**Biometric Security: Enhancing the security and reliability of biometric authentication systems.**

**Yashaswini Aitha 700777106 , Gayathri Kandukuri 700764360, Vanama Niteesh 700755890, Shaik Tasmin Sultana 700756274, Harshavardhini Bagari 700775039, Dilshad Fathima - 700773370**

**Abstract:**

Biometrics is one of the authentication methods which verifies identity by analyzing unique physiological and behavioral features such as fingerprints, facial recognition, iris scans, voice recognition, and handwritten signatures to authenticate individuals. This method is more convenient and secure than traditional authentication techniques. Biometric systems are incredibly difficult to hack due to the extreme complexity and randomness of biometric data. Nevertheless, improving the security and dependability of biometric systems is essential to achieving their full potential. This study examines methods for strengthening biometric systems, such as using liveness detection, multi-factor authentication (MFA) and advanced algorithms to increase accuracy and prevent fraud. To guarantee continued security and system integrity, focus on the importance of continuous authentication, adaptable performance in all kinds of environmental situations, and periodic system audits. This abstract provides an idea for creating biometric security solutions that are more safe, dependable, and easy to use to lessen the possibility of unwanted access and safeguard private information. The primary concern in Biometric usage is Privacy issues regarding the storage and use of sensitive biometric data, potential for inaccuracies depending on the technology and it could be expensive to implement, especially for smaller organizations or use cases where manual methods are sufficient.

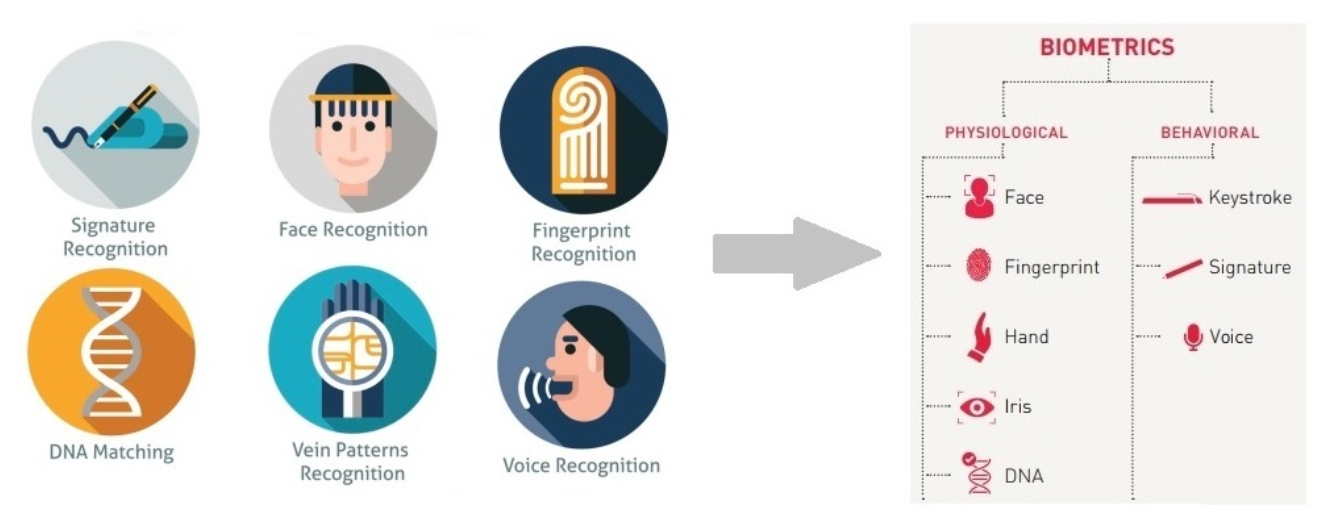
**Introduction:**

Biometric identification makes use of unique biological features like fingerprints, facial recognition, iris scans, and voiceprints to verify individuals' identities. Compared to traditional authentication technologies like passwords or tokens, biometrics offer a less intrusive and more natural method of ensuring safe access control. However, the increasing use of biometric systems has raised concerns over data security, spoofing attacks, and reliability under varied circumstances.

