International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 12 | Dec -2016 www.irjet.net p-ISSN: 2395-0072

Cuckoo Search Optimization for Feature Selection in Face & Fingerprint

Nishu Rani[1], Rajan Sachdeva[2]
[1] *Research Fellow*
[2] *Assistant Professor*
GGS College of Modern Technology, Kharar, Punjab, India

Abstract- Recognition of the people by the method of their characteristics of biometric is very much popular and common in the society. Biometrics is the technology and science of analysing and measuring biological information of the body of human, extraction of feature set from the data acquired and then contrasting this set against the set of template in the database. The studies of experiment demonstrate that unimodal systems of biometric had numerous disadvantages with respect to accuracy and performance. The approaches of multimodal biometric are increasing in importance for identification and verification of an individual, as they offer better results of recognition and in this way enhance the security as contrasted to biometrics which is dependent upon single modality. In this paper, fingerprint verification and face recognition are combined as both of these biometric are accepted widely. These modalities are utilized because of their ease and comparatively less cost. Multimodal biometric systems perform better and hence increase the accuracy and also security of the system.

***Keywords*— Biometrics, Fingerprint recognition, face recognition, multimodal.**

I. INTRODUCTION

In today's world, verification which is based on verification has been getting very much consideration chiefly, on account of the unprecedented extent of fraud identity following in our general public and the expanding accentuation on the developing applications of automatic personal identification. The term "biometrics" is gotten from e words of Greek – "bio" which implies life and "metrics" which intends to measure. A more nitty gritty meaning of biometrics is any naturally robust, measurable and exceptional characteristic or individual quality, which can be made utilization of to perceive an individual or check the asserted personality of an individual". The strategy of biometric identification is favoured over conventional methods including PINs (Personal Identification Numbers) and passwords for various reasons, 1) the individual to be verified is to be present physically at the identification point or/and 2) identification in the view of techniques of biometric reduces the need to hold up under at the top of priority list a carry token or password. [1]

Example of biometrics:

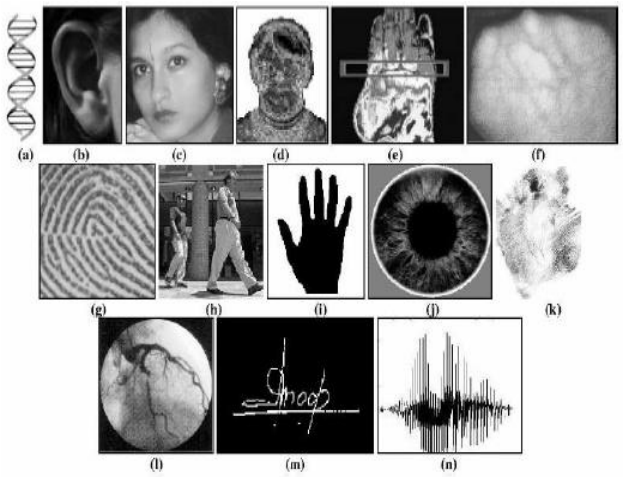

Fig.1. Examples of biometric characteristics: (a) DNA, (b) ear, (c) face, (d) facial thermo gram, (e) hand thermo gram, (f) hand vein, (g) fingerprint, (h) gait,(i) hand geometry, (j) iris, (k) palm print, (l) retina, (m) signature, and (n) voice.

Normally, there are mainly two types of biometric systems: identification and verification. In systems of identification, a signature which is biometric of a fairly new customer is provided to a system. Then the system compares the new signature of biometric with the database of the biometric signatures which are existing of known persons for identifying if that person is known previously or the person is stranger. In the systems of verification, the user provides a biometric signature and then the system verifies this signature, if that biometric signature belongs to the identity which is claimed. Both of these systems demand the storage of massive number of templates of biometric for achieving efficient identity recognition. With the increasing utilization of systems of fingerprint recognition the main question comes how to store and handle the acquired data of fingerprint. [1]

Any behavioural or physiological characteristic of human can be utilized as a characteristic of biometric as soon as it fulfils the requirements explained below:

1. Universality: Every individual should have unique characteristic.

2. Distinctiveness: any two individuals must be sufficiently dissimilar in the provisions of characteristic.

3. Permanence: the characteristic must be invariant sufficiently (in the view of the criterion of matching) over interval of time.

4. Collectability: the characteristic could be quantitatively measured.

But in the biometric systems which are practical, there are numerous other problems which should be taken care of incorporating:

1. Circumvention: which replicate how simply the system can be made fool by utilizing methods which are fraudulent.

2. Acceptability: which specify the extent up to which individuals are prepared for accepting the utilization of specific identifier of a biometric in their daily life.

