International Journal of Current Advanced Research
ISSN: O: 2319-6475, ISSN: P: 2319 – 6505, Impact Factor: SJIF: 5.995
Available Online at www.journalijcar.org
Volume 6; Issue 7; July 2017; Page No. 4487-4492
DOI: http://dx.doi.org/10.24327/ijcar.2017.4492.0524

Research Article

BIOMETRIC BASED AUTHENTICATION SYSTEM: A SURVEY

Om Prakash Sharma[1] and Jitendra Sheetlani*[2]

[1]Sri Satya Sai University of Technology & Medical Sciences Opp.Oilfed Plant, Indore-Bhopal Road, Sehore (M.P)
[2]Sri Satya Sai University of Technology & Medical Sciences, Sehore (M.P)

A R T I C L E I N F O

Article History:

Received 8th April, 2017
Received in revised form 10th May, 2017 Accepted 25th June, 2017
Published online 28th July, 2017

Key words:

Biometric, unimodal, multimodal, feature-extraction, matcher module, fusion

A B S T R A C T

A Biometric recognition system provides automatic identification of an individual based on a unique feature. Among the various biometric technologies, multimodal based authentication has gain more popularity for its accuracy and efficiency as recognition system. Unlike unimodal, multimodal biometric system incorporates two or more individual biometric trait, as a result the overall system recognition rate increases significantly. This is true even in the presence of erroneous, incomplete or missing data. This paper gives an overview of some the popular and novel research directions that have recently emerged in the biometric security domain.

INTRODUCTION

In this age of automation, struggling to thrive for robust and efficient computational systems, there is an ever-growing need to authenticate and identify individuals. Authentication of a person to recognize one identity is an important problem in the society [1]. The problem of recognizing or authenticating users has been overcome by using various technologies.

The Biometrics-based authentication and identification techniques have emerge as one the most promising and reliable method [2]. Biometrics requires that the person to be identified or verified to be physically present at the point-of-identification and relies on "something what you are or you posses" to provide enhance security in terms of increased efficiency, and improved accuracy.

Biometric system overcomes some of the limitations of traditional way of authenticating the person which uses technologies based on ID cards and PIN: ID cards that may be lost, stolen, forgotten, or misplaced whereas PIN may be forgotten or guessed by the third person (unauthorized user). Apart from these, the traditional identification methods are unable to differentiate between an authorized person and an imposter's who masquerade as authorized person [3].

Automated biometrics deals with physiological or behavioral characteristics such as fingerprints, signature, palm-print, iris, hand, voice and face that can be used to authenticate a person's identity or establish an identity from a database.

Corresponding author:* **Jitendra Sheetlani
Sri Satya Sai University of Technology & Medical Sciences, Sehore (M.P)

The rapid progress and advancement in computational devices, electronic goods and e-commerce market, there is a growing need to authenticate identity of a person for secure login and transaction processing [3]. Thus biometrics based authentication is getting more and more popularity world-wide.

Biometric System

The term “Biometrics” is derived from the Greek words “bio” which means life and the “metrics” means to measure. It refers to identifying an individual based on his or her unique characteristics. Any human physiological (such as iris, fingerprint, palm etc) or behavioral (such as signature, writing style, gait etc) features can be used for personal identification as long as it satisfies the attributes like universality, uniqueness, permanence, collectability and acceptability [4].

Operation

A biometric system is designed and implemented using either single trait or multiple traits. Systems using one trait are called unimodal biometric systems while those using more than one trait are called multimodal biometric systems [1]. Depending on the application and its usage, a biometric system may operate either as verification or as identification [2].

Verification

Here an individual who desires to be recognized claims an identity. The system does one-to-one comparison so that claimant is recognized. Verification avoids multiple people from using the same identity [4].

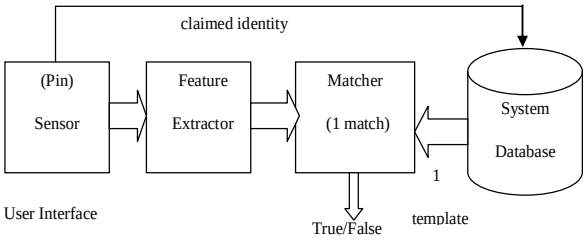

Fig 1 Block Diagram for Verification [4]

Identification

Here an individual is recognized without any claim about his identity. The system does one-to-many comparison so that claimant is recognized and it may fail if the person is not enrolled in the system database. Identification avoids a single person to have many identities.