**Benefits of Biometrics:**

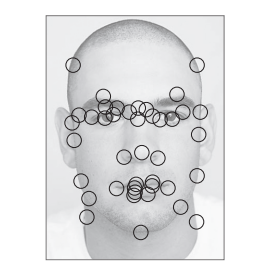
One of the biggest strengths of biometrics in its ability to identify an individual is convenience. Gone are the days when one needs to memorize a password or Personal Identification Number (PIN) code. Biometric authentication is completed by facial scan, fingerprint scan, or some other passive means of recognizing people. The second major strength that's propelling biometric technology onto the curve of adoption is enhanced digital security. An individual's unique physical features are hard to mimic for cybercriminals. This makes biometric-based identity authentication a superior security feature. According to Onfido's 2023 Identity Fraud Report, fraud with biometrics is very low because the technology applies real-time friction to the efforts of cybercriminals to fake an identity. And this heightened sense of privacy/security leads citizens to enroll in online government identity programs.

**Types of Biometric Authentication:**



**Facial Recognition:**

The most common form of secure biometric authentication is facial recognition. Facial recognition is generally used as a standalone security measure. In essence, facial recognition technology involves the citizen's phone camera snapping the individual's face and authenticating the identity of the person by scanning facial geometry and measurements. It confirms the identity of the user when the facial geometry matches facial geometry saved in the company database. The facial features of the user are typically uploaded to the platform at the time of enrollment. Fortunately, most smartphone users already depend on facial biometric technology, so the enrollment would be even less onerous. Anything that lowers friction to identity verification is a blessing for governments seeking to digitalize further. On the downside, such biometric verification will inevitably result in false rejections over time because people's faces change with age. At a later stage, the citizen will have to re-register in the biometrics recognition mechanism if he or she needs to continue using the digital identity solution. It should also be noted that this form of identity verification is literally worthless for those individuals who cannot display their faces due to religious or cultural inclinations.



**Fingerprint Scanning:**

Fingerprint scanning pervades identity confirmation. The technology is used either as the only type of biometric identifier or as a secondary level of protection in a multi-factor setup. According to research published by IEEE, about 75% of people feel comfortable using a fingerprint scanner for identification purposes. In most cases, "flat" fingerprint biometrics, as they are called, are captured by placing one's fingers on a reader device. Identification of a person using this method is easy enough if the registry is face-to-face. Remote application environments for a fingerprint reader are more involved, however. In this method, a "3D" fingerprint is captured using a photograph, which leads to misalignment with the biometric engine. The result is a spurious error. To solve this issue, extensive efforts are being directed towards developing change-inducing technologies that will be able to translate these fingerprint identification information safely in a way that they will become compatible with existing flat registries.



**Voice Recognition:**

Identities can also be authenticated by voice recognition. Phones that have voice recognition capabilities integrated within them can listen to the voice of the user to ensure that it is identical to the sound sample retained on record. This biometric-based authentication is extensively used in e-commerce and banking. Voice is a biological marker and as unique as your fingerprint or iris, so it's very difficult to fake a user's voice, and vocal biometric systems are very secure and guard against cyber attacks. Voice recognition authentication is also simple to use, accurate, and cost-effective.

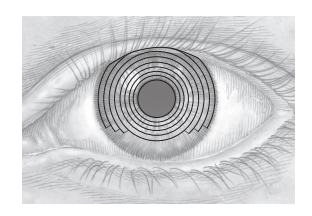


**Behavioral Biometrics:**

In finance, a field from which citizen IDs often borrow, behavioral biometrics is a widely used method for verifying a user's identity. With regards to citizen identity authentication, this type of biometric technology can be utilized as a secondary layer of security in combination with some of the more traditional forms of biometrics. Behavior-based biometric systems create a user profile based on an individual's behavioral characteristics while they are interacting with their device(s). As a few examples of behavioral data that have been collected, take characteristic keystrokes made on a mobile phone, the typical location of the user using the application, gait biometrics, and lip patterns. From these data, a biometric system can make a better estimation of what behaviors are usual for the person. Therefore, if the behavior of the user is straying from "normal" behavior, the user will be alerted to fraud.

