Figure 12: Illustration of Keystroke Dynamics

i) Vein Recognition

Vein recognition is a type of biometrics that can be used to identify individuals based on the vein patterns in the human finger. Vein recognition is a fairly recent technological advance in the field of biometrics. It is used in hospitals, law enforcement, military facilities and other applications that require very high levels of security. Vein recognition biometric devices can also be used for PC login, bank ATM identification verification, and many other applications such as opening car doors. Vein recognition biometrics is a particularly impressive and promising technology because it requires only a single-chip design, meaning that the units are relatively small and cheap. The ID verification process is very fast and contact-less. Using a light-transmission technique, the structure of the vein pattern can be detected, captured and subsequently verified. The user's vein pattern structure is image processed by the device and stored in a relevant data repository in the form of digital data. Many feel that vein recognition biometrics can produce higher accuracy rates than finger print recognition and finger vein patterns are virtually impossible to forge. [6]

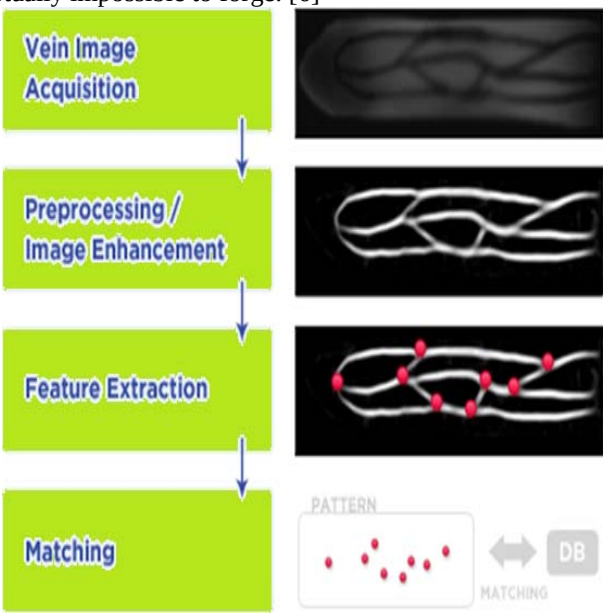

Figure 13: Steps in vein recognition

Figure 14: Vein recognition

j) Signature Recognition

The authentication of an individual by the analysis of handwriting style, in particular the signature. There are two key types of digital handwritten signature authentication, Static and Dynamic. Static is most often a visual comparison between one scanned signature and another scanned signature, or a scanned signature against an ink signature. Technology is available to check two scanned signatures using advances algorithms. Dynamic is becoming more popular as ceremony data is captured along with the X,Y,T and P Coordinates of the signor from the signing device. This data can be utilized in a court of law using digital forensic examination tools, and to create a biometric template from which dynamic signatures can be authenticated either at time of signing or post signing, and as triggers in workflow processes. [7]

Figure 15: Signature Recognition

3. Advantages of Biometrics

As biometrics technology gets more advanced and sophisticated, a greater number of advantages of biometrics used for security purposes and data protection in the workplace are being identified. Basically, biometrics technology is an automated method of monitoring access based on physiological or behavioural characteristics used for recognition and verification. Many different versions of biometric security have been developed, including identification by fingerprints, face, iris/retina, hand geometry, and voice verification. Here are some of the advantages that biometrics offer over more traditional security practices. [8]

- Identification is accurate. Unlike other security systems that rely on passwords or smart cards, one of the greatest advantages of biometrics is the accuracy it provides. When the system is set up correctly, biological characteristics like fingerprints and retinal scans provide completely unique data sets that cannot be replicated easily. This makes it very difficult for anyone but an authorized user to gain access without permission.
- Employee tracking. Since biometrics systems are essentially automatic and therefore data tracking is simple to implement, they offer employers and managers great opportunities for oversight concerning daily activities and operations. Certain events, transactions, and other activities are linked to a specific person, making it possible for employers to track chains of events. Biometrics can also significantly cut down on certain dishonest employee practices that can really eat away at a company's bottom line, such as buddy punching and other forms of fraud.
- Biometrics methods offer convenience. Some other advantages of biometrics products concern the efficiency and convenience they lend to access control. Passwords and pins are easily forgotten, can be written down and subsequently stolen, and are sometime hacked. Once obtained, they can be easily used by someone other than the authorized person. Smart cards and keys can similarly be lost or stolen, and can also be used by an imposter without detection. But with biometrics, something like fingerprints won't be lost and can't be easily obtained and replicated by someone trying to illicitly gain access.
- Systems are user friendly. Once they've been installed and implemented, biometrics systems are able to identify people very rapidly, uniformly, and reliably. Typically, only minimum training is needed to get the system operational, and there's no need for expensive password administrators. In addition, high-quality systems don't tend to need a large amount of maintenance, further cutting costs.

