International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 03 | March - 2022 ISSN: 2582-3930

Biometric System and Recognition

Mentor – Mrs. Vidya
Assistant Professor
Department of CSE
Alvas Institute of Engineering and Technology

Anush Shetty
B. E
Department of CSE
Alva's Institute of Engineering and Technology,
Mijar, Moodbidri

Adarsha N Y
B. E
Department of CSE
Alva's Institute of Engineering and Technology,
Mijar, Moodbidri

Abhishek Joshi
B. E
Department of CSE
Alva's Institute of Engineering and Technology,
Mijar, Moodbidri

Sudarshan Shetty
B. E
Department of CSE
Alva's Institute of Engineering and Technology,
Mijar, Moodbidri

Abstract – In this paper, the emerging requirements of reliable and highly accurate personal identification in a number of government and commercial applications (e.g., international border crossings, access to buildings, laptops and mobile phones) have served as an impetus for a tremendous growth in biometric recognition technology. Biometrics refers to the automatic recognition of an individual by using anatomical or behavioral traits associated with that person. By using biometrics, it is possible to recognize a person based on who you are, rather than by what you possess (e.g., an ID card) or what you remember (e.g., a password). Biometrics is automated recognition of individuals based on their behavioral and biological characteristics", a vulnerability in biometric security results in incorrect recognition or failure to correctly recognize individuals. This paper presents a framework for integrating the ancillary information with the output of a primary biometric system.

Keywords – Biometrics, recognition, biometric security and sensors, computer vision.

I. INTRODUCTION

Biometric systems automatically recognize individuals based on their physiological and/or behavioral characteristics like fingerprint, face, hand-geometry, iris, retina, palm-print, voice, gait, signature, and keystroke dynamics. Biometric systems that use a single trait for recognition, called unimodal biometric systems, are affected by problems like noisy sensor data, non-universality and/or lack of distinctiveness of the chosen biometric trait, unacceptable error rates, and spoof attacks. Some of the problems associated with unimodal biometric systems can be overcome by the use of multimodal biometric systems that combine the evidence obtained from multiple sources. A multimodal biometric system based on different biometric identifiers like fingerprint, iris, face, and hand-geometry can be expected to be more robust to noise, address the problem of non-universality, improve the matching accuracy, and provide reasonable protection against spoof attacks. However, such a system will require a longer verification time thereby causing inconvenience to the users.

This concentrates on system vulnerabilities which are a consequence of this core biometric challenge. Since biometric systems are implemented on server computers, they are vulnerable to all cryptographic, virus and other attacks which plague modern computer systems. A practical biometric system should meet the specified recognition accuracy, speed, and resource requirements, be harmless to the users, be accepted by the intended population, be easy to use and be sufficiently robust to various fraudulent methods and attacks on the system. Biometrics are believed to provide solutions to a wide range of problems involving identity checking in the context of national ID programmers' in developing countries.

II. BIOMETRICS SECURITY OVERVIEW

Biometric security is a security mechanism that identifies people by verifying their physical or behavioral characteristics. It is currently the strongest and most accurate physical security technique that is used for identity verification. Biometrics are mainly used in security systems of environments that are subject to theft or that have critical physical security requirements. The biometric technology currently used most often in physical access control is fingerprint recognition because of its lower price. For high-security environments, iris recognition provides the best accuracy, followed by palm vein recognition. Some biometric security systems verify identities using one or more detection technologies, while others don't verify the identity at all to keep costs low.

Fig 1 – Categories of Biometrics Security

The benefits that biometric security systems offer are:

- Biometric systems strengthen security - One of the key benefits of biometric security devices is that they can help to increase your protection. It’s much harder, for example, to clone or steal a fingerprint than an access card. In situations where you need to increase security, biometrics can also be used for multifactor verification. After someone’s presented their badge, for example, they then need to present their fingerprint to verify that they are who they claim to be. This is safer than using a PIN for verification as that can easily be passed to other people.
- Biometric systems improve convenience - Biometric security systems can also offer users more convenience. It’s easy to forget a card or key, but you always have your biometrics with you. And if the identifier allows handsfree or long-distance recognition, the convenience levels increase further – you may be allowed to enter your building simply by having your face scanned as you pass the entrance.
- Privacy - As biometrics are classified as sensitive personal data in European General Data Protection Regulation (GDPR), it’s important to use and store biometric information in line with local regulations. In some countries, for example, you’re not allowed to store any biometric data in a central database.

Biometric systems will, undoubtedly, be used increasingly more in physical access control in the coming years. Especially as technology develops to mitigate some of the risks that remain.

