International Journal of Electronics Engineering (ISSN: 0973-7383
Volume 11 • Issue 1 pp. 414-420 Jan 2019-June 2019 www.csjournals.com

An Advanced Approach Biometric System Security by Fusing Face and Fingerprint Traits

Sakshi Nagpal
M.Tech. Student, Department of Computer Science and application, K.U. Kurukshetra, Haryana, INDIA

Abstract: Biometric includes physical and behavioral characteristics of the person for identifying an actual user and imposter. Unimodal biometric system (having single biometric trait) provide recognition but contain some limitation such as high error rate, non-universality, noise in sensed data etc. These problems could be overcome by multimodal approaches which combine more than one trait of a user for authentication. Multimodal provides better performance, accuracy and security over a unimodal biometric system. The main aim of introducing liveness detection with multimodal biometric is that we can use this approach in a highly secured application such as defence and bank application. So in this paper liveness detection technique (which detect whether the enrolled user is live or not) is defined with a multimodal approach. This paper presents a new approach for increasing security and performance by the combination of face and fingerprint biometric together with liveness detection technique.
Keyword: fusion level, liveness detection, multi-biometric, unimodal biometric.

1. Introduction

Biometric technology provides several advantages over conventional security methods like pin, password, key, card etc. The Biometric system grants authentication by different physiological and behavioral traits of a person. Biometric systems are basically of two types based on the use of a biometric trait for identification and verification. The types of biometric system are

- Unimodal biometric system
- Multimodal biometric system

The Unimodal system has an only single source of information for authorization of a valid user. But sometimes single trait do not provide good quality of sample due to deformations problem in a biometric trait such as the same sample of hand geometry do not capture after swelling, face images changes according to the lightening, voice change due to the cold or illness etc. The error rate of the unimodal biometric system is also high because of some problems (for e.g. lack of individuality, lack of different representation, susceptibility to circumvention). The high error rate is not suitable for a more secure application.

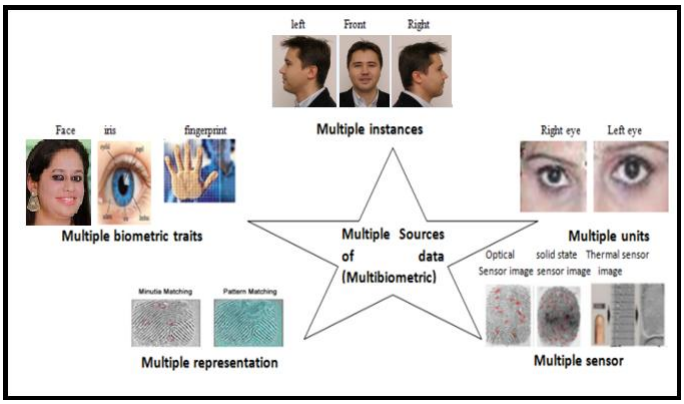

Fig 1 Different category of Multi-Biometrics

The level of Security is also increased by this technique as compared to unimodal. Multimodal biometric is one of the types of five categories of the multibiometric system as shown in Fig 1.

1.1 Classifications of Multibiometric System

1.1.1 Multiple sensor systems

Multiple sensor systems capture single biometric trait by using two or more different sensors. For authentication, fingerprint samples taken by optical and solid state sensor [3].

1.1.2 Multiple representation systems

In this type multiple representation methods are used for storing template. Template is generated by extracting their minutiae point and pattern from capturing sample.

1.1.3 Multimodal system (multiple biometric traits)

The multimodal system includes more than one biometric trait or the combination of different modalities is used for better secure results. For e.g. combination of correlated traits (voice and lip movement) and uncorrelated trait (face and fingerprint) are used for authentication.

1.1.4 Multiple instance system

In this category of system, multiple instances of same biometric trait are acquired either by same sensor or different sensor. For e.g. instance of the face, biometrics trait is the front view, left side view and right side view as shown in Fig 1.

1.1.5 Multiple unit systems

This type of system contains different units of the same biometric trait. For e.g. left and right eyes samples are used as a different unit for authentication.

1.2 Fusion levels in biometric system

The results of two or more unimodal biometric are combining using fusion for making multibiometric system. There are mainly two level of fusion which is further divided into four level of fusion (shown in fig 2) are discussed below [4]:

1.2.1 Sensor level fusion

At this level sample capture from the different sensor or multiple instances of the same trait from the same sensor are fused together. This is an early stage of fusion.

1.2.2 Feature extraction level fusion

Samples taken from the same or different sensor are preprocessed and send to feature extraction module for further processing. Feature extraction module extract feature set individually. So the extracting feature set of each samples are fused together for making a single combine vector by this level of fusion.

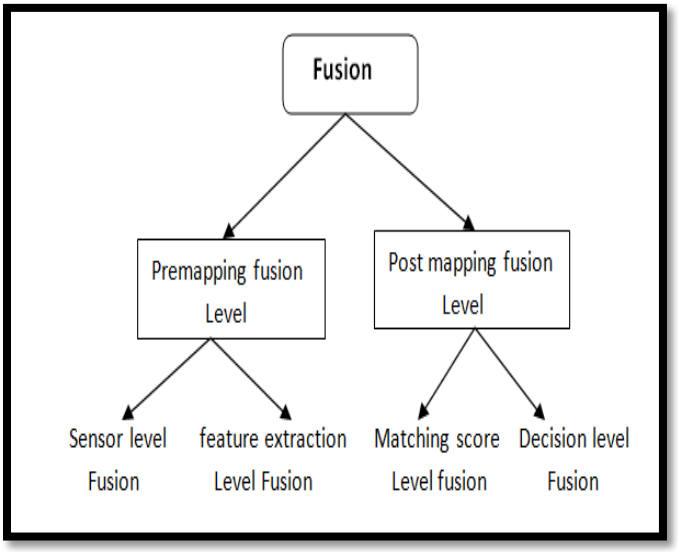

Fig 2 Fusion level for multibiometric system

1.2.3 Matching score level fusion

This type of fusion is used to getting match score from different matcher. All the results obtained from each matcher are fused together by matching score level fusion.

1.2.4 Decision level fusion

Decision level fusion can apply at the end of biometric system processing. This is the last stage of fusion where the outputs of all the decision modules are combined for providing better performance and accessibility.

The multimodal biometric system performs any of the above fusion strategies for better output. In proposed model multimodal technique is used with decision level fusion of face and fingerprint biometric traits.

1.3 Liveness detection

The new technology liveness detection is also used with the multimodal approach for protection against spoof attacks. For making a secure biometric system, liveness detection is a good technique that determines the sample given by user either live or not. Liveness technique is just used after captured the sample by the sensor in our new proposed approach. Currently, liveness detection becomes a better approach in the field of recognition for protecting against imposter fake samples. By using this new approach performance and security level of a system are improved. This is mainly used for differentiating whether the given sample is real or not [5]. Liveness detection in biometric system can be performed at two stages:

1. Acquisition stage
2. Preprocessing stage

Our proposed architecture uses liveness detection approach at sensor level (acquisition stage) for both modalities face and fingerprint. Liveness detection at sensor level is mainly used for reducing spoofing attacks. There are mainly three categories of liveness detection techniques which are discussed below [6]:

1. Liveness detection based on the intrinsic property of human being like physical property (density, elasticity), visual property (color) and body fluids (oxygen, DNA) etc.
2. Liveness detection based on the involuntary signal of person such as pulse, blood flow, perspiration, blood pressure etc
3. Liveness detection based on the bodily response of the person. This type includes either voluntary (where user response is needed) or involuntary (without user response). For e.g. pupil expansion, knee reflex, eye blinking and smiling.

2. Related work

User authentication is a basic requirement for any type of security system. In the field of biometric many researchers do their work for providing secure user authentication. The literature available for secure authentication by using different new approach is discussed below:

B. G [7] discussed prevention method against spoof attack in face recognition. Liveness detection of the user with their facial feature like eye blinking, lip movement, forehead movement defined in their paper for better security. The different pattern is detected with the help of a camera and checks the liveness of face sample. This is better approach given by author for identification of the fake user (imposter). The proposed system developed by author provides better security, performance and accuracy for face recognition.

Unimodal biometric systems have some limitations which are alleviated by the multimodal biometric approach. Gambhir [8] discussed a multimodal approach for person recognition. The different modalities such as face and ear recognition were used by the author for providing better recognition model. The developed model possesses many unique qualities like PCA analysis algorithm in MATLAB for face and ear recognition matcher module. Overall performance was improved by fusion of both traits.

Multimodal systems have more advantages than a single biometric system. Abdolahi [9]Proposed an identification system based on fingerprint and iris with fuzzy logic. Decision level fusion strategy was used by the author for combining results. Effect of each biometric result combination was defined by fuzzy logic.