**Iris Recognition:**

Although niche, iris recognition is perhaps the most secure and future-proof means of identification authentication. Remarkably, it has been discovered that iris scanners are as much as 99.59% accurate, a sign of how trustworthy the technology is when it comes to safeguarding digital identities. In order to use in identifying an individual, iris recognition requires a mobile camera able to scan the eye using infrared light. Used together with facial recognition, iris scanning is convenient to use for confirming the identity of a citizen because an iris's patterns never change throughout one's life. And there are fewer false rejections when it comes to iris biometrics than with fingerprint sensors.

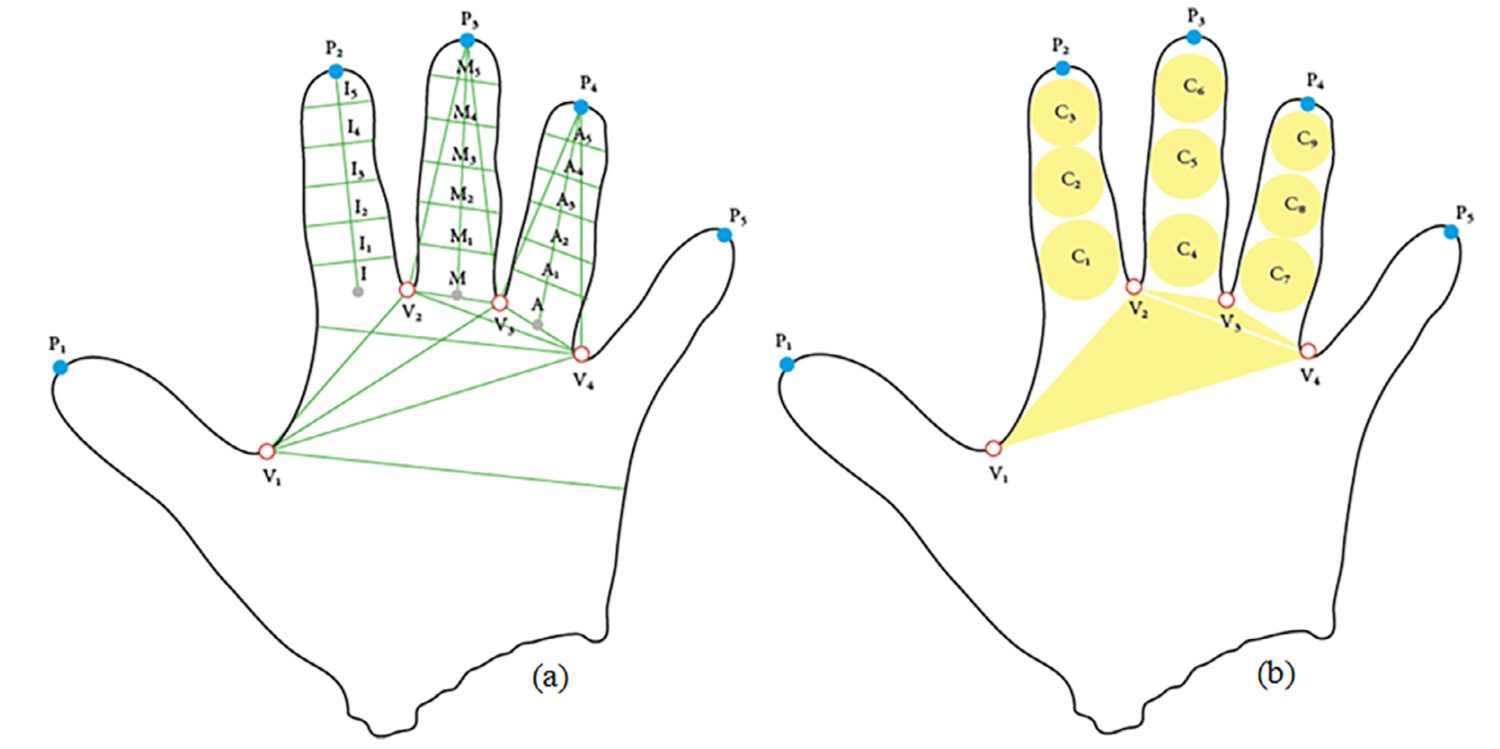


**Vein Recognition:**

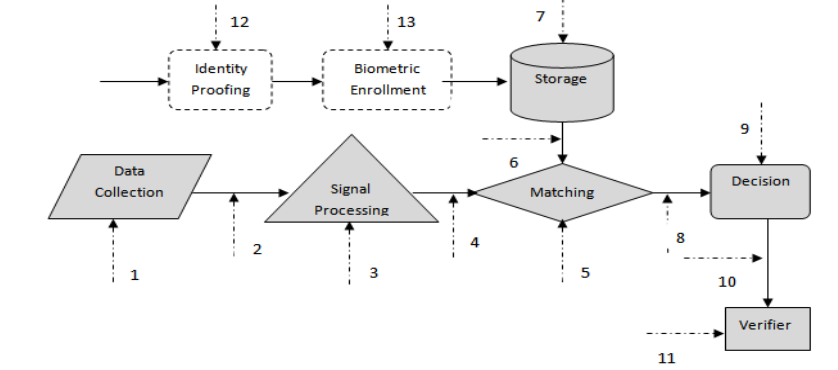
Vein identification, like that of the iris, is very safe for identification verification. Vein recognition employs the unique patterns of an individual's veins. Vein biometrics has been applied in the banking industry since 2004.

So how convenient is vein recognition in identifying an individual?

Since blood vessels are sub-dermal, it is nearly impossible to forge vein recognition. Fujitsu, a Japanese technology giant researching and creating biometric technology, claims vein biometrics yields less than a 0.00008% rate of false rejection in the identification of identities. Vein pattern recognition requires that the user possess a smartphone or tablet with a near-infrared camera. Furthermore, the camera must be capable of detecting the unique patterns of palm, finger, or even eye veins. Once the image of the veins is captured, the biometric app will compare the imagery with the vascular features on file.



