IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710


# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 8, August 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.569

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008180|

# New Approach and Technique for Multimodal Biometric System Recognition

**Nilesh Koli, Vaibhav Dighole**

U.G Student, Department of Information Technology, B.K. Birla College of Arts, Commerce and Science (Autonomous), Kalyan, Maharashtra, India.

U.G Student, Department of Information Technology, B.K. Birla College of Arts, Commerce and Science (Autonomous), Kalyan, Maharashtra, India.

**ABSTRACT:** In today's world it is fact that passwords are no more suitable for security needs of twenty-first century world. It is possible to steal passwords, loose, and forget. Anyone can misuse the password. As an alternative, nowadays, biometric devices are being used for identifying the people. Biometric device uses the physical and behavioral characteristics of the people for identification. There are two types of biometric identifiers. One is physiological characteristics and the other is behavioral characteristics. Biometric technology recognizes an individual based on fingerprints, signature, face, DNA, typing rhythms, or iris. This provides secure and convenient authentication. These systems are in use across many areas like defense, government, finance, banking, consumer electronics, home safety, healthcare, etc.

Internet-based applications like online banking and other e-commerce applications are making biometric as the first and convenient choice. Future scope of biometric in each and every aspect of life is limitless and it is aimed toward improved security and protection of data that is personal. The research in biometric has gained momentum as security needs are increasing for protection of personalised information. Biometrics research is boosted further because of the interest shown in this technology by government, consumers, and other enterprises. Multimodal biometric systems provide better security and convenience to the users compared to traditional methods of authentication.

**KEYWORDS:-** Iris, Biometric, Gait, DNA recognition, retina recognition, fuzzy fusion, body odor recognition, etc.

## I. INTRODUCTION

Biometric-system evaluation quantifies how well bio-metric systems accommodate these properties.Typically, biometric evaluations require that an inde-pendent party design the evaluation, collect the testdata, administer the test, and analyze the results.We designed this article to provide you with suffi-cient information to know what questions to ask whenevaluating a biometric system, and to assist you indetermining if performance levels meet the require-ments of your application. For example, if you plan touse a biometric to reduce—as opposed to eliminate—fraud, then a low-performance biometric system maybe sufficient. On the other hand, completely replacingan existing security system with a biometric-based onemay require a high-performance biometric system, orthe required performance may be beyond what current technology can provide.Here we focus on biometric applications that givethe user some control over data acquisition. Theseapplications recognize subjects from mug shots, passport photos, and scanned fingerprints. Examples notcovered include recognition from surveillance photosor from latent fingerprints left at a crime scene.Of the biometrics that meet these constraints, voice,face, and fingerprint systems have undergone the moststudy and testing—and therefore occupy the bulk ofour discussion. While iris recognition has receivedmuch attention in the media lately, few independentevaluations of its effectiveness have been published.

## II. FEATURES

With the push to a digital world, more and more SMEs and start-ups are automating their routine day-to-day tasks. While most organisations today use a card reader and other digital devices, they still rely on manual time tracking and complex spreadsheets to monitor the time and attendance of employees. Time-consuming and labour-intensive, manual time tracking is not only difficult but also curbs the future growth and expansion of your business. Your organisation can reach its full potential only when you create an efficient internal system that is scalable and effective.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008180|

Moving to a biometric attendance system is the first step in your journey to enhance the security of your organisation and increase the productivity of your employees. With plenty of biometric access control systems in the market.

2.**1** Access Control
Apart from time-tracking system, biometric systems can also be used for security purposes like restricting non-authorised personnel into protected areas of the building. Look for devices that have integrated access control functionalities. Integrated systems lead to enhance the productivity as well as security of the organisation.

2.2 User Capacity
Look for a biometric attendance system that can store and verify a large number of templates (fingerprints, face, palm, etc), even if your organisation has just a few employees currently. This way, the device will be able to enrol new employees as your business grows over the years.

2.3 Connectivity
Internet connectivity is a required feature of the biometric machines. Readers transfer clock-in and clock-out time of the individual employees to the attendance and HR payroll system. When it comes to updating the system and keeping it working without bugs in the future also, internet connectivity is mandatory. As we are talking about connectivity, USB connectivity can be additional to have back up of the data quickly using an external device.

2.4 Identification Time
The success of a biometric attendance system depends on the time taken for the identification by the biometric machine. Look for devices that sense fingerprints quickly within a fraction of a second and auto push the data to the server for accurate time of the attendance. For example, Matrix COSEC Face Recognition takes <2 sec to identify an individual.

