Review of Recent Recognition Systems

Seelam Prabhu Das
Associate Professor
Department of Electronics and Communication Engineering
Srinivasa Institute of Engg;&Tech., Cheyyeru,Amalapuram , AP, India.

Boda Ravi
Assistant Professor
Department of Electronics and Communication Engineering
Sri Chaitanya College of Engg., Karimnagar , AP, India.

Abstract - As technology and services have developed in the modern world, human activities and transactions have proliferated in which rapid and reliable personal identification is required. Examples include passport control, computer login control, bank automatic teller machines and other transactions authorization premises access control, and security systems generally. All such identification efforts share the common goals of speed, reliability and automation. The technology is designed to automatically take a picture from the passengers and match it to the digitized image stored in the biometric passports. Recently, US government is also conducting a Registered Travelers Program which uses a combination of fingerprint and iris recognition technology to speed up the security check process at some airports [23].In the field of financial services, biometric technology has shown a great potential in offering more comfort to customers while increasing their security. This Paper presents the overview of all recognition systems.

Keywords — Voice print, chaotic morphogenesis, Authentication, smart card, Vein recognition.

I. INTRODUCTION

A biometric system provides automatic recognition of an individual based on some sort of unique feature or characteristic possessed by the individual. The developments in science and technology have made it possible to use biometrics in applications where it is required to establish or confirm the identity of individuals. In recent years, biometric identity cards and passports have been issued in some countries based on iris, fingerprint and face recognition technologies to improve border control process and simplify passenger travel at the airports. In UK and Australia, biometric passports based on face recognition are being issued [22]. As an example, banking services and payments based on biometrics are going to be much safer, faster and easier than the existing methods based on credit and debit cards. Proposed forms of payments such as pay and touch scheme based on fingerprint or smart cards with stored iris information on them are examples of such applications. Although there are still some concerns about using biometrics in the mass consumer applications due to information protection issues, it is believed that the technology will find its way to be widely used in many different applications. Moreover, access control applications such as database access and computer login also benefit from the new offered technologies. Compared to passwords, biometric technologies offer more secure and comfortable accessibility and have dealt with problems such as forgetting or hacking passwords. Overall, the future of biometric technology is believed to be open for more investments based on the new services it has to offer to the society. Biometrics such as signatures, photographs, fingerprints, voiceprints, DNA and retinal blood vessel patterns all have significant drawbacks.

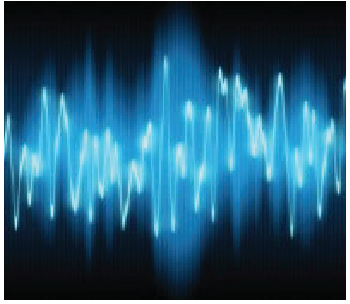
- **Face Recognition:** Changes with Age, Expression, Viewing angle, Illumination.
- **Finger Print Recognition:** Fingerprints or handprints require physical contact, and they also can be counterfeited and marred by artifacts.
- **Speech Recognition:** Electronically recorded voiceprints are susceptible to changes in a person's voice, and they can be counterfeited.
- **Signature Recognition:** Signatures and photographs are cheap and easy to obtain and store, they are impossible to identify automatically with assurance, and are easily forged

II. PROPOSED SYSTEMS

Voice/Speech Recognition

A **Voice Recognition** *voiceprint* is a spectrogram. A spectrogram is a graph that shows a sound's frequency on the vertical axis and time on the horizontal axis. Different speech creates different shapes on the graph. Spectrograms also use colour or shades of grey to represent the acoustical qualities of sound. All of our voices are uniquely different (including twins) and cannot be exactly duplicated. Speech is made up of two components. A *physiological* component (the **voice** tract) and a *behavioural* component (the accent).

Some companies use **voice recognition** so that people can gain access to information without being physically present, like in a phone call. Unfortunately people can bypass this system by using a pre recorded voice from an authorized person. That's why some systems will use several randomly chosen voice passwords or use general voiceprints instead prints of specific words. The voiceprint generated upon enrolment is characterized by the vocal tract and a cold does not affect the vocal tract. Only extreme vocal conditions such as laryngitis will prevent the system from proper **voice recognition**



During enrolment, the user is prompted to repeat a short phrase or a sequence of numbers. **Voice recognition** can utilize various audio capture devices (microphones, telephones and PC microphones). The performance of voice recognition systems may vary depending on the quality of the audio signal. Random words and phrases are used so that no unauthorized use is suspected.