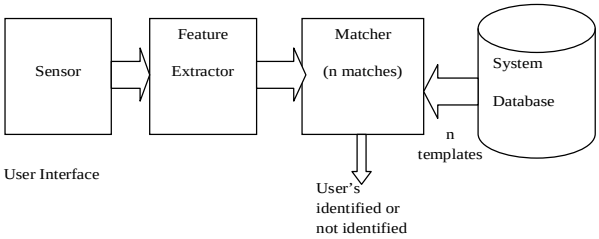

Fig 2 Block Diagram for Identification [4]

Metrics and Measures

The performance of a biometric system depends upon the computational assessment on accuracy and other quantifiable characteristics of the system. None of the metrics are adequate enough to give a reliable and desired result about the identification accuracy of a biometric system [1]. The decision made by a biometric system about an individual's is either a genuine or is an impostor type decision. Thus the result can be represented by two statistical distributions called genuine distribution and impostor distribution, respectively. For each type of decision, there are two possible decision outcomes, true or false [7]. In total there are four possible outcomes:

- A genuine individual is accepted.
- A genuine individual is rejected.
- An impostor is rejected.
- An impostor is accepted.

In general, False Acceptance Rate (FAR) is defined as the rate of acceptance of an impostor and is computed as:

$$FAR = \frac{\text{Number of imposter accepted} * 100}{\text{Total number of imposter comparisions}}\%$$

Next, the False Rejection Rate (FRR), defined as rate of rejection of a genuine user is computed as:

$$FRR = \frac{\text{Number of genuine person regected} * 100}{\text{Total number of genuine comparisions}}\%$$

And finally the Equal Error Rate (EER), the value at which the FAR and FRR are equal is computed as:

$$ERR = FAR \text{ for which } FAR = FRR$$

Types of Biometric System

Depending upon the use of either a single trait or multiple traits for person authentication Biometric systems is classified as:

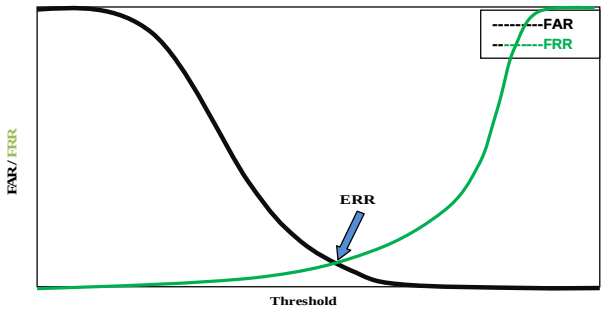

Fig 3 Calculating FAR, FRR, and EER [1] [4]

- Unimodal System-Model using single trait or modality.
- Multimodal biometric-Model using a combination of two or more modalities.

Unimodal System

Model using single trait are called unimodal biometric systems while those using more than one trait are called multimodal biometric systems [1]. Most biometric systems deployed in real-world applications are unimodal. They rely on the single characteristic as source of information for authentication (e.g., single fingerprint or Iris). Since each biometric has its own strengths and weaknesses, the choices depend on the application and its use. Not a single biometric is expected to effectively meet the requirements of all the applications. One can say that no biometric is "optimal." The requirement of a specific biometric for a specific application depends upon the kind of operation is expected from the application and the properties of the biometric traits. Table 1.1 gives a brief comparison on various biometric modalities as result of various experiments and perception of different authors where High, Medium, and Low are denoted by H, M, and L, respectively [4].

Table I Performance Comparison of Unimodal Biometric Systems [Jain et al, 2004]

Biometric traits	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
DNA	H	H	H	L	H	L	L
Ear	M	M	H	M	M	H	M
Face	H	L	M	H	L	H	H
Facial Thermo gram	H	H	L	H	M	H	L
Fingerprint	M	H	H	M	H	M	M
Gait	M	L	L	H	L	H	M
Hand Geometry	M	M	M	H	M	M	M
Hand vein	M	M	M	M	M	M	L
Iris	H	H	H	M	H	L	L
Keystroke	L	L	L	M	L	M	M
Odor	H	H	H	L	L	M	L
Palm print	M	H	H	M	H	M	M
Retina	H	H	M	L	H	L	L
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H

Multimodal Biometric System

Model using a combination of two or more biometric modalities in a verification or identification system as in figure 1.3 are called multimodal system. The lower accuracy rate and reliability of traditional authentication and unimodal biometric systems has pushed many end users to opt for

multimodal biometric systems as it provide a maximum level of accuracy during authentication process.