3. Performance: which talk about the acquirable speed and accuracy of recognition, the resources needed for achieving the required speed and accuracy of recognition, and also the factors like environmental and operational which will put impact on the speed and accuracy. [2]

II. FINGERPRINT RECOGNITION

A fingerprint normally shows up as a progression of dark lines that speaks to the high cresting part of the ridge peel of friction, though the valleys in between these ridges appear as white space and are low shadow portion of the ridge peel of friction. The Fig. 2 shows the fundamental features of biometric like ridge endings, bifurcations and core of fingerprint. The points at which ridge endings are there are the focuses at which stoppage of ridge. Bifurcations are the points on the image of fingerprint at which there is division of one ridge to two. And core is the central point of pattern of fingerprint. [3]

Fig. 2 Biometric features of fingerprint image [3]

Fingerprint recognition is utilized for identification of user on account of its ease, reliable usability and performance as contrasted to different biometrics, for example, iris, face, signature etc. and is utilized in applications of commercial and forensic like electronic personal ID cards and investigation of crime. The systems of fingerprint recognition database might have huge number of images of fingerprint. An image of fingerprint has extensive measure of information and the storage of databases of image of fingerprint is on tremendous storage devices which are secondary. Fingerprints are unique individual's identifiers. Extensive measure of fingerprints are collected and put away in numerous applications incorporating access control and forensics. Huge amount of information in a database expends more amount of memory and the data present in the fingerprints must be compressed by taking out the elements which are visible only. The images of fingerprint have high energy in few bands of high frequency acquired from the pattern of ridge-valley and different structures. [4]

III. FACE RECOGNITION

Face recognition is an area of research which is active and hence they can be used in applications of wide range, for example, security and surveillance. Face is an advanced structure which is multidimensional and requires a decent technique of computing for purpose of recognition. The system of face recognition can be used in two modes: Verification and Identification. The extraction of the features of face incorporates localizing presumably the most qualitative elements of the image of face such as mouth, nose and eyes region. [5]

Face recognition has dependably been an exceptionally difficult task for the researchers. On another hand, it has dependably been extremely hard for implementing because of all diverse circumstances that face of human can be found. Because of the difficulty in the task of the recognition of face, quantity of techniques is diverse and large. It is not surmise that images are dependably captured in perfect conditions, there might be variation in expression, pose and illumination. Such difficulties are more unmistakable in recognition of heterogeneous face. In a decade ago, there were numerous methods created for handling such types of issues. From surveys of face recognition, it implies that they have face recognition of the images of that face which are of same sort. This confines the face recognition or particular data type. Such circumstance can be handled by utilizing images of face of diverse methodology, it allude as heterogeneous faces. [6]

IV. MULTIMODAL BIOMETRIC SYSTEM

A multimodal security system contains various solutions of security which also offer mutual backup. A multimodal security solution utilizes security at two or more levels at the purpose of section to your business place. A multimodal solution would, for instance, comprise of a swipe card in blend with PIN code. Interestingly, a uni-modal solution would include the utilization of swipe card or PIN code only. It is additionally conceivable to utilize a security solution which is uni-modal in few sections of building and solution which is multi-modal in some others. For a multi-modal solution to perform very well, it must utilize various systems of security and technologies inside of every mode. Along these lines, the accuracy and quality of the process of authentication and verification are upgraded. [7]

Various levels of fusion are: Sensor level, feature level, matching score level, and decision level.

1. Sensor level fusion: we combined the traits of biometric taken from diverse sensors to make a process and trait of biometric which is composite.
2. Feature level fusion: Signal originating from distinctive channels of biometric are pre-processed initially, and feature vectors are separately extracted by utilizing particular algorithms and then these vectors are combined to make a composite feature vector.
3. Matching score level fusion: Instead of combining the feature vector, these are processed separately and individual score of matching is found, hen relying upon the accuracy of every score of matching of biometric which will be utilized for classification.
4. Decision level fusion: Every modality is firstly pre-classified autonomously. Multimodal system of biometric an execute any of these strategies fusion or may be combination of these for enhancing the system's performance. [7]

V. MOTIVATION

Fingerprint verification system and Face recognition system are combined as these modalities are widely accepted. These modalities are widely used due to easy data acquisition and relatively low cost. Multimodal biometric is designed to enhance the real time verification and reliability rates. Integrating face and fingerprint biometric helps in identifying the person. So for this integration, an effective fusion level and fusion mode is required**.** Now our aim is to propose optimized feature extraction using face & fingerprint modalities with SIFT and Minutiae algorithm and then fuse the both modalities at feature level because feature level fusion provides better recognition performances. After that an optimized technique (cuckoo search algorithm) is applied to collect the optimized features from existing feature set and then obtain the decision.