Table 1: Strengths of each methods.

Technique	strengths
Fingerprint	Mature technology; highly accurate; low cost; small size, becoming widely acceptable
Hand Geometry	accurate and flexible; widely acceptable to users
Voice Recognition	Usable over existing telephone system; good for remote access and monitoring;
Face Recognition	Widely acceptable to users; low cost; no direct contact; passive monitoring possible
Iris Scan	Highly accurate; works with eyeglasses; more acceptable to users than retina scan
Retina Scan	Highly accurate
Keystroke Authentication	Widely acceptable to users; low cost; uses existing hardware
Vein Recognition	More precise than fingerprint and accurate also
Signature Recognition	Widely acceptable to users

4. Issues in Biometrics

The use of biometrics is centuries old as the need for unique identification of individuals has existed throughout history. The more recent examples of its use are of Frenchman Alphonse Bertillon who developed "Anthropometrics" in 1888 and the Englishman Edward Henry who in 1900 used fingerprints for the first time to classify and identify criminals. However, since the tragic events of 9/11 biometric technology has been gaining popularity as the public now expects greater security. Additionally, there are some tangible benefits in the use of biometrics. For example, it is unique, convenient and fulfils the need for strong authentication. The main applications so far are governmental, e.g. ID Cards, e-passports, e-borders, air and port security and policing systems. Among the commercial enterprise the leading users are the travel industry, transport and financial services. However, there are serious ethical issues in the use of biometric technology. The main issues concern the personal privacy, the conflict with one's beliefs and values and the collection, protection and use of personal biometric data. The civil liberty organisations argue that the technology undermines the human rights for privacy and anonymity. It is intrusive and has the capability to make serious impact on personal freedom and democratic rights. The technology is prone to failure and is not fake proof as it can be spoofed. But due to many issues and threats around the world, e.g. threat of terrorism, identity theft and fraud, security, illegal immigration, benefit fraud and crime prevention and detection issues, it has become important to have the capability to freeze someone identity for later identification and verification. At the same time since 9/11 the biometric technology has advanced tremendously. The hardware has improved in design and accuracy, the prices have come down and, therefore, biometrics has firmed its place in the security world. The public concern regarding the issues mentioned above cannot be ignored. There is a compelling need to find "Workable and Deployable" solutions to these issues. The academics have a very important role to play through consultations, workshops and student education. [9]

5. Conclusion

Biometrics is a new advance technology which has improved time to time to meet the changing requirements. It is having major impact in security, authentication systems and also privacy. From fingerprint to signature the technology has augmented by its own features. Though there are some ethical and social issues being faced, no one can reject the statement that the technology has helped the human kind a lot.

References

[1] http://www.isaca.org/Journal/Past-Issues/2004/Volume 4/Documents/jpdf044-Biometrics-AnOverview.pdf
[2] Jammi Ashok et. al. / (IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 07, 2010, 2402-2408, AN OVERVIEW OF BIOMETRICS
[3] http://www.cse.wustl.edu/~jain/cse571-11/ftp/biomet.pdf
[4] http://www.globalsecurity.org/security/systems/biometrics-eye_scan.htm
[5] http://www.idcontrol.com/keystroke-biometrics
[6] http://findbiometrics.com/solutions/vein-recognition/

[7] http://www.biometricsinstitute.org/pages/types-of-biometrics.html
[8] http://enlightenme.com/advantages-of-biometrics/

Author Profile

Akshatha M A, Graduate in Computer science and Engineering from ATME College of Engineering under Visveshvaraya Technological University (VTU).