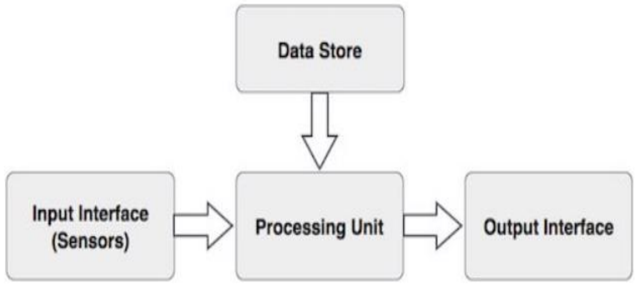

Fig 2 – Basic Components of a Biometric System

III. CLASSIFICATION OF BIOMETRICS TECHNIQUES

There are a few Biometrics techniques which are extensively characterized and used are discussed here. Note that the accuracy estimates of biometric systems are dependent on a number of test conditions (e.g., population characteristics and specific sensors used).

1. Fingerprint
2. Face
3. Voice
4. Iris

A. FINGERPRINT BIOMETRIC

Fingerprint security systems is a good option to put into place because they tend to be difficult to hack, as there is not a password or any sort of data to input. Rather, fingerprint security systems utilize biometric technology. Every individual has their own unique features, in particular, their own unique fingerprint. Utilizing fingerprint access control technology allows businesses to build a secure workplace with regulated access to certain buildings or rooms.

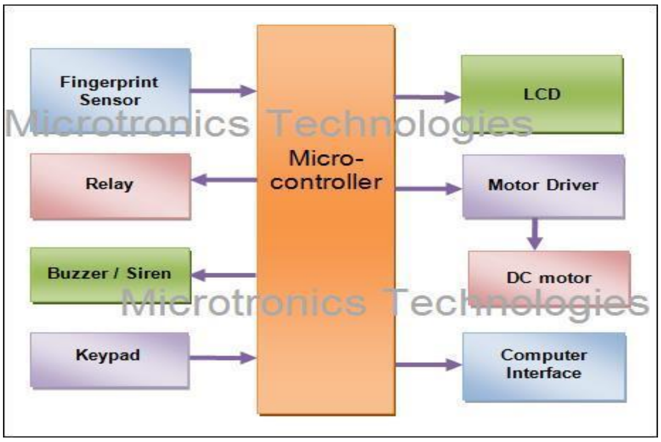

Fig 3 – Block Diagram for working of a Fingerprint Sensor

A new approach based on local texture pattern is proposed uses multi-scale Local Binary Patterns and Local Derivative Patterns as feature extraction techniques. Since palm vein feature extraction is a challenging problem in hand pattern recognition this approach promises for better results. Fingerprint based security system is the most secured system as compared to other systems. Reason is that RFID card or Keys of lock can be stolen, password may be leaked. However, thumbnail of every human being is unique, so lock will not open unless the same person is present to give the impression of fingerprint. One of the main advantages is that this system remembers the stored password even if the power supply is turned off. Using Fingerprint saves time to gain access as compared to other methods like RFID card, Password or Key. We can send this data to a remote location using mobile or internet. We can use non-contact fingerprint sensor. Which is also called as touchless 3D fingerprint scanner. We can implement other related modules like fire sensor, GSM modem.

B. FACE BIOMETRIC

A facial recognition system is to identifying or verifying a person from a digital image automatically. A number of algorithms have been proposed for face recognition. Different existing techniques for human face recognition can be summarized. Such algorithms divided into categories of geometric feature-based and appearance-based methods. Eigen faces used for recognition. Nonetheless, like any other technology, facial recognition isn’t impeccable. Deep learning algorithms applied to most of these systems.

Facial analysis algorithms enable security cameras to learn your household's regular faces. This makes for more seamless system control (the camera can "recognize" you at the door and disarm the alarm) and increases the detail of alerts.

Fig 4 – Facial Recognition System Concept

At present face recognition systems which are used impose a number of restrictions on how facial images are obtained. These systems automatically detect the correct face image and are able to recognize the person.

Let’s see how the facial recognition works:

a. The face detection process is an essential step in detecting and locating human faces in images and videos.
b. The face capture process transforms analog information (a face) into a set of digital information (data or vectors) based on the person's facial features.
c. The face match process verifies if two faces belong to the same person.

A newly emerging trend is three-dimensional (3D) face recognition which declared to achieve improved accuracies. This technique used 3D sensors to capture shape of face. Advantage of 3D facial recognition is that it is not influenced by changes in lighting. Face detection and face match processes for verification / identification are speedy.