**Vulnerable points of biometric systems, Threats and Countermeasures.**



Attacks during processing/interaction [Attack points 1, 3, 5, 9, 11],

|  |  |  |
| --- | --- | --- |
| Location | Threats | Countermeasures |
| 1 Data Collection | Spoofing  Use of un-trusted device  (Device substitution)  Overloading/Flooding  (Denial of Service) | * Liveness Dection * Challenge/Response * Mutually authenticate/use symmetric key or asymmetric key * Rugged devices |
| 3 Signal Processing | Insertion of imposter  data | * Use strong tested algorithms |
| 5 Matching | Component replacement  Insertion of imposter data  “Guessing”(FAR attack)    Manipulation of match score  Hill-climbing | * Signed components * Use strong tested biometric algorithms * Use strong tested biometric algorithms * 1:1 matching * Multi-biometric/ multi-factor * .Debugger hostile environment * Coarse scoring * Trusted sensor(Mutual authentication) * Secure channel |
| 9 Decision | Hill climbing attack  Manipulation of threshold setting  Manipulation of match decision  Component replacement  (“yes machine”) | * Coarse scoring * Mutual Authentication * Secure channel * Protected function(access control) * Data protection * Debugger hostile environment * Sign components |
| 11 Application  (verifier) | Malicious code | * Conform to standards (BioAPI, CBEFF) * Code signing |

Attacks on the biometric data when it is at rest (in memory or in storage)

[Attack points 1, 3, 5, 9, 11 “above” + 7 “below”].

|  |  |  |
| --- | --- | --- |
| 7 Storage | Database compromise  (reading template,  replacing template(s),  changing bindings) | * Hardened server * DB access controls * Sign templates, Store * encrypted templates * Store template on smart cards or other device. |

Attacks between stages (when the biometric data is in transmission)

[Attack points 2, 4, 6, 8, 10].

|  |  |  |
| --- | --- | --- |
| Location | Threats | Countermeasures |
| 2 Raw data transmission  4 Processed data transmission  6 Template retrieval | Eavesdropping attack  Replay attack  Man in the middle attack | * Transmit data over encrypted path/secure channel * Mutually authenticate/use symmetric key or Asymmetric key * Digitally sign data * Utilize Timestamp/Time to Live (TTL) tag * Bind biometric to PKI certificate * Transmit data over encrypted path/secure channel |
| 8 Matching score transmission | Hill climbing attack  Manipulation of match score  Component replacement  (“yes machine”) | * Coarse scores * Trusted sensor (Mutual authentication) * Secure channel * Secure channel * Mutual authentication between matcher and decision * components |
| 10 Communication to application | Eavesdropping attack  Maniplication of match decision | * Transmit data over encrypted path/secure channel * Transmit data over encrypted path/secure channel |

**References:**

[1] K. Jain, K. Nandakumar, and A. Nagar, “Biometric template security,” EURASIP, vol. 8, no. 2, pp. 1–17, 2008.

[2] Jain, A.K., Ross, A., Pankanti, S.: Biometrics: a tool for information security.

IEEE Trans. on Information Forensics and Security 1, 125–143 (2006)

[3] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, Handbook of Fingerprint

Recognition. Springer-Verlag, 2003.

[4] U. Uludag and A. K. Jain, “Attacks on biometric systems: a case study in

finger-prints,” in Proc. SPIE, Security, Seganography and Watermarking of

Multimedia Contents VI, vol. 5306, pp. 622–633, (San Jose, CA),January 2004.

[5] Hao, F., R. Anderson, and J. Daugman, Combining cryptography with

biometrics effectively.

[6] IBG, Vulnerabilities of Biometric Technologies - Transcript of September

Teleconference. 2005.

[7] B. Schneier, “Security Pitfalls in Cryptography,” Proceedings of

the CardTech/SecureTech Conference, CardTech/SecureTech,

Bethesda, MD (1998), pp. 621–626.

[8] B. Schneier, Applied Cryptography, John Wiley & Sons, Inc.,

New York (1996).

[9] J. W. Osterburg, T. Parthasarathy, T. E. S. Raghavan, and

S. L. Sclove, “Development of a Mathematical Formula for

the Calculation of Fingerprint Probabilities Based on Individual Characteristics,” Journal of the American Statistical Association 72, 772–778 (1977).

[10] S. L. Sclove, “The Occurrence of Fingerprint Characteristics

as a Two Dimensional Process,” Journal of the American Statistical Association 74, 588–595 (1979).

[11] D. A. Stoney, J. I. Thronton, and D. Crim, “A Critical Analysis of Quantitative Fingerprint Individuality Models,” Journal of Forensic Sciences 31, No. 4, 1187–1216 (1986).

[12] WSQ Gray-Scale Fingerprint Image Compression Specification,

IAFIS-IC-0110v2, Federal Bureau of Investigation, Criminal

Justice Information Services Division (1993).

[13] N. Memon and P. W. Wong, “Protecting Digital Media Content,” Communications of the ACM 41, No. 7, 35–43 (1998).

[14] F. A. Petitcolas, R. J. Anderson, and M. G. Kuhn, “Information Hiding—A Survey,” Proceedings of the IEEE 87, No.

7, 1062–1078 (1999).