Most of the unimodal systems often face significant challenges due to sensitivity to noise, intra-class variability, data quality, non universality, spoofing attack and many other factors. These limitations of unimodal systems can be overcome by using multimodal biometric systems. Overall the multi-biometric system reduces False accept rate (FAR), False reject rate (FRR).

A multimodal system overcomes the stated limitations of unimodal by providing information on multiple evidences of the same identity. These systems help to achieve an increase in performance that may not be feasible relying just on a single biometric trait.

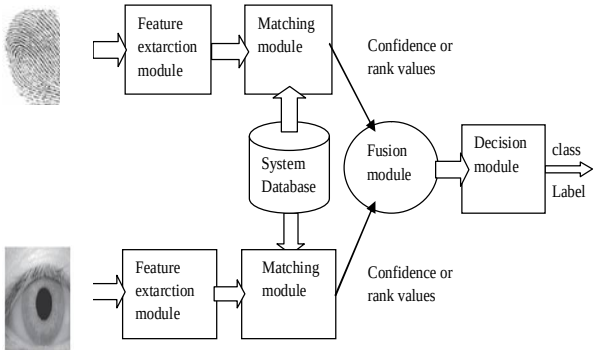

Fig 4 Block Diagram of Multimodal Biometric System [22]

Fusion Levels in Multimodal

In recent years, fusion in multimodal has gained popularity among many researchers as it provides benefit for various multi biometric analysis tasks. Multimodal biometric systems can be designed to operate in one of the five categories [23]:

1. *Multiple Sensors:* It can be Optical and Capacitance sensor.
2. *Multiple Biometrics:* It can be both Face and Fingerprint.
3. *Multiple Units of the same biometric:* It can be Right index and middle finger.
4. *Multiple Snapshots of the same biometric:* It can be two templates or snapshots of right index.
5. *Multiple Representations and Matching Algorithms for the same biometric:* It can be Minutiae and Non Minutiae based matcher.

The data in Multi-biometrics can be combined at different fusion levels such as [22]:

1. *Data-sensor level:* Direct concatenation of information as captured.
2. *Feature extraction level:* Pre-processed feature vectors are combined to form a composite feature vector.
3. *Matching score level:* Individual matching score is found and finally these matching scores are combined to make classification.
4. *Ranking level:* Use of a subset of sorted possible matches from individual modalities for final decision.
5. *Decision level:* The final classification is based on fusion of the outputs of different modalities.

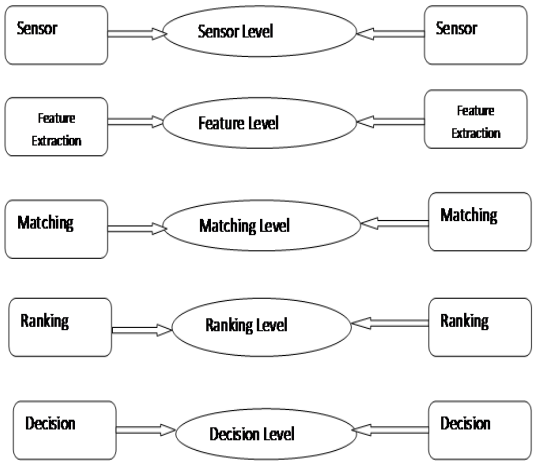

Fig. 5 Various Level of Fusion

Advantages of Multimodal over Unimodal

Accuracy: Since multimodal biometrics uses information from two or more modalities (such as fingerprint and finger vein pattern; or fingerprint and iris or it may be any other combination) compare to unimodal biometric systems which uses single piece of evidence as information from single biometric (e.g. fingerprint, iris, palm, signature, voice, or face), the accuracy of a multimodal biometrics system is higher resulting in almost zero FAR & FRR rates (as it collect information from multiple piece of evidence). The decision is concluded based on the outcome of fusion strategies for each single subsystem decision or opinion. Hence the multimodal biometrics is more accurate than unimodal or any other traditional authentication system [6].

Increased and Reliable Recognition: It is believed that multimodal systems provides a greater assurance level for an accurate match in verification as well as in identification modes, as it rely on multiple piece of evidence (i.e. multiple traits), where each single trait offer additional information about the authenticity of any identity claimed.

Enhanced Security: Another advantage of a multimodal system is that by making use of multiple evidences for identification, a system can set higher threshold value getting recognized. Thus a system administrator can take a decision as per the level of security needed [6].

Vulnerability: Spoofing has become a biggest threat to authentication systems. The biometric system whether it is multimodal or unimodal all is vulnerable to spoofing. Whenever an imposter masquerade any system as an authorized user a system has undergone spoofing attack.