B.M [10] Combined two biometric traits finger vein and fingerprint for providing secure identification system. The proposed system acquires finger vein and fingerprint simultaneously and result is combined by using nonlinear fusion approach.

Preethi [11] Proposed an approach for providing better protection against imposter attack. This approach uses the combination of three biometric traits such as the face, fingerprint, and iris. Liveness detection technique also discussed by the authors for differentiating whether the sample given is live or not.

3. Proposed model

In our proposed work combination of two biometric traits such as face and fingerprint are used with liveness detection for making better authentication system. This model gives better security and accessibility. In this approach fingerprint liveness is checked by perspiration method at the sensor level. When fingerprint contact with

sensor surface physiological perspiration process varies according to time. Mostly sensors (optical, solid state sensor etc.) are sensitive to the environmental condition such as a change in moisture, temperature etc. So, if the sensor detects perspiration presence in specific time domain then it means fingerprint sample given to sensor is a real otherwise imposter fake fingerprint. Another biometric trait (face) which is used in proposed multimodal approach also used liveness detection technique. Face liveness detection is checked by user response of eye blinking and smiling face captured by a web camera. There is no need of extra hardware for checking liveness for both traits. Proposed model contains these two phases for increasing security level and accessibility.

i. Liveness detection at sensor level for checking the sample given by the user is real or not.

ii. Decision level fusion combines decision of both modalities and decides whether the user is real or an imposter.

Every biometric system requires two stages for verification and identification of the user. First is enrollment and second are authentications. In our proposed system at enrollment stage, the template of face and fingerprint traits are stored in the database (shown in fig 3) which are further used for comparing new samples in the authentication phase.

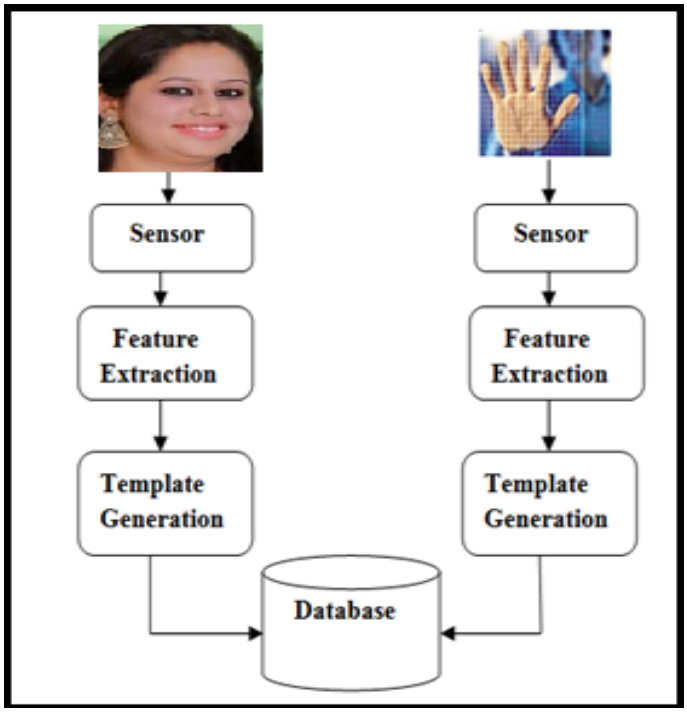

Fig 3 Enrollment phase

In authentication phase firstly liveness detection is applied at sensor level for checking whether the newly captured sample is live or not as shown in fig 4. If the given sample live then features extractor module present a template by extracting their feature set and send to the matcher module which compares that template with stored template. Matcher module matches template and generates match score which is further sent to decision module. Decision modules make a decision on the behalf of match score. At this point, our novel approach uses decision level fusion. Fusion combines results of both approaches and makes a single result as shown in table 1. Algorithm of given approach define each and every step of architecture model as given below:

3.1 Algorithm for Authentication

1 Face and fingerprint samples are presented to the different sensors.

2 Liveness is checked at sensor level for both modalities

a) Fingerprint sample liveness is checked by the sensor itself by sensing perspiration.

b) Face liveness is checked by capturing user response of eye blinking and smiling face through the web camera.