2.5 Durability and Ruggedness
Look for devices that are rugged, durable, and can work in extreme temperatures especially if your organisation attracts a lot of dirt and dust. Some fingerprint time-attendance systems like Matrix **COSEC ARGO** come with scratch-proof optical sensors and waterproof. This ensures that irrespective of environmental factors and handling, the time-attendance system always works perfectly. Further, you should also check for dust or water resistance in your solution.

2.6 Integration to Payroll Management Systems
The data from the system plays a vital role in improving the efficacy of HR payroll management systems. With precise attendance details of employees, it's easier for the HR team to compute employee salaries quickly and perfectly. Go for systems that send data directly to the HR payroll software, thus, simplifying payroll computations.

2.7 Support
While biometric attendance systems are easy-to-install and easy-to-use, there may be instances when you would face some issues and require expert assistance. Always purchase your device from reputed companies like Matrix, which offer you both online support and offline service support.

## III. RESEARCH ON DIFFERENT BIOMETRIC SYSTEM

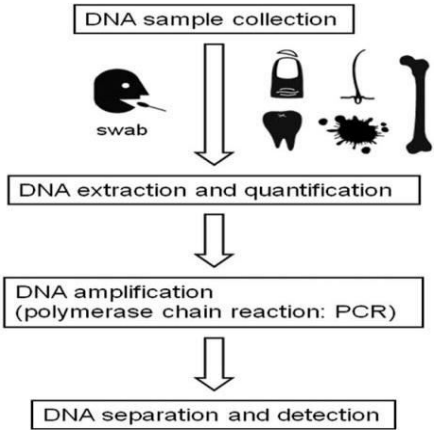
3.1 DNA biometric recognition
DNA is an increasingly useful biometric, and is encountered most often in forensics and healthcare.

For forensics, current DNA identification technologies measure short tandem repeat sequences (STRs) in the nuclear or mitochondrial DNA. The chosen STR sequences (typically 13 or more) are not linked to any known genetic characteristic, but vary from person to person in accordance with well-known population statistics. For this reason, measuring the lengths of these STRs provides a highly accurate and easily stored attribute that can be compared to others for potential identification, lead generation, exclusion, or family matching of an individual or individuals.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008180|




Determining the lengths of the STRs in a DNA sample involves some fairly advanced chemistry and associated processes. Before the advent of rapid DNA identification technology, this work was confined to certified laboratories with trained technicians and six different specialized laboratory instruments. Results usually came back after several days. Recent rapid DNA identification technologies have reduced this process down to one portable desktop instrument with automated processing taking about 90 minutes.

3.2 Gait Recognition

Gait recognition is based on the notion that each person has a distinctive and idiosyncratic way of walking, which can easily be discerned from a biomechanic viewpoint. Human movement does consist of synchronized movements of hundreds of muscles and joints, though basic movement patterns are similar, gait does vary from one person to another in terms of timing and magnitude.

As a consequence, minor variations in gait style can be used as a biometric identifier to identify individuals.
Gait recognition groups spatial-temporal parameters, such as step length, step width, walking speed and cycle time with kinematic parameters, such as joint rotation of the hip, knee and ankle, mean joint angles of the hip, knee and ankle and thigh, trunk and foot angles. Also considered is the correlation between step length and the height of an individual.
Because human ambulation is one form of human movements, gait recognition is closely related to vision methods that detect, track, and analyze human behaviors in human motion analysis. Gait recognition technologies are currently in their infancy. Currently, there are two main types of gait recognition techniques in development.

The first is gait recognition based on the automatic analysis of video imagery. This approach is the most popular approach studied and involves analysis of video samples of a subject's walk and the trajectories of joints and angles. A mathematical model of the motion is created, and is subsequently compared against other samples in order to determine identity.

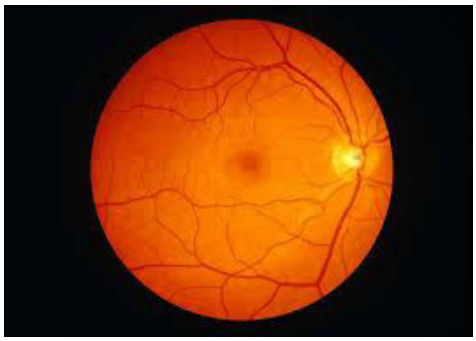
| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008180|

The second method uses a radar system, which records the gait cycle that the various body parts of the subject creates. This data is then compared to other samples in order to perform identification.
In both models, human body analysis is employed in an unobtrusive way using technical instrumentation that measures body movements, body mechanics and the activity of specific muscle groups.