The research work is based on following objectives:

1. To study face and fingerprint modalities.
2. To study fusion schemes in biometrics.
3. To collect optimized features using Cuckoo Search algorithm.
4. To compare the results with previous studies.

VI. PROPOSED SCHEME

In this research work, we have combined two biometric systems making it multimodal biometric system.

1. Choice of Modality: In this work, fingerprint verification system and face recognition system are combined as these modalities are widely accepted. A combined system enhances security and accuracy.

2. Feature Extraction

Face: In this work, we use Scale-invariant feature transform (SIFT) to extract the features. It is widely used because it is invariant to changes in illumination, image noise, rotation, scaling and small changes in view point.

Fingerprint: To extract features, we can use Minutiae based technique where fingerprint image is normalized, pre processed using Gabor filters, binarized and thinned, is then subjected to minutiae extraction.

3. Feature Optimization: In this work, optimized features are collected from the extracted features, we follow Cuckoo Search Algorithm. In the computer science field of artificial intelligence, cuckoo search (CS) is a search-heuristic. It is used to generate useful solutions to optimization and search problems. It was inspired by some cuckoo species by laying their eggs in the nests of other host birds. It reduces the computational cost significantly.

4. Level of Fusion: This work presents a novel user authentication system based on a combined acquisition of fingerprint and face. Feature level fusion is used as it is better and gives the optimal identification results.

The flowchart is shown below:

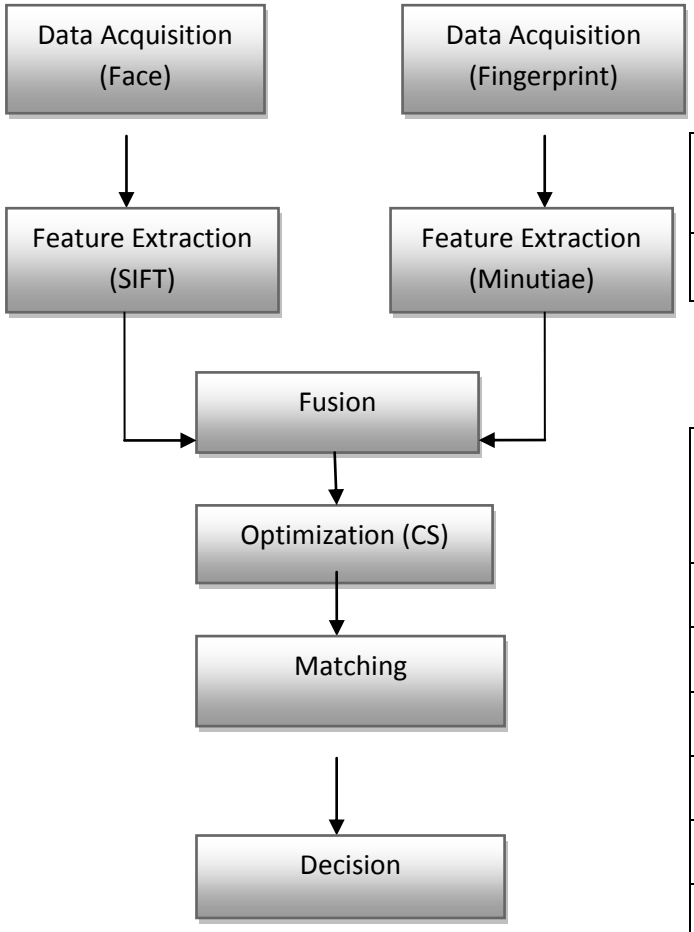

Fig. 3 Proposed algorithm level decision

VII. RESULTS AND DISCUSSIONS

In this section, we present the results of the proposed work.

For face and fingerprint Samples:

Total Number of Samples in the database=40

Number of Sample that falsely accepted=1

$$FAR = \frac{\text{Total Number of Samples} - \text{Number of Samples that Falsely accepted}}{\text{Total Number of Samples}}$$

$$\text{So, } \mathbf{FAR} = \frac{40-1}{40} = \frac{39}{40} = 0.97\%$$

For face and fingerprint Samples:

Total Number of Samples in the database=40

Number of Sample that falsely rejected=0

$$FRR = \frac{\text{Total Number of Samples} - \text{Number of Samples that Falsely rejected}}{\text{Total Number of Samples}}$$

$$\text{So, } \mathbf{FRR} = \frac{40-0}{40} = \frac{40}{40} = 0.00\%$$

FAR	FRR	Accuracy = [100-(FAR+FRR)]
0.97	0.00	99.03%

Table 1: FAR, FRR and ACCURACY

Sample No.	Face	Fingerprint	Fusion	Cuckoo Search	Total
1	0.3	0.03	0.07	5.13	5.53
2	0.07	0.07	0.06	4.99	5.19
3	0.03	0.06	0.05	5.5	5.64
4	0.04	0.15	0.09	6.12	6.4
5	0.09	0.03	0.03	4.89	5.04
6	0.17	0.16	0.07	4.14	4.54
7	0.03	0.03	0.06	5.4	5.52
8	0.07	0.04	0.05	5.16	5.32
9	0.06	0.09	0.04	4.90	5.09
10	0.15	0.17	0.05	5.17	5.54
11	0.17	0.03	0.08	6.11	6.39
12	0.19	0.07	0.06	6.8	7.12
13	0.12	0.03	0.07	5.9	6.12
14	0.05	0.04	0.06	5.1	5.25
15	0.04	0.09	0.05	5.19	5.37

16	0.05	0.04	0.04	4.99	5.12
17	0.18	0.06	0.05	5.78	6.07
18	0.07	0.19	0.04	5.16	5.46
19	0.03	0.12	0.06	5.13	5.34
20	0.04	0.05	0.07	4.99	5.15

Table 2: Time analysis (seconds)

VIII. CONCLUSION & FUTURE SCOPE

The main aim of this research is to combine the two methods of biometric i.e. fingerprint recognition and face recognition to make the multimodal biometric system. A multimodal biometric system provides many benefits: firstly, a multimodal system can enhance the reliability of the process of verification. Secondly, multimodal system can capture the unique characteristics of biometric which are of more varied and much larger population target. Thirdly, a multimodal system is significantly harder to spoof than a unimodal biometric system.

ACKNOWLEDGMENT

The paper has been written with the kind assistance, guidance and active support of my department who have helped me in this work. I would like to thank all the individuals whose encouragement and support has made the completion of this work possible.

REFERENCES

[1] Vani Perumal, Dr. Jagannathan Ramaswamy, "An Innovative Scheme for Effectual Fingerprint Data Compression Using Bezier Curve Representations", International Journal of Computer Science and Information Security (IJCSIS), Vol. 6, No. 1, 2009

[2] Anil K. Jain, Arun Ross, Salil Prabhakar, "An Introduction to Biometric Recognition", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, No.1, January 2004.

[3] Swapnil Raut, Nisha Wankhade, "Fingerprint Compression Technique using Sparse Representation", International Journal of Science and Research (IJSR), Vol. 4, Issue 4, April 2015.

[4] Lakshmipriya. S, "A Survey on Fingerprint Compression Methods", International Journal of Modern Trends in Engineering and Research, Vol. 2, Issue 7, July 2015.

[5] Sarabjit Singh, Amritpal Kaur, Taqdir, "A Face Recognition Technique using Local Binary Pattern Method", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 4, Issue 3, March 2015.

[6] Ketki Kalamkar, Prakash Mohod, "A Review on Face Recognition Using Different Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 5, Issue 1, January 2015.

[7] Sonam Shukla, Pradeep Mishra, "A Hybrid Model of Multimodal Biometrics System using Fingerprint and Face as Traits", International Journal of Soft Computing and Engineering (IJCSE), Vol. 2, Issue 1, March 2012.

[8] A. Rattani, D. R. Kisku, M. Bicego, "Feature Level Fusion of Face and Fingerprint Biometrics", First IEEE International Conference 978-1-4244-1597-7, pp.1-6, 27-29 Sept.2007.

[9] Darwish, A, Ashraf. , and Schaefer, Gerald. , " Human Authentication using Face and Fingerprint Biometrics" IEEE Trans. on Second International Conference on Computational Intelligence, Communication Systems and Networks, 978-0-7695-4158, 2010.

[10] Abdolahi, Mohamad. , and Mohamdi, Ajid. , "Multimodal Biometric system Fusion Using Fingerprint and Iris with Fuzzy Logic", International Journal of Soft Computing and Engineering (IJSCE), Vol. 02, Issue 06, January 2013.

[11] Xin-She Yang, Suash Deb, " Cuckoo Search with Levy Flights", World Congress on Nature and Biologically Inspired Computing, 2009.