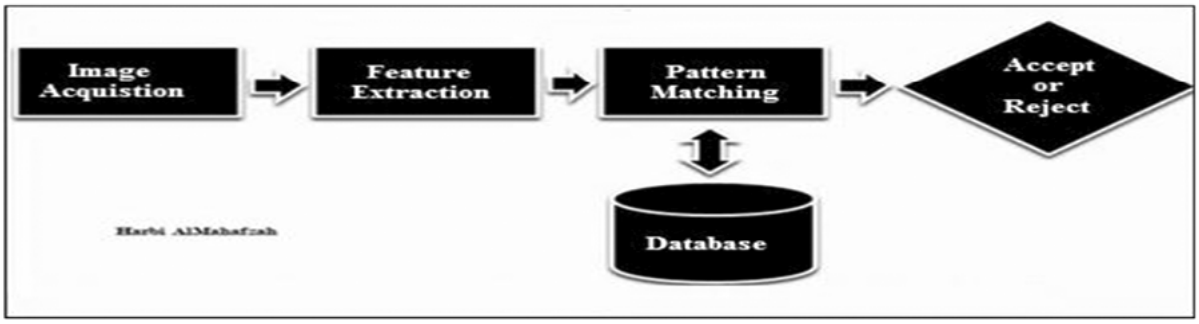

Figure 1: Generic Biometric System [30]

1.2. Comparison Of Various Biometric Technologies

Personal features of a behavioral or physical feature that satisfies seven properties like Acceptability, Performance, Collectability, Permanence, Circumvention, Distinctiveness and Universality may be stated to be a biometric [28]. Universality is referred to all individuals must have biometric feature. Distinctiveness helps to confirm that no two individuals are identical on the basis of biometric traits. Permanence stands for biometric features of a person must vary sufficiently with time period. Collection is referred like it must be measured easily without taking any problem to real user. Performance correlates to speed, technology accuracy in use. Acceptability stands for a meaning that user accepts it without any [22] problem with collection of Circumvention and the biometric that correlates with ease with how the biometric features may be obtained.

Vivid comparisons of how the various biometric identifiers in the concepts of 7 features are displayed in Table-1.

Table 1
Comparison of various biometric technologies

	Biometric Parameters						
Biometrics	*Universality*	*Uniqueness*	*Permanence*	*Collectability*	*Performance*	*Acceptability*	*Circumvention*
Face	High	Low	Med	High	Low	High	Low
Finger Print	Med	High	High	Med	High	Med	High
Hand Geometry	Med	Med	Med	High	Med	Med	Med
Iris	High	High	High	Med	High	Low	High
Signature	Low	Low	Low	High	Low	High	Low
Voice Print	Med	Low	Med	Low	Low	High	Low
F. Thermo gram	High	High	Low	High	Med	High	High
Retinal Scan	High	High	Med	Low	High	Low	High
Iris recognition	High	Med	Med	Med	High	Med	Low

In this 'High' denotes a specific biometric identifier that is giving well performance, on the contrary weak performance obtained [30] from the evaluation procedure is denoted as 'low' and average performance obtained from the procedure is denoted as 'medium'. When is proved for all biometric features contains benefits and disadvantages in all the aspects. Therefore on the basis of above said restrictions it can be said that this is good to use more than one biometric identifier. The weakness and strength of various biometric integrities [32] have provided. Therefore on selecting from the various combination of the biometric identification might be easy with the regular use of the provided table that will help user to develop a huge performance of biometric identification as well as authentication and an accurate identification.

Table 2
Weakness and Strength of individual Biometric Identities

Biometric-Identifier	*Strengths*	*Weakness*
Finger- scan	easy to use, High level of accuracy, flexibility	unable to enroll some percentage of users, Performance can deteriorate the over time
Facial- scan	Able to operate without user cooperation	Changes in physiological feature reduce matching accuracy
Signature- scan	Resistant to imposters	Lead to increased error rates
Hand- scan	Reliable core technology, stable physiological characteristic.	Limited accuracy
Retina- scan	Highly accurate	Difficult to use
Iris-scan	Resistance to false matching	Difficult of use

1.3. Limitations In Biometric System

There are two essential sorts of acknowledgment blunders in biometrics: false acknowledges rate (FAR) and the false reject rate (FRR). A False accept rate happens when an unmatched arrangement of biometric information is acknowledged wrongly as a match by the framework. A False reject rate happens when a coordinating arrangement of biometric information is wrongly dismisses by the framework. At the point when you attempt to overcome one of the mistakes by fluctuating the edge, the other blunder rate increments naturally. Hence equalization is to be found, with a choice edge that can be indicated to either minimize the danger of FAR, or to minimize the danger of FRR [11]. Different issues are:

- Having Noise in detected information.
- Intra-class variety in the information.
- Inter-class likeness in the information.
- Spoof assaults.

To defeat these issues multimodal biometrics framework was presented.

2. MULTI-MODAL BIOMETRIC SYSTEM

Multi-modal biometric is that type of system which combines all results attained from more than one biometric feature for the use of personal identification. Multi-modal biometric systems have been more reliable due to the fact that various open biometric modalities have being in use. With use of more biometric modalities, [4] it has resulted in secure and high accurate biometric identification system, with the unimodal biometric system will not be able to give correct identification for non-universality. For an example, some percentages of the people may wear; cut prints, finger-print where the biometric can reduce the incorrect results. In Multi-modal biometric Systems, one failure of the technology cannot effect on the individual identification and technologies have been successfully used. Therefore spoofing is reduced to a greater extent and will improve the efficiency of whole system. The failure minimization is used to enroll the rate in multi-modal evaluation can be significant and that may be one of main merits of prevailing system.

2.1. Fusion Level

Multi-modal system can be combined in several different levels as described below:

Sensor level: From the multiple sensors raw data acquired is processed and combined in order to get new data so that the features can be extracted from it. For instance, in face biometrics, the 3D depth and 2D texture data (which are acquired using two totally different sensors) are amalgamated to get a 3D texture image of the face that might then be subjected to feature extraction and matching

Feature level: From multiple information sources the feature sets which are extracted are often amalgamated to make a new feature set to represent the individual. The geometric feature of the hand, for instance, is also increased with the eigen-coefficients of the face so as to construct a replacement high-dimension feature vector. A feature selection/transformation procedure is also adopted to elicit a stripped-down feature set from the high-dimensional feature vector.

Match score level: During this case, multiple classifiers output a group of match scores that are coalesced to get one scalar score. As an illustration, the match scores generated by the hand and face modalities of a user are fused using a normal add rule order to get a brand new match score. With the help of this score the final decision is made. *Rank level:* An identification system where every classifier is accomplice a rank with each enrolled identity this type of fusion is applicable. So the fusion involve in developing the multiple ranks combine with the identity and concluding in making new rank that will help in making the final decision. Borda count is one of the techniques which may be used while making the decision.

Decision level: In this type of fusion each matcher matched with its own class label it means either accept or reject in an identification system. In this a single class label may be originated by using techniques like behaviour knowledge space, majority voting, etc.

2.2. Methods for Multimodal Fusion

The methods of fusion are broadly categories in three ways: estimation-based, rule-based and classification based methods. On the basis of basic nature these methods are categorized and it genetically means distribution

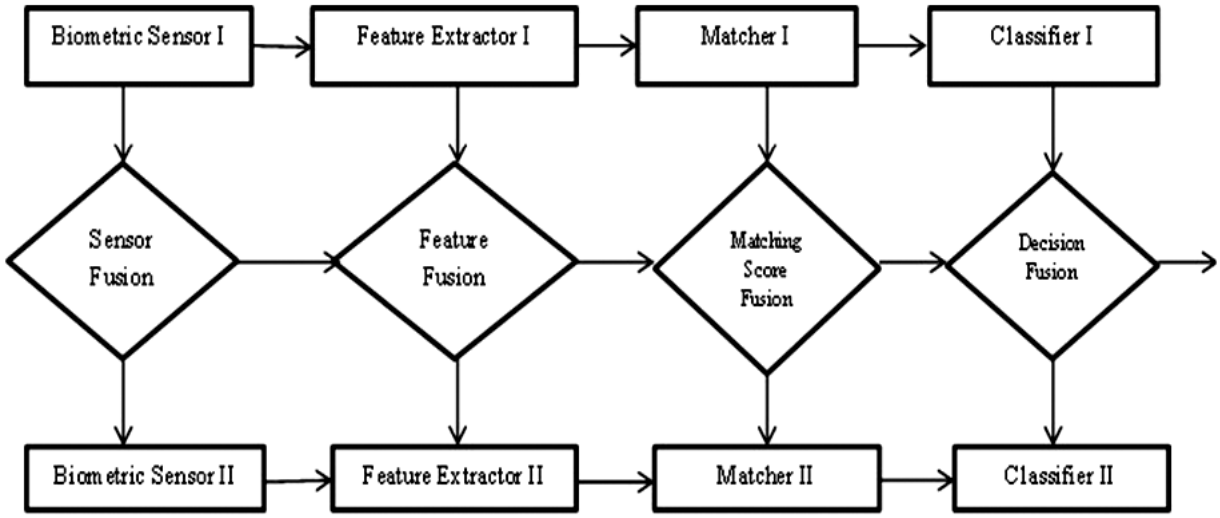

Figure2: LEVELS of fusion

of problem space i.e. by using estimation-based methods the estimating parameter problem is resolved. Similarly by using rule based or classification based method the problem of retrieving the decision on the basis of certain observation can be resolved. But if the observation collected from various modalities then the fusion of observation score would be required by the method before making or estimating the classification decision.

2.2.1. Rule-based fusion methods

For fusing the multimodal information this method comprises of collection of basic rules. It includes statistical rule based method like MAX, MIN, linear weighted fusion (i.e. sum and product), majority voting, AND, OR. For the specific application perspective the customer defined rules are made. If between different modalities the temporal alignment quality is good then the rule based scheme performs well.

2.2.2. Classification-based fusion methods

To classify the multimodal observation into one pre-defined class's different classification technique is used in this method. The method comprises in this category are bayesian inference, dynamic bayesian networks, maximum entropy model, support vector machine, dempster–shafer theory and neural networks. From the perceptive of machine learning these methods can be further classified as discriminative and generative model. So basically generative models are dynamic Bayesian and Bayesian inference networks where as discriminative models are neural networks and support vector machine.

2.2.3. Estimation-based fusion methods

The extended Kalman filter, particle filter and Kalman filter fusion methods are included in estimation category. Based on multimodal data in order to deduce the state of moving object these methods are used primarily. For example, for the task of object tracking i.e. to deduce the position of the object different modalities like vedio and audio are fused.

3. RELATED WORK

Peng, et al. [4] proposed the multimodal biometrics that offers the score-level fusion method depend upon the triangle norm with their four finger traits, with two or three combined in methods. *Sepasian et al.* [5] proposed three stage method for unique finger impression distinguishing proof and upgrade utilizing CLAHE (Contract

Limited Adaptive Histogram Equalization) alongside clasp limit, standard deviation and sliding neighbourhood amid handling of unique finger impression picture. Firstly, CLAHE with clasp cutoff is connected to build the differentiation of little tiles existing in unique finger impression picture and consolidating the neighboring tiles utilizing a bilinear interjection to kill the misleadingly instigated limits. Besides, picture is deteriorated into a variety of particular pieces and the segregation of square is acquired by processing the standard deviation of lattice components to expel the picture foundation and get the limits for district of interest. In conclusion, by utilizing a slide neighborhood preparing, an improvement of picture is gotten by clearing up the Minutiae in every particular pixel, the procedure alluded to as diminishing. *Kumari and Aruna* [6] proposed the biometrics long touted as useful tool to solve authentication and identification issues for forensics, immigration and customs, computer and physical security. *Ujwalla, et al.* [8] aimed on fusing the two biometric features that names Fingerprint and Iris at the feature level into the frequency domain. Multimodal biometric systems are made by many biometric features which the conclusion in higher accuracy and dependent to recognize subjects

Gottschlich et al.[10] states that Gabor channel assume an essential part in improvement of different kind of pictures and extraction of Gabor elements. With the end goal of improved bended structures in uproarious pictures, creator presented bended Gabor channels which adjust their shape to the course of stream. In this, creator connected bended Gabor channel to bended edge and valley structure of low quality unique mark picture. Firstly, two introduction field gauge strategies are consolidated so as to get more strong assessment for loud picture. Next, bended districts are made by taking after the admiration ive nearby introduction which is utilized to appraise the neighborhood edge recurrence. In conclusion, bended Gabor channel are characterized in light of bended area and after that connected for upgrade of low-quality. *Houda et al.* [11] unified the viewpoint to express the singular points which define topological structure and hugely influence orientation to use the Gabor basis functions. At the end of points, we have been provided into the classes by technique of Poincare index to the Fingerprint classification .*Teddy et al.* [13] investigated the research performance from three methods for the multimodal biometric recognition of combined fingerprints and iris: weighted rule, classical sum rule, and fuzzy logic method.

Shanthini and Swamynathan[14] introduced that the message conveyed between the client are encoded by cancellable cryptographic key produced from unique mark components of collectors by applying hereditary administrators and after that inserted inside the mixed face biometric of sender utilizing steganography strategy. The collector first unscrambles the facial picture of sender and after that isolates the facial picture and scrambled information. Collector checks the sender utilizing Eigen face acknowledgment calculation and on the off chance that it is the honest to goodness sender then decode the figure content with the key created utilizing beneficiaries unique finger impression biometrics. Along these lines, the recipient guarantees the validity of the sender and information. *Kalra and Lamba* [15] proposed Multi biometric systems can be imitated unification of two unimodal biometric systems. These systems can be predicted to sound with the residence of several independent segments of evidence. However, it is signed in unparallel levels of the security. It is proposed to blend the Iris recognition technique and multimodal fingerprint.

Binsu et al.[16] secured assault utilizing cryptography techniques, which worry with encryption of information. Encryption is the procedure of encoding message in a manner that aggressor can't read it, yet approved gathering can. To avoid assault, imperceptible watermarking strategy is utilized with cryptography. The biometric attribute is changed utilizing imperceptible watermark data and after that secured by cryptography. The encryption calculation is very reasonable for interactive media and additionally for content information. The format is made safely utilizing encryption lastly put away as a part of database.

Ujwalla, et al. [18] proposed the development of iris fusion and fingerprint system that can be utilized the Hamming Distance which based on matcher to give larger accuracy than different unimodal system

Malhotra and Kant [19] utilized peculiarity of iris example, iris acknowledgment frameworks got a one of a kind mapping for every individual. Distinguishing proof of individual is conceivable by applying coordinating calculation. In this, Daugman s elastic sheet modular is utilized for iris standardization and unwrapping, and for

examination of various elements recognition administrator is performed, highlights extricated are encoded utilizing Haar wavelets and hamming separation as a coordinated calculation is utilized for characterization. This edge identification calculation Canny is observed to be the best one to remove the vast majority of iris surface. The achievement rate is 81% and false Accept rate is 9% and false Reject rate is 10%. *Ghayoumi M. et al.*[20] given precise, solid examples and calculation for individual affirmation and acknowledgment and its answers broadly utilized as a part of government, military and commercial ventures. Recognized that unimodal biometric endure with numerous issues, for example, uproarious information and parody assault, a few issues can be understood by multimodal biometric framework that utilizations two or more biometric modalities and different techniques and coordination methodologies can be connected to consolidate the data in multimodal framework.

Dinakardas et al. [21] projected the multimodal face recognition system which the results from both Fisher face projections, Principal Component Analysis, LBP feature extraction and minutia extraction on individual biometric traits . The identification system is used iris and fingerprint of person to recognize the person. *Bharadi, et al.* [23] proposed the KNN classifier which is used for the multi-instance iris recognition and unimodal fingerprint recognition. In this paper, feature vector of the fingerprint and iris are combined with the use of decision fusion technique. *Kalra and Lamba*[24] proposed consolidating of multimodal unique mark and Iris acknowledgment system. In this, creator initially extricated the elements from both and after that level combination of separated elements lastly connected an encryption method to the melded yield.

Danil et al. [26] dissected the execution got by multimodal biometric framework that join the element extraction of iris and unique mark unimodal biometric and score level combination between these procedures in of observations with their individual modalities of test subject to give the sparse representations. Therefore, it takes the account correlations during the couples of information between the biometric modalities.

4. CONCLUSION

We have concentrated on the past studies done by different creators and their strategies. CLAHE with clasp limit give better complexity of little tiles and gabor channel can be utilized to enhance coordinating execution. Cancellable cryptographic and imperceptible watermarking procedures can be utilized to secure biometric layout. Watchful edge recognition calculation can separate the majority of the iris surface with 81% achievement rate.

To choose from all modalities and a select particular trait or traits which will be used in a biometric security system will depend on the actual application. As compared to other modalities like face, voice, palm print, hand geometry, DNA or signature, the most easy to conduct, has least error rate, requires less equipment which is not very costly either and it gives immediate output. [23] There are many limitations of a uni-modal biometric system which can be overcome using a multimodal system. Finger print and iris recognition combined together with any security technique discussed above can prove to be very accurate. There are many ways of combining different information at different levels to improve the performance, deter spoofing and reduce error rates. A strategy of combining various classifiers can be used. [26] The soft biometric features can be used in combination with fingerprint and iris. Many different fusion, rank level or any other level scenarios are possible in a multi biometric authentication system, the most common one as observed is matching score level fusion.

However, various multi-modal systems are available to authenticate the person, choosing the optimal fusion level, fixed modal, and redundant in the expressed features that are few of short timing face view in the designing of multi-modal biometric system which requires to be noticed. The individual methods have been possible into the multi-modal systems, integration strategies and perfect fusion levels that are selected to consolidate the data.

REFERENCES

[1] Steve Zhou and Junping Sun, "A Novel Approach for Code Match in Iris Recognition," 2013 IEEE/ACIS 12th International Conference on Computer and Information Science (ICIS), pp. 123-128, 16-20June, 2013.

[2] Gawande, Ujwalla, Mukesh Zaveri, and Avichal Kapur. "Bimodal biometric system: feature level fusion of iris and fingerprint." Biometric Technology Today 2013.

[3] Benaliouche, Houda, and Mohamed Touahria."Comparative study of multimodal biometric recognition by fusion of iris and fingerprint." The Scientific World Journal 2014 (2014).

[4] Peng, Jialiang, et al. "Multimodal biometricauthentication based on score level fusion of finger biometrics." Optik-International Journal for Light and Electron Optics 125.23 (2014): 6891-6897.

[5] Sepasian, M., Balachandran, W., & Mares, C. (2008, October 22-24). Image Enhancement for Fingerprint Minutiae-Based Algorithms Using CLAHE, Standard Deviation Analysis and Sliding Neighborhood. Proceedings of the World Congress on Engineering and Computer Science: WCECS 2008, pp. 1-6, San Francisco, USA, ISBN: 987-988-98671-0-2.

[6] KUMARI, P. ARUNA, AND G. JAYA SUMA, "A NOVEL MULTIMODAL BIOMETRIC SCHEME FOR PERSONAL AUTHENTICATION." International Journal of Research in Engineering & Technology (IMPACT: IJRET) ISSN(E): 2321-8843; ISSN(P): 2347-4599 Vol. 2, Issue 2, Feb 2014, 55-66

[7] Mishra, A. ,. "Multimodal Biometrics it is: Need for Future System. " International Journals of Computer Application, 3(4), pp. 28-33, ISSN: 0975-8887, DOI: 10.5120/720-1012.

[8] Gawande, Ujwalla, "A high speed frequency based multimodal biometric system using iris and fingerprint." International Journal on Advanced Computer Engineering and Communication Technology 1.2 (2012): 66-73.

[9] Shekhar, Shashi, et al. "Joint sparse representation for robust multimodal biometrics recognition." Pattern Analysis and Machine Intelligence, IEEE Transactions on 36.1 (2014): 113-126.

[10] Gottschlich, C., (2012, April). Curved Gabor Filters for Fingerprint Image Enhancement. IEEE Transactions on Image Processing, 21(4), pp. 2220-2227, DOI: 10.1109/TIP.2011.2170696.

[11] Benaliouche, Houda, and Mohamed Touahria. "Comparative study of multimodal biometric recognition by fusion of iris and fingerprint." The Scientific World Journal 2014 (2014).

[12] Gudavalli, M., Babu, A. V., Raju, S. V., & Kumar, D. S. (2012, March 26-29). Multimodal Biometrics–Sources, Architecture and Fusion Techniques: An Overview, IEEE: International Symposium on Biometrics and Security Technologies, pp. 27-34, Taipei, ISBN: 978-0-7695-4696-4/12, DOI: 10.1109/ISBAST.2012.24

[13] Ko, Teddy. "Multimodal biometric identification for large user population using fingerprint, face and iris recognition." Applied Imagery and Pattern Recognition Workshop, 2005. Proceedings. 34th. IEEE, 2005.

[14] Shanthini, B., & Swamynathan, S. (2012). Multimodal Biometric-based Secured Authentication System using Steganography. Journal of Computer Science, 8 (7), pp. 1012-1021, 2012, ISSN 1549-3636.

[15] Sakshi Kalra, Anil Lamba "Improving Performance by combining Fingerprint and Iris in Multimodal Biometric" International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 4522-4525.

[16] Kovoor, B. C., Supriya, M. H., & Jacob, P. K. (2013, September). Effectiveness of Feature Detection Operators on the Performance of IRIS Biometric Recognition System. IJNSA: International Journal of Network Security and its Applications, 5(5), pp. 73-82, DOI: 10.521/ijnsa.2013.5506

[17] Bimi Jain, Dr. M. K. Gupta and Prof. Jyoti Bharti, (2012), "Efficient Iris Recognition Algorithm Using Method Of Moments", International Journal of Artificial Intelligence & Applications, vol. 3, pp. 93- 105.

[18] Gawande, Ujwalla, et al. "Fingerprint-Iris Fusion Based Multimodal Biometric System Using Single Hamming Distance Matcher." e-ISSN: 2278-7461, p-ISSN: 2319-6491 Volume 2, Issue 4 (February 2013) PP: 54-61

[19] Malhotra, S., & Verma, C. K. (2013, May). A novel approach for securing Biometric System Template,International Journal of Advanced Research in Computer Science and Software Engineering, 3(5), pp. 397-403, ISSN: 2277-128X.

[20] Ghayoumi, Mehdi. "A review of multimodal biometric systems: Fusion methods and their applications." Computer and Information Science (ICIS), 2015 IEEE/ACIS 14th International Conference on. IEEE, 2015.

[21] Dinakardas, C., S. Perumal Sankar, and Nivia George. "A multimodal performance evaluation on two different models based on face, fingerprint and iris templates." Emerging Trends in VLSI, Embedded System, Nano Electronics and Telecommunication System (ICEVENT), 2013 International Conference on. IEEE, 2013.

[22] Baker, S., Bowyer, K. W., Flynn, P. J., and Phillips, P. J. (2012). Template aging in iris biometrics: Evidence of increased false reject rate in ICE 2006. In Burge, M. and Bowyer, K. W., editors, Handbook of Iris Recognition. Springer.

[23] Bharadi, Vinayak Ashok, Bhavesh Pandya, and Bhushan Nemade. "Multimodal biometric recognition using iris & fingerprint: By texture feature extraction using hybrid wavelets." Confluence The Next Generation Information Technology Summit (Confluence), 2014 5th International Conference-. IEEE, 2014.

[24] Kalra, S., & Lamba, A. (2014). A Survey on Multimodal Biometric. International Journal of Computer Scienceand Information Technology, 59 (2), pp. 2148-2151, ISSN: 0975-9646

[25] Lahane, P. U., and S. R. Ganorkar. "Fusion of Iris & Fingerprint Biometric for Security Purpose." International Journal of Scientific & Engineering Research3.8 (2012): 1-5.

[26] Daniel, D. M., Mihaela C., & Romulus, T. (2014). Combining Features Extraction and Score Level Fusion in aMultimodal Biometric System, IEEE, DOI: 978-1-4799-7267-8/14.