3.3 Eyes retina recognition
A retinal scan is performed by casting an unperceived beam of low-energy infrared light into a person's eye as they look through the scanner's eyepiece. This beam of light traces a standardized path on the retina.



Once the scanner device captures a retinal image, specialized software compiles the unique features of the network of retinal blood vessels into a template. Retinal scan algorithms require a high-quality image and will not let a user enroll or verify until the system is able to capture an image of sufficient quality. The retina template generated is typically one of the smallest of any biometric technology.

Retinal scan is a highly dependable technology because it is highly accurate and difficult to spoof, in terms of identification. The technology, however, has notable disadvantages including difficult image acquisition and limited user applications. Often enrollment in a retinal scan biometric system is lengthy due to requirement of multiple image capture, which can cause user discomfort. However, once user is acclimated to the process, an enrolled person can be identified with a retinal scan process in seconds.

Retinal scan technology has robust matching capabilities and is typically configured to do one-to-many identification against a database of users. However, because quality image acquisition is so difficult, many attempts are often required to get to the point where a match can take place.

Retinal scan devices are mainly used for physical access applications and are usually used in environments requiring exceptionally high degrees of security and accountability such as high-level government, military, and corrections applications. Retinal scanning has been utilized by several U.S. government agencies including the Federal Bureau of Investigation (FBI), the Central Intelligence Agency (CIA), and NASA.

3.4 Fuzzy Fusion:-
Decision level fusion
The authentication system is composed of two modules AFAS to realize a multimodal authenticationsystem combining the obtained scores from the single systems, Figure 4. With more details, the proposed authentication system is composed of "AFAS1"

subsystem that performs index fingerprint processing and recognition, and of "AFAS2" subsystem that performs the middle finger's fingerprint recognition and processing.

The proposed and implemented fusion module uses the fuzzy logic principles and methods to combine the scores products by two subsystem AFAS [11]. Fuzzy logic processes imprecise information like human thinking and it allows to obtain intermediate values between true and false, accepted and refused, by partial membership set. A fuzzy inference system composed of two input and one output variables has been implemented. The output represents the decision taken by whole system

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008180|

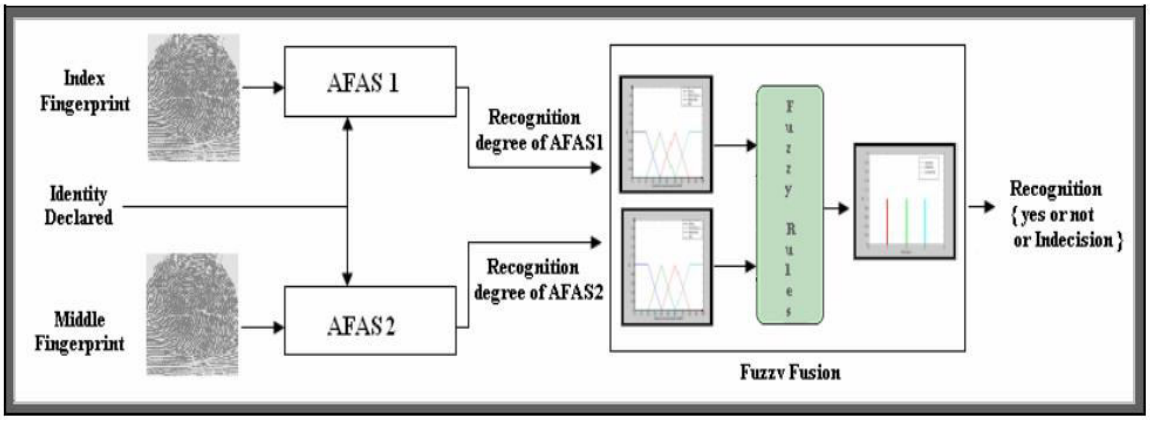



Fig.4. The general scheme of the proposed system architecture with decision fusion

Matching score level fusion

The proposed system architecture is composed of two AFAS modules and the fusion is realized combining the matching score of both AFAS and the quality measure of fingerprint images. The fusion has been obtained by a fuzzy system with four input and one output variables. The output variable represents the decision of the whole system. The fuzzy system uses the knowledge base built with above fuzzy rules. Each rule has the following common guidelines: − if the input images have good quality and fingerprints are very similar to the stored fingerprints then certainly the user is who he/she claims to be.