User Acceptance: Multimodal systems are widely accepted due to higher accuracy, system is reliable, have larger security options, and is capable of handling spoofing attacks. The systems are getting widely deployed. The deployments where security and accuracy are essential, no matter how small or big the requirement is multimodal systems are gaining high importance [6].

Related Work

The interests in application of biometric, especially multimodal based biometric systems, several techniques and approaches have already been designed and developed for multimodal based biometric authentication system using

different biometric traits and different fusion level (mechanisms). Here, this section will introduce a short review from renowned researchers on some multimodal related works and their methods that has been designed and implemented by them.

In 2005, Jain et al. proposed a multimodal technique using face, fingerprint and hand geometry, with score level fusion. The matching of modalities such as fingerprint is done using minutiae-based matcher, which has similarity scores as output and for face recognition PCA has been used, which has Euclidean distance as output, and for a hand geometry, 14-dimensional features vector is used, which also has Euclidean distance as output [11].

In 2006, Li et al. proposed a new feature on hand metric, which is a combination of palm-print, hand shape and knuckle print. The features were integrated from these three biometrics using feature level fusion based on Kernel Principle Component Analysis (a combination of kernel projection and PCA dimension reduction) [12]. Again in 2007, Li *et.al* introduced a Full-space Linear Discriminant Analysis (FSLDA) for recognition using ear images, face images and the combined ear and face images [13].

In 2008, Nandakumar et al. introduced a multimodal system based on match score level fusion. They designed a framework which could optimally combine the match scores that is based on the likelihood ratio test. The system replicates the distributions of genuine and impostor match scores as finite Gaussian mixture model [14].

In 2009, Monwar and Gavrilova presented a system based on rank level fusion mechanism using fisher image method as matching algorithm and logistic regression count for face, ear and signature as biometric traits [15]. Kala *et.al* used face and voice characteristics for their system based on rank level fusion in 2010 [16].

In 2011, Meraoumia *et.al* introduced a system for person recognition using two different modalities palm-print and Finger Knuckle-Print (FKP) [17]. In 2012, Hariprasath *et.al* proposed a multimodal system using iris and palm print based on Wavelet Packet Analysis [18]. Trabelsi *et.al* introduced a new system based on fusion of hand vein and finger vein modalities in 2013 [19].

Table II Multimodal Biometric Systems based on different fusion Mechanisms

Year	Fused Modules	Authors	Level
2005	Face+Iris	Rose And Jain	Match Score
2006	Palmprint+Hand+ Knuckleprint	Li et.al	Feature
2007	Face+Ear	Li Yuan et.al	Rank
2008	Fingerprint+Face+Hand Geometry	Nandakumar et.al	Match Score
2009	Face+Ear+Signature	Monvar et.al	Rank
2010	Face+Voice	Rahul Kala et.al	Rank
2011	Finger-Knuckle-Print And Palmprint	Abdallah et.al	Match Score
2012	Iris+Palmprint	Hariprasath. et.al	Feature
2013	Finger Vein+Hand Vein	Trabelsi et.al	Match Score
2014	Ecg+Sound	Bugdol,And Mitas	Feature
2015	Palmprint+Fingerprint+Face	Deshpande et.al	Match Score

In 2014, Bugdol *et.al* presented a novel approach on behavioral biometric feature that combines ECG and sound signal. The signal acquisition has been carried out in a small stress condition as the user utter sounds at a given pitch [20].

In 2015, Deshpande *et.al* introduced a techniques which could integrates fingerprint, palm-print and face that undergoes fusion at score level [21].

Recent advancement in Features Extraction Tools

For any object to get accurately recognized its features need to be uniquely extracted and mapped with the features in the database and decision is taken. Most feature detectors as a tool makes use of the computational derivatives or more complex measures, the second moment matrix for the Harris detector or entropy for the salient regions detector. Due to repetition in procedure for each and every location in feature coordinate space which includes position, scale and shape, it makes the feature extraction process computationally expensive and not suitable for many applications [10]. Thus to overcome the computational efficiencies, several feature detectors that have been designed and developed.

The DoG, SURF, and FAST detectors are competitive with the standard, and being more computationally expensive feature detectors yet may produce better results for some applications. The DoGs detector approximates the Laplacian using multiple scale space pyramids. SURF makes use of integral images to efficiently compute a rough approximation of the Hessian matrix. FAST evaluates only a limited number of individual pixel intensities using decision trees.