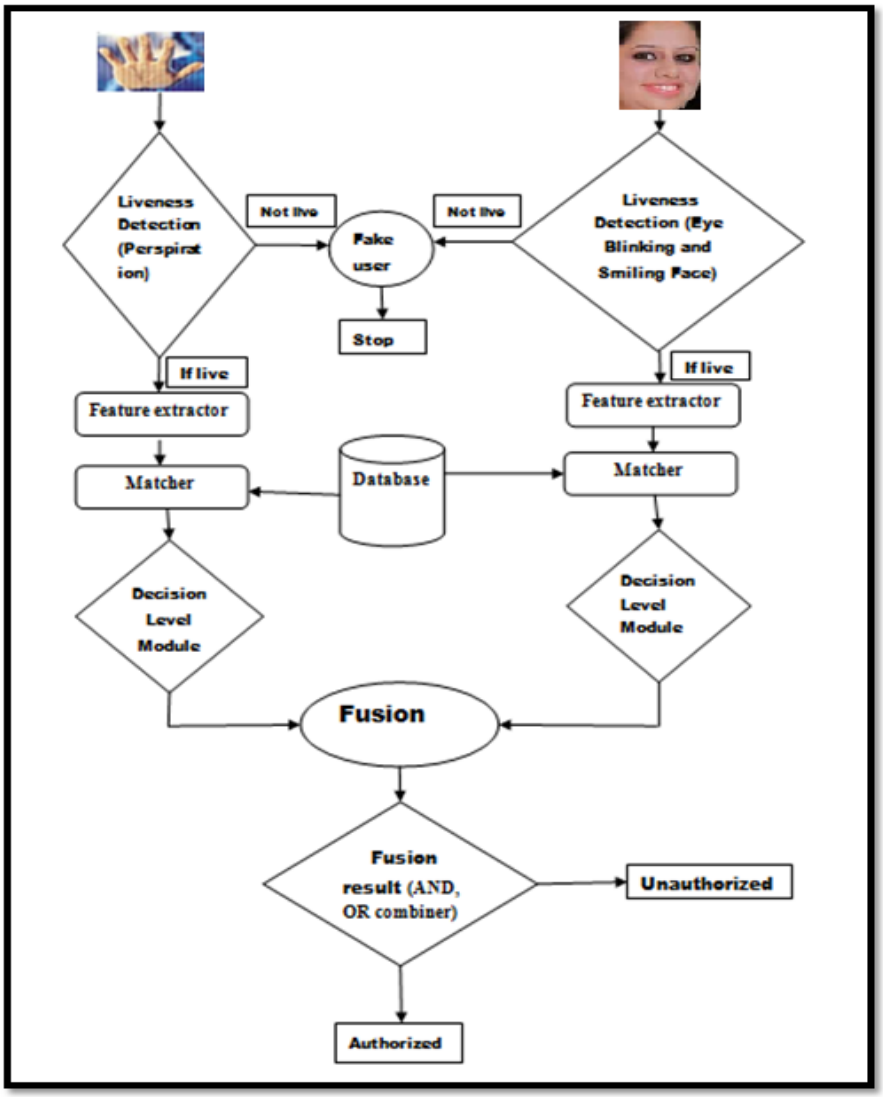

Fig 4 Authentication with liveness detection

3. If both input samples are live then
a) Sample sends to feature extractor module
Else
b) Fake user samples
4. Feature extractor modules generate templates individually by extracting their feature set and template send to matcher modules.
5. Both matchers match the receiving templates with stored templates in enrollment phase and generate match score which is a basis for taking a decision by decision module
6. Both decision level modules compare match score with the threshold value and provide results for fusion.
If match scores >= threshold value
Then
Real user
Else
Fake user
End
7. The important thing in this approach is fusion which is done on the results of decision module. Fusion combines decision of both approach and decides whether the person is authorized or not according to these steps:
i) Recognition of person with high threshold value

IF fdmr=real AND fcdmr=real THEN
Recognize authorized user
ELSE
Recognize unauthorized user

ii) Recognition of person with normal threshold value

IF fdmr=real AND fcdmr=real OR fdmr=real AND fcdmr=fake OR fdmr= fake AND fcdmr=real THEN
Recognize authorized user
ELSE
Recognize unauthorized user

8. End

Table 1 shows fusion result with respect to the high threshold value. The application will give The result as authorized user according to the high threshold value if and only if both traits decision module's output will be "real" otherwise recognize an unauthorized user. So this strategy can apply for the tight secure application like bank and defence application.

Table 2 shows fusion result with the normal threshold value. This strategy can be applied for those applications where the user wants high accessibility instead of high security. We can apply this approach for attendance system of any organization where required results are according to the normal threshold value.