− if the input images have good quality and fingerprints are not very similar to the stored fingerprints then certainly the user is an impostor".

− if AFAS1 works with an input bad quality image and AFAS2 works with an input

good quality image then the AFAS2 decision will be more discriminant than AFAS1. The figure 5 shows the scheme of the proposed architecture with matching score level fusion

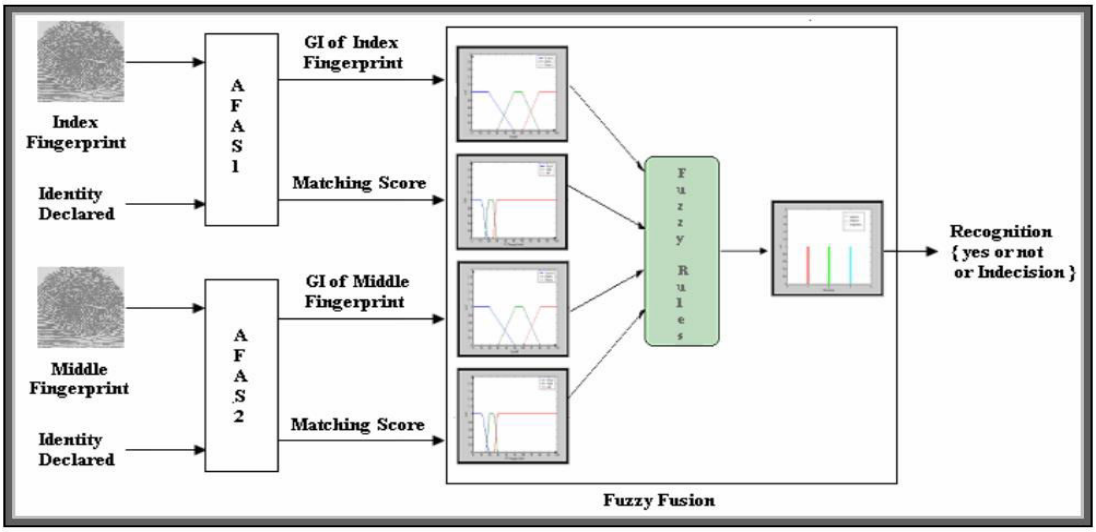



Fig.5. General scheme of the proposed architecture with matching score level fusion.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008180|

3.5 Human body odor

Every human body exudes an odor that characterizes its chemical composition and which could be used for distinguishing various individuals. That means, body odor is one of the physical characteristics of a human that can be used to identify people. The human odor is released from various parts of body and exists in various forms such as exhalation, armpits, urine, stools, farts or feet. The study of odors is a growing field but is a complex and difficult one. The complexity of odors arises from the sensory nature of smell. The perception of odor sensation is

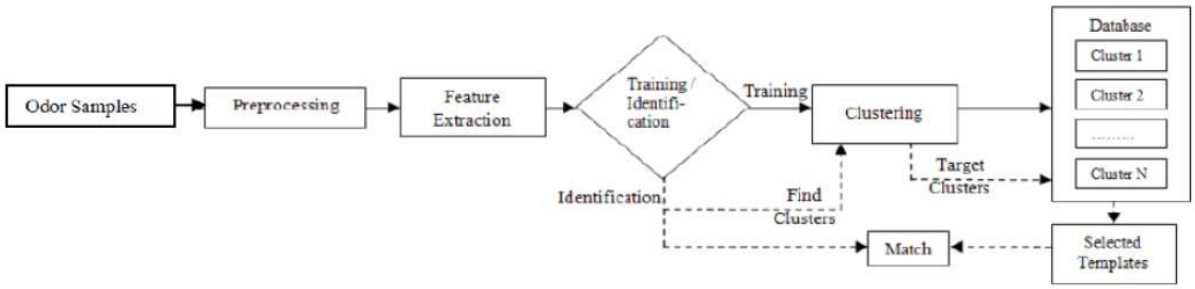



Fig 3: A Typical Odor Biometric Identification System
Source: Natale et al (2000)

hard to investigate because exposure to a volatile chemical elicits a different response based on sensory and physiological signals, and interpretation of these signals influenced by experience, expectations, personality or situational factors. Odors are mixtures of light and small molecules that, coming in contact with various human sensory systems, also at very low concentrations in the inhaled air, are able to stimulate an anatomical response: the experienced perception is the odor.