C. VOICE BIOMETRIC

Voice authentication is a form of biometric authentication. Voice recognition is a form of biometrics, and voice authentication is the use of a user’s speech to authenticate users. Voice and user speech can serve as a unique marker of a user’s ID. The voice recognition system is the capacity of a device or program to receive and understand dictation, or to understand a spoken instruction. When this system is used with a computer, analog signal must be converted into digital using ADC. In a computer, a digital data base, syllables and vocabulary of words and syllables are required to decode the signal. The forms of the speech are stored on the hard drive and loaded into memory when the program is run. The stored forms are checked by the computer against the o/p of the analog to digital converter.

The speech of person changes over time due to age, medical/physical conditions, and emotional state. Different text dependent and text independent techniques have been used for recognition. Text-dependent systems based on Hidden Markov Model (HMM) using Gaussian or multi-Gaussian distributions are more popular. Voice authentication carries many of the same advantages of other biometrics, including:

1. Harder to fake than other forms of authentication. A password can be stolen, and a token can be copied or forged if security isn’t kept tight. Biometric data is much harder to fake, all things being equal, and it is much harder to steal through practices like broad phishing attacks.

2. Supports streamlined user experience. Logging into a system shouldn’t be difficult, regardless of whether or not it’s one of your employees or one of your clients or customers. With biometrics, secure authentication methods can rely on the person just being there, rather than remembering a complex password.

3. Accessible and convenient on a variety of devices. Biometrics are becoming incredibly common on devices like laptops, tablets or smartphones. That makes it that much easier to integrate next-level security across a productive device ecosystem for distributed teams.

4. Contactless login. This is something unique to speech recognition (among a few other biometrics like facial scanning). With speech recognition, you don’t have to touch anything–which, as we’ve learned from the pandemic, is a safe and responsible step to take.

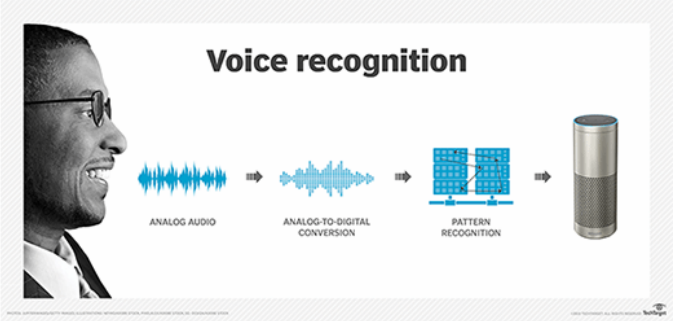

Fig 5 – Voice Recognition System Concept

D. IRIS BIOMETRIC

Iris scanning biometrics measure the unique patterns in the colored circle of your eye to verify and authenticate your identity. Contactless, fast and renowned for its accuracy, biometric iris recognition can operate at long distances, with some solutions that leverage the modality requiring only a glance from a user. The iris usually has a brown, blue, gray, or greenish color, with complex patterns that are visible upon close inspection. A person’s iris pattern is unique and remains unchanged throughout life. Also, covered by the cornea, the iris is well protected from damage, making it a suitable body part for biometric authentication. This technique has been tested for real time implementations.

Some of the features of Iris Recognition technique are:

1. Highly accurate and fast, iris recognition boasts of having top-class precision among different types of biometric authentication technologies.
2. Remains unchanged throughout life. (This does not constitute a guarantee.)
3. Since the iris is different between the left and right eye, recognition can be performed separately by each eye.
4. Because of using an infrared camera, recognition is available even at night or in the dark.

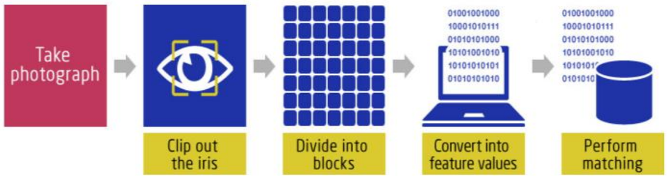

Fig 6 - Mechanism of Iris Recognition Technique

The applicability of iris recognition biometric technology is not only restricted to the security concerns but also pertinent to be applicable in various sectors. The major applications of biometric iris recognition technology involve restricting unauthorized access in the facilities, immigration at the airports, hospitals and clinics, border control system, to unlock various devices and smart phones, aviation security, various government schemes, and many more. It is believed that it is impossible to forge identification data using this method. The fact is that, in addition to the individual pattern of the iris, the human eye has unique reflective characteristics (due to the state of tissues and natural moisture), which are considered in the process of reading information.