Table 1 Fusion result with high threshold value

Fingerprint decision module result (fdmr)	Face decision module result (fcdmr)	Final result
Real	Real	Authorized
Real	Fake	Unauthorized
Fake	Real	Unauthorized
Fake	Fake	Unauthorized

Table 2 Fusion result with normal threshold value

Finger print decision module result (fdmr)	Face decision module result (fcdmr)	Final fusion result
Real	Real	Authorized
Real	Fake	Authorized
Fake	Real	Authorized
Fake	Fake	Unauthorized

There are some drawbacks in this novel approach

a) Cost of overall approach is high because it uses different devices for face recognition and fingerprint trait.
b) It requires the same type of matcher because the different variety of matcher provides match score in the different form. Different forms of match score do not provide an accurate result of decision module.

4. Conclusion

Biometric authentication system based on the single trait has some limitation which can be removed by using the combination of more than one traits. We have proposed the novel approach by combining face and fingerprint biometric traits for better recognition, liveness detection technique is also used with the presented multimodal

approach for a better result. Liveness detection is used at the sensor level for checking the dummy users. The proposed approach provides better security, accessibility and performance. This proposed model can be used in future for those applications where the required security system is according to the high threshold value.

References

[1] Komal sondhi and yogesh bansal, "concept of unimodal and multimodal biometric system," vol. 04, no. 06, 2014.

[2] K. Sasidhar, vijaya l kakulapati, kolikipogu ramakrishna, and k.kailasarao ramakrishna, "multimodal biometric systems –study to improve accuracy and performance," vol. 1, no. 02, 2010.

[3] V. Sireesha and k. Sandhyarani, "overview of multimodal biometrics," vol. 04, no. 01, 2013.

[4] Mini singh ahuja and sumit chabbra, "a survey of multimodal biometrics".

[5] Chakraborty, saptarshi das and and dhrubajyoti, "an overview of face liveness detection," vol. 03, no. 02, 2014.

[6] Sonal girdhar and chander kant, "a novel approach for detecting fingerprint liveness," vol. 4, no. 6, 2015.

[7] Nalinakshi b. G, sanjeevakumar m. Hatture, manjunath s. Gabasavalgi, and rashmi p. Karchi, "liveness detection technique for prevention of spoof attack in face recognition system," vol. 03, no. 12, 2013.

[8] Abhishek gambhir, sanket narke, shraddha borhade, and gayatri bokade, "person recognition using multimodal biometrics," vol. 04, no. 04, 2014.

[9] Mohamad abdolahi, majid mohamadi, and mehdi jafari, "multimodal biometric system fusion using fingerprint and iris with fuzzy logic," vol. 02, no. 06, 2013.

[10] Shruthi b.m, pooja mohnani, mallinath, and ashwin. R.g, "multimodal biometric authentication combining finger vein and fingerprint," vol. 07, no. 10, 2013.

[11] Preethi. V and prof.s. Chidambaram, "fake multi-biometric detection for applications of fingerprint, iris and face recognition," vol. 21, no. 2, 2015.

[12] Gurpreet singh and vineet kumar gagandeep kaur, "a review on biometric recognition," vol. 6, 2014.

[13] Dr.l.r.karlmarx s. Veluchamy, "technical review of multimodel biometrics system," vol. 4.

[14] Anil lamba sakshi kalra, "a survey on multimodel biometric," vol. 5, 2014.

[15] Chander kant rubal jain, "attacks on biometric system: an overview," vol. 01, no. 07, 2015.

[16] Ahmad obied, "how to attack biometric system in your spare time".

[17] Dr.k.rameshkumar mrs.u.latha, "a study on attacks and security against fingerprint template database," international journal of emerging trends & technology in computer science (ijettcs), vol. 2, no. 5, september 2013.

[18] Michael kimwele, stephen kimani joseph mwema, "a simple review of biometric template protection schemes used in preventing adversary attacks on biometric fingerprint templates," international journal of computer trends and technology (ijctt), vol. 20, no. 1, feb 2015.

[19] Ahlal h. Montaser,fawzia elhashmi mohamad abdulmonam omar alaswad, "vulnerabilities of biometric authentication “threats and countermeasures”," international journal of information & computation technology, vol. 4, 2014.

[20] Amitabh wahi s.hemalatha, "a study of liveness detection in face biometric systems ," vol. 91, 2014.

[21] Chris roberts, "biometric attack vectors and defences," journal homepage: www.elsevier.com/locate/cose, 2007.

[22] Jing dong and tieniu tan, "security enhancement of biometrics, cryptography and data hiding by their combinations".