Table III Performance measure of feature detectors tools against invariance [10]

Feature Detector	Corner	Blob	Region	Rotational Invariant	Scale Invariant	Affine Invariant	Repeatability	Location Accuracy	Robustness	Efficiency
Harris	√			√			+++	+++	+++	++
Hessian		√		√			++	++	++	+
SUSAN	√			√			++	++	++	+++
Harris-Laplace	√	√		√	√		+++	+++	++	+
Hessian-Laplace	√	√		√	√		+++	+++	+++	+
DoG	√	√		√	√		++	++	++	++
SURF	√	√		√	√		++	++	++	+++
Harris-Affine	√	√		√	√	√	+++	+++	++	++
Hessian-Affine	√	√		√	√	√	+++	+++	+++	++
Salient-Region	√	√		√	√	√	+	+	++	+
Edge-based	√			√	√	√	+++	+++	+	+
MSER				√	√	√	+++	+++	++	+++
Intensity-based			√	√	√	√	++	++	++	++
Super-pixels			√	√	√	√	+	+	+	+

The feature detectors in Table 1 are organized in 4 groups according to their invariance: rotation, similarity, affine, and from various viewpoints for 2D or 3D images and videos frames.

Rotational Invariance: For rotation invariant features, Harris detector plays an important role in the highest repeatability and localization accuracy. The Hessian detector finds blobs which are not well localized and requires second-order

derivatives to be computed. The SUSAN detector avoids computation of derivatives and is known for its efficiency, however the absence of smoothing makes it more prone to noise. Most of the rotation invariant methods are suitable for applications that only use the spatial location of the features with no large scale changes [10].

Scale Invariance: In case of the scale-invariant group, Harris-Laplace inherited from the Harris detector plays an important role in high repeatability and localization accuracy. But the scale estimation is less accurate as a result of the multi-scale nature of corners. Hessian-Laplace is more robust than its single scale version. This is due to the fact that blob-like structures are better localized in scale than corners and the detector benefits from multi-scale analysis although it is less accurately localized in the image plane [10]. Since DoG and SURF detectors were designed for efficiency thus their other properties are slightly compromised and yet for most applications they are still more than sufficient.

Affine invariance: For affine invariant Harris and Hessian continue the work from observations of previous groups. The Salient regions proceed by computing a histogram and its entropy for each candidate region in scale or affine space as result of large computational cost. The positive side of the system is that the regions can be ranked according to their complexity or information content. By exploiting the system, some applications using only small subset of the salient regions results in good performance. Thus the scale-invariant has been extended to affine invariance. In case of edge based regions, the focus is on corners formed by edge junctions that result in good localization accuracy and repeatability with just a few numbers of features being detected [10].

Region Detectors: The region detectors works by segmenting boundaries of uniform regions. In case of Intensity based regions, a heuristic method is used to find similar regions to MSER. Super pixels are also based on segmentation methods but the computational cost is higher like normalized cuts. The invariance level of super pixels is dependent on how segmentation algorithm is used. Unlike super pixels, as MSER selects only the most stable regions results in high repeatability and efficiency [10].

CONCLUSION

The purpose of using a biometrics is to provide an effective authentication mechanism to recognize a person with the help of one's biological characteristics eliminating the use of traditional way of authentication. These techniques are very inconvenient to be used for recognition (use of ID card, password, physical keys etc) [1]. From the survey it has been clear that there is a scope to extend the research work in the area of multi-biometric as it results in high discriminating feature and uniqueness.

The use of Multi-Biometrics takes advantages of the capabilities of each biometric technology while overcoming the limitations of a single technology. The demand of Multi-Biometrics system gives an ample opportunity to exploit the area of biometric. Thus with help of Wavelet, SIFT, SURF and FAST as a discriminating tool, we can improve the recognition rate as compared to the existing technique. One can also try to exploit these systems to reduce the cost of implementation, so small organizations can afford such systems.

References

1. Surya Prakash and Phalguni Gupta, "An Efficient Ear Localization Technique", Image and Vision Computing, 30(1), pp. 38-50, (2012).
2. Divyakant T. Meva, Dr C. K. Kumbharana, "Design and evaluation of multimodal biometric system with fingerprint and face recognition", I. J. of Scientific and Research Publications, ISSN 2250-3153 Volume 5, Issue 4, (2015).
3. Divyakant T. Meva, C K Kumbharana, "Comparative study of different fusion techniques in multimodal biometric authentication", International Journal of Computer Applications, ISSN: 0975-8887, Volume - 66(19), pp. 16-19, (2013).
4. Anil K. Jain, Fellow, IEEE, Arun Ross, Member, IEEE, and Sahil Prabhakar, Member, IEEE, "An Introduction to Biometric Recognition", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, No. 1, (2004).
5. M.L. Gavrilova, "Biometric-Based Authentication for Cyber-world Security: Challenges and Opportunities", pp 1-16, (2014).
6. Ekhlas Uddin, "Multimodal Biometric System Using Rank-Level Fusion Approach", http://www.researchgate.net/ publication/24248205, (2015).
7. K. Delac and M. Grgic, "A survey of biometric recognition methods", In International Symposium Electronics in Marine, ELMAR, (2004).
8. Zhang, D., Nandkumar K., and Jain, A.: Handbook of Multi-Biometrics. Springer, (2006).
9. P. Aruna, K. KumariI and G. Jaya Suma., "A Novel Multimodal Biometric Scheme for Personal Authentication", International Journal of Research in Engineering & Technology, ISSN(E): 2321-8843; ISSN(P): 2347-4599, Vol. 2, Issue 2, pp. 55-66, (2014).
10. Tinne Tuytelaars1 and Krystian Mikolajczyk2, "Local Invariant Feature Detectors: A Survey", Foundations and TrendsR in Computer Graphics and Vision Vol. 3, No. 3 (2007) 177-280 @ 2008 T. Tuytelaars and K. Mikolajczyk DOI: 10.1561/0600000017
11. A.K.Jain, K.Nandakumar, and A.Ross, "Score normalization in multimodal biometric systems", Pattern Recognition 38, 12, pp.2270-2285, 2005.
12. Q. Li, Z. Qiu, D.Sun, "Feature-level Fusion of Hand Biometrics for Personal Verification Based on Kernel PCA",(eds) LNCS 3832, ICB, pp.744-750, 2006
13. Y.Li, Z.Mu, X.Xu, "Multimodal Recognition Based on Face and Ear", Proceedings of the International Conference on Wavelet Analysis and Pattern Recognition, 2007.
14. K.Nandakumar, Y.Chen, S.C.Dass et.al, "Likelihood Ratio-based Biometric Score Fusion", IEEE Trans on Pattern Analysis and Machine Intelligence, 30 (2): pp.342-347, 2008.
15. Monwar and Gavrilova, "Multimodal biometric system using rank-level fusion approach", 2009.
16. R. Kala, H.Vazirani, A. Shukla, and R. Tiwari.: Fusion of Speech and Face by Enhanced Modular Neural Network. ICISTM, CCIS 54, pp.363-372, 2010.
17. A. Meraoumia, S. Chitroub, and A. Bouridane, "Fusion of Finger- Knuckle-Print and Palmprint for an Efficient

Multi-biometric System of Person Recognition", IEEE ICC proceedings, 2011.
18. S.Hariprasath, T.N.Prabakar, "Multimodal Biometric Recognition Using Iris Feature Extraction and Palmprint Features", ICAESM, 2012.
19. R.BTrabelsi, A.D. Masmoudi, and D.S.Masmoudi, "A New Multimodal Biometric System Based on Finger Vein and Hand Vein Recognition", International Journal of Engineering and Technology, 2013.
20. D.Marcin, W. Andrzej, "Multimodal biometric system combining ECG and sound signals", Pattern Recognition Letters 38, pp.107-112, 2014.
21. A. S.Deshpande, S.M.Patil and R. Lathi, "A Multimodal Biometric Recognition System based on Fusion of Palmprint, Fingerprint and Face", International Journal of Electronics and Computer Science Engineering, 2015.
22. Ms. Priyanka S. Patil, Prof. (Dr.) A. S. Abhyankar, "Multimodal Biometric Identification System Based On Iris & Fingerprint", IOSR Journal of VLSI and Signal Processing (IOSR-JVSP) e-ISSN: 2319-4200, p-ISSN No. : 2319-4197 Volume 1, Issue 6 (Mar.-Apr. 2013), PP 76-8.
23. A S Raju, V Udayashankara, "Biometric Person Authentication: A Review", International Conference on Contemporary Computing and Informatics (IC3I), 2014.

How to cite this article:

Om Prakash Sharma and Jitendra Sheetlani (2017) 'Biometric Based Authentication System: A Survey', *International Journal of Current Advanced Research*, 06(07), pp. 4487-4492. DOI: http://dx.doi.org/10.24327/ijcar.2017.4492.0524

****