IV. COMPARISON AMONG DIFFERENT BIOMETRIC RECOGNITION TECHNIQUE

Recognition Technique	**Advantage & Disadvantage**
Fingerprint Recognition	User Experience – Convenient and fast, Spoof-proof – Biometrics are hard to fake or steal, Data breaches – Biometric databases can still be hacked
Face Recognition	Improved Security, High Accuracy, Data Storage Problems, Disturbance in Camera Angle
Voice Recognition	Security - Every individual has a unique voice, Hardware support - Any device you choose to enroll must have a microphone to support the use of voice biometrics
Iris Recognition	No physical contact when scanning, Accurate matching performance, generally require close proximity to camera

V. CONCLUSION

In this paper, we have studied about automatic human identification has numerous applications in many areas where the identity of person needs. To get the higher or air tight security complex security systems have been developed. In this scenario human identification plays an important role in every field of life. The conventional knowledge-based and token-based methods do not really provide positive person recognition because they rely on surrogate representations of the person’s identity (e.g., exclusive knowledge or possession). It is, thus, imperative that any system assuring reliable person recognition would involve a biometric component. This is not, however, to state that biometrics alone can deliver error-free person recognition. In fact, a sound system design will often entail incorporation of many biometric and non-biometric components (building blocks) to provide reliable person recognition. As biometric technology matures, there will be an increasing interaction among the market, technology, and the applications. Based on this understanding, a biometric requirement list was developed to include: original biometric image must be destroyed, biometrics must be encrypted, biometrics used only for verification, fingerprint image cannot be reconstructed, and finger cannot be used as a unique ID. At the same time, biometric systems are being used in many scenarios with high security value. Recent work in standards bodies has given much thought to security standards for biometrics. However, biometrics can also provide (with careful use) the identity assurance that is foundational to systems security. This shows that in examining biometric errors it is not always possible to make clear distinctions between the effects of images databases, algorithms, system settings, and operators’ practices. The relationships between biometric technologies, gender and ethnicity are emergent, multiple and complex. While this also entails that the political effects of biometric recognition practices are messier than is sometimes assumed, there are a number of issues that require attention.

VI. REFRENCES

[1] Jain, A.K., Ross, A., Prabhakar, S.: An Introduction to Biometric Recognition. IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics 14, 4–20 (2004)

[2] Teoh, A.B.J., Goh, A., Ngo, D.C.L.: Random Multispace Quantization as an Analytic Mechanism for Bio Hashing of Biometric and Random Identity Inputs. IEEE Transactions on Pattern Analysis and Machine Intelligence 28(12), 1892–1901 (2006)

[3] B. Kumar, C. Xie and J. Thornton, “Iris verification using correlation filters”, Proceedings of Fourth International Conference on Audio and Video Based Biometric Person Authentication, (2003)

[4] Beveridge, J. R., Givens, G. H., Phillips, P. J. and Draper, B. A. (2009) Factors that influence algorithm performance in the face recognition grand challenge, Computer Vision and Image Understanding, 113(6)

[5] N. K. Ratha, J. H. Connell, and R. M. Bolle. Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal, 40:614{634, 2001.

[6] U. Uludag and A.K. Jain. Attacks on Biometric Systems: A Case Study in Fingerprints. In Proceedings of SPIE Conference on Security, Seganography and Watermarking of Multimedia Contents VI, pages 622{633, San Jose, USA, January 2004.

[7] S. Parashar, A. Vardhan, C. Patvardhan and P. K. Kalra, "Design and Implementation of a Robust Palm Biometrics", Proceedings of Sixth Indian Conference on Computer Vision, Graphics & Image Processing, (2008),

[8] LaFors-Owczinyk, K. and Van der Ploeg, I. (2016) Migrants at/as risk: Identity Verification and risk-assessment technologies in the Netherlands, in: I. Van der Ploeg and J. Pridmore (Eds) Digitizing Identities. Doing Identity in a Networked World, pp. 261–281 (New York: Routledge).

[9] Van der Ploeg, I. (2011) Normative assumptions in biometrics: On bodily differences and automated classifications, in: S. van der Van der Hoff and M.M. Groothuis (eds) Innovating Government - Normative, Policy and Technological Dimensions of Modern Government, pp. 29–40 (The Hague: T.M.C. Asser Press/Springer).

[10] J. Wayman. The cotton ball problem. In Proceedings of Biometrics Consortium Conference, Washington DC, USA,2004