The benefits of **voice recognition** are that it can use existing telephone systems, it can be automated and used with speech recognition and that it has a low perceived invasiveness. The weakness of the system is a high false non-matching rate. **Speech recognition** is the computing task of validating a user's claimed *identity* by using characteristics extracted from their **voice**. Speaker recognition uses the acoustic features of speech that are different in all of us. These acoustic patterns reflect both anatomy (size and shape of mouth & throat) and learned behavior patterns (voice pitch & speaking style), If a **speaker** claims to be of a certain *identity* and their **speech** is used to verify this claim. This is called **verification** or *authentication*. Identification is the task of determining an unknown speaker's identity.

Speech recognition can be divided into two methods. Text dependent and text independent methods. Text dependent relies on a person saying a pre determined phrase whereas text independent can be any text or phrase. The methods can easily be deceived by someone playing a pre recorded phrase of a person who is authorized. A *speech* **recognition** system has two phases. Enrolment and verification. During enrolment, the **speaker's voice** is recorded and typically a number of features are extracted to form a voice print, template or model. In the verification phase, a speech sample or utterance is compared against a previously created voiceprint. For identification systems, the utterance is compared against multiple voiceprints in order to determine the best match or matches, while verification systems compare an utterance against a single voiceprint. Because of this process, verification is faster than identification. **Voice / speech recognition** systems are mostly used for telephone based applications. Voice verification is used in government offices, healthcare, call centres, financial services and customer authentication for service calls.

Iris Scanners & Recognition

Iris cameras perform recognition detection of a person’s identity by mathematical analysis of the random patterns that are visible within the iris of an eye from some distance. It combines computer vision, pattern recognition, statistical inference and optics. Of all the biometric devices and scanners available today, it is generally conceded that iris recognition is the most accurate. The automated method of iris recognition is relatively young, existing in patent since only 1994.The iris is the colored ring around the pupil of every human being and like a snowflake, no two are alike. Each are unique in their own way, exhibiting a distinctive pattern that forms randomly in utero, n a process called **chaotic morphogenesis**. The iris is a muscle that regulates the size of the pupil, controlling the amount of light that enters the eye. Iris recognition is rarely impeded by glasses or contact lenses and can be scanned from 10cm to a few meters away. The iris remains stable over time as long as there are no injuries and a single enrolment scan can last a lifetime.

Some medical and surgical procedures can affect the overall shape and color of an iris but the fine texture remains stable over many decades. Even blind people can use this scan technology since **iris recognition** technology is iris *pattern*-dependent not sight dependent. Iris scanning is an ideal way of biometric identification since the iris is an internal organ that is largely protected by damage and wear by the cornea. This makes it more attractive then fingerprints which can be difficult to recognize after several years of certain types of manual labor. The iris is also mostly flat and controlled by 2 muscles so it helps make the **iris** movements more predictable then facial recognition. Even genetically identical twins have completely different iris patterns. **Iris cameras**, in general, take a digital photo of the iris pattern and recreating an *encrypted* digital template of that pattern. That encrypted template cannot be re-engineered or reproduced in any sort of visual image. Iris recognition therefore affords the highest level defense against identity theft, the most rapidly growing crime. The imaging process involves no lasers or bright lights and authentication is essentially non-contact. Today's commercial **iris** cameras use infrared light to illuminate the iris without causing harm or discomfort to the subject. Before *scanning* of the iris takes place, the iris is located using landmark features. These landmark features, and the distinct shape of the iris allow for imaging, feature isolation and extraction. Localization of the iris is an important step in iris recognition because, if done improperly, resultant noise (i.e.: eyelashes, reflections, pupils and eyelids) in the image may lead to poor performance. The general uses of *iris recognition* so far have been: substituting for passports (automated international border crossing); aviation security and controlling access to restricted areas at airports; database access and computer login; premises access control; hospital settings including mother-infant pairing in maternity wards; "watch list" screening at border crossings; and it is under consideration for *biometrically* enabled National Identity Cards. Having only become automated and available within the last decade, the **iris recognition** concept and industry are still relatively new. Through the determination and commitment of the **iris** industry and government evaluations, growth and progress will continue.

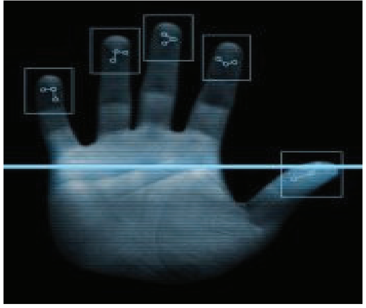
Biometrics Fingerprint Readers for ID and Access Control

Fingerprint readers take impressions of the friction ridges of the skin on the underside of the tip of the fingers. Fingerprints are used to identify you and are unique and different to everyone and do not change over time. Even identical twins who share their DNA do not have the same fingerprints. Police and Government agencies have used these modes of identifying humans for many years but other agencies are starting to use *biometric* **fingerprint** readers for *identification* in many different applications. **Fingerprints** are formed when the friction ridges of the skin come in contact with a surface that is receptive to a print by using an agent to form the print like perspiration, oil, ink, grease, etc. The agent is transferred to the surface and leaves an impression which forms the fingerprint. There are several methods of biometric ***fingerprinting***. A live scan devise basically reads or photographs fingerprints by measuring the physical difference between ridges and valleys. The procedure for capturing a fingerprint using a sensor consists of rolling or touching with the finger onto a sensing area, capturing the difference between valleys and ridges using a **reader**

In order to "*lift*" latent *prints* it is necessary to use a developer like a powder or chemical reagent to develop or produce a high degree of visual contrast between ridge patterns and the surface on which it was left. There are many different types of chemicals used in developing fingerprints and choosing one depends on the agent used to make the fingerprint. There are advances in the industry to form an SKP *fingerprinting* technique which is non-contact and does not require the use of developers, has the potential to allow fingerprints to be retrieved while still leaving intact any material that could subsequently be subjected to DNA analysis. Besides forensic agencies, many companies are turning to *fingerprint readers* to identify employees and potential security threats, as in airports and government agencies. Military personnel records will contain scans of fingerprints or toe prints to identify bodies in trauma scenes and possible situations where fire victims' fingerprints have been burned. The computer hardware industry has used **fingerprint** *readers / scanners* for years and the automotive industry is starting to catch on to the idea to identify their owners. Other arenas where fingerprinting is starting to make an impression are in schools in the UK and are making their way to the US are used for electronic registration, cashless catering and library access. Whatever the application, **fingerprints** are the most commonly used forensic evidence worldwide. With many advances in the industry year after year, we will be seeing more **fingerprint readers** for *identification* in our daily lives as time moves on.

Biometrics Hand/Palm Scanners and Finger Readers

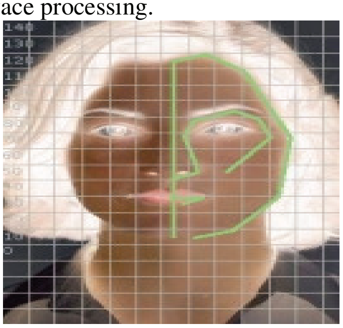
A person's **hand/palm and finger** are unique however not as unique as their fingerprints or irises, for this reason, businesses and schools like to use **hand scanner** and **finger reader** biometrics technology, to authenticate but not identify its users. *Authentication* is a one-to-one comparison; it compares your characteristic with your stored information. *Identification*, on the other hand, is a one-to-many comparison. In this way, some people may find it less intrusive. **Hand scanner and finger** reader *recognition systems* measure and analyze the overall structure, shape and proportions of the hand, e.g. length, width and thickness of hand, fingers and joints; characteristics of the skin surface such as creases and ridges. The **hand** and **finger** *scanner/reader devices* still maintain accuracy even when hands are dirty, which are good in construction areas; and also have the ability to work under extreme temperatures ranging from negative 30 to 150 degrees F. To use a **hand scanner**, you simply place your hand on a flat surface, aligning your **fingers** against several pegs to ensure an accurate reading. Then, a camera takes one or more pictures of your hand and the shadow it casts.