## IV. FUTURE

Like any emerging technology, biometrics offers numerous benefits and also raises legitimate concerns. On the plus side, biometrics frees consumers and businesses as well as citizens and governments from the burden of constantly having to prove that you are who you say you are. Biometrics opens the door to a password-free, key-free, and PIN-free world where all you need to do is speak, look, or touch in order to be identified and verified. Since biological characteristics are unique to each individual, they cannot be easily forged or stolen. And to protect against possible spoofing (voice mimic, face photo), many biometric systems require the authentication scan, imprint, conversation, to be "live."In short, biometrics is a better way and in the long run, a more efficient way to verify a person's identity and assure access security.

For example:

Business offices, factories, and educational institutes are using biometric attendance systems to track employee clock-in/out time. With biometrics, buddy punching (when a co-worker clocks in/out on your behalf) and timesheet manipulation are no longer possible.

Casinos are employing face recognition to monitor people as they enter and leave the property. Known trouble-makers or banned gamblers are identified the second they step across the threshold, so security wastes no time in escorting them off the premises.

Banks and financial institutes are one of the biggest beneficiaries of biometric technologies– or should we say, their customers are. Biometrics makes identity theft impossible while eliminating the need to remember passwords, PINs, and security keys to authenticate customers and process their transactions, whether online or on site.

## V. CONCLUSION

The majority of conventional biometric systems (iris scanners ,voice recognition, fingerprint/hand geometry, etc) can only assure that the correct user is present at the time of login. Indeed, such systems perform much better than the haptic identification systems studied in this report however, after a user logs in, these systems have no way to detect if the correct user is still present. The haptic verification systems overcome this difficulty. During the usage of the haptic application, our haptic-biometrics system can determine continuously and as needed whether the user who is using the system is still the user that originally logged in. This operation is applicable to high-security environments, where each manipulation of the system would ideally be followed by identity conformation/rejection. We also believe that the

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008180|

haptic biometric system can be improved by incorporating an adaptive feedback between the feature extraction and feature selections process. Adaptive feedback can be developed based on the nature of the requirements of the haptic based application but also by the preliminary analysis from the relative entropy approach.

## REFERENCES

1. T. Mansfield, G. Kelly, D. Chandler, J. Kane, "Biometric Product Testing" Final Report, Centre for Mathematics and Scientific Computing National Physical Laboratory Queen's Road Teddington Middlesex , 2001.
2. O.C. Kurban, T. Yildirim, A. Bilgiç, A multi-biometric recognition system based on deep features of face and gesture energy image, in *2017 IEEE International Conference on Innovations in Intelligent Systems and Applications (INISTA)*. IEEE (2017)
3. Qiang Zhang and Xiaopeng Wei, *A novel couple images encryption algorithm based on DNA subsequence operation and chaotic system*, pp. 6276-6281, 2013.
4. Zheng, S.: CASIA Gait Database collected by Institute of Automation, Chinese Academy of Sciences, CASIA Gait Database
5. Kusakunniran, W., Zhang, J., Wu, Q., Li, H.: Multiple Views Gait Recognition using View Transformation Model of Gait Energy Image. In: Second IEEE International Workshop on Tracking Humans for the Evaluation of their Motion in Image Sequences (THEMIS 2009): a workshop in ICCV 2009, pp. 1058–1064 (2009)
6. Goh, K.G., Lee, M.L., Hsu, W., Wang, H.: ADRIS: An Automatic Diabetic Retinal Image Screening System. In: Medical Data Mining and Knowledge Discovery, Springer, Heidelberg (2000)
7. Li, H., Chutatape, O.: Automated feature extraction in color retinal images by a model based approach. IEEE Trans. Biomed. Eng. 51, 246–254 (2004)
8. P. Verlinde, G. Chollet, and M. Acheroy, "Multi-Modal Identity Verification Using Expert Fusion", Information Fusion, 1(1):17-33, July 2000.
9. Baldisserra, D., Franco, A., Maio, D., & Maltoni, D. (2005). Fake Fingerprint Detection by Odor Analysis. In Zhang, David and Jain, Anil (Eds.)., *Advances in Biometrics: Lecture Notes in Computer Science. Volume 3832/2005*. (pp. 365--272). Berlin: Springer.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.569

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details