The scanner uses this information to determine the length, width, thickness and curvature of your hand or finger, knuckle shape, distance between joints and bone structure and translucency. It translates that information into a numerical template. **Hand** *scanners* and **Finger** *readers* are great in controlling access instead of key or card passes. Hand and fingers cannot be forgotten or lost for someone to steal and gain access to your facility. The benefits of hand and finger recognition are many. It is easy to use and non-intrusive; a small amount of data is required to identify the users so more templates can be easily stored in one stand alone devise; low failure to enroll rates. **Hand and finger scanner** *recognition* systems are best used for *verification* due to less accurate detection compared to fingerprint detection and can be more expensive than these devices. Some drawbacks, Minor injuries to hands may occur, and weight fluctuations can prevent the device from working properly. Sometimes systems need to be updated regularly to accommodate these changes. **Hand** and **finger readers** are generally optical, although they may incorporate other reader technologies such as capacitive sensors also used in a "liveness" test. Other technologies include ultrasound, and thermal imaging. In this respect hand and finger readers are similar to fingerprint readers. Some **palm** and **finger scanners** have the capability of capturing 10-print fingerprints, as well as palm prints. Low resolution hand and finger readers (generally less than 100 dpi) can effectively only record principal lines and wrinkles. High resolution hand and finger readers (generally greater than 400 dpi) are able to record point features and minutiae. Some hand and finger recognition systems scan the entire hand and fingers, while others allow the hand and finger images to be segmented in order to improve performance and reliability. In general terms, reliability and accuracy is improved by searching smaller data sets. **Hand and finger biometrics** systems are the most widely used scanning devices and are used for time & attendance, and access to restricted areas and buildings. They exist in apartment buildings, offices, airports, day care centres, hospitals and immigration facilities. To find a supplier for **Hand scanner** and **Finger reader** Biometrics, please follow the links below.

Facial Recognition

A **facial recognition** *device* is one that views an image or video of a person and compares it to one that is in the database. It does this by comparing structure, shape and proportions of the face; distance between the eyes, nose, mouth and jaw; upper outlines of the eye sockets; the sides of the mouth; location of the nose and eyes; and the area surrounding the check bones. Upon enrolment in a **facial recognition** program, several pictures are taken of the subject at different angles and with different facial expressions. At time of verification and identification the subject stands in front of the camera for a few seconds, and then the image is compared to those that have been previously recorded. To prevent a subject from using a picture or mask when being scanned in a **facial recognition** program, some security measures have been put into place. When the user is being scanned, they may be asked to *blink, smile or nod their head.* Another security feature would be the use of facial *thermography* to record the heat in the face. The main **facial recognition** methods are: feature analysis, neural network, eigenfaces, automatic face processing.



Some facial recognition software algorithms identify faces by extracting features from an image of a subject's face. Other *algorithms* normalize a gallery of face images and then compress the face data, only saving the data in the image that can be used for facial recognition. A probe image is then compared with the face data.A fairly new method on the market is three-dimensional **facial recognition**. This method uses 3-D sensors to capture information about the shape of a face. This information is then used to identify distinctive features on the face, such as the contour of eye sockets, nose and chin.The advantages of 3-D facial recognition are that it is not affected by changes in lighting, and it can identify a face from a variety of angles, including profile view.Another new technique in **facial recognition** uses the visual details of the skin, as captured in standard digital or scanned images. This technique is called skin texture analysis, turns the unique lines, patterns, and spots apparent in a person's skin into a mathematical space. Preliminary tests have shown that using skin texture analysis in facial recognition can increase performance in identification by 20 to 25 percent.The benefits of facial recognition are that it is not intrusive, can be done from a distance even without the user being aware they are being scanned. (i.e.: bank or government office)What sets apart **facial recognition** from other biometric techniques is that it can be used for surveillance purposes; as in searching for wanted criminals, suspected terrorists, and missing children. Facial recognition can be done from far away so with no contact with the subject so they are unaware they are being scanned.**Facial recognition** is most beneficial to use for facial authentication than for identification purposes, as it is too easy for someone to alter their face, features with a disguise or mask, etc. Environment is also a consideration as well as subject motion and focus on the camera.Facial recognition, when used in combination with another biometric method, can improve verification and identification results dramatically.To find a **facial recognition** device, please click on one of our supplier links.

Biometrics Smart Cards

A **smart card** is a pocket sized plastic card with an embedded chip that can process data, used in industries such as health care, banking, government and **biometrics**. Smart cards can process data via input and output of information. A smart card is essentially a mini processor. **Smart cards** provide identification, authentication, data storage, access to buildings, bank machines, communications & entertainment. The first smart card technology was used in 1983 in pay phones in France. The international payment brands Visa, MasterCard & Euro pay agreed in 1993 to work together to create the specifications to produce smart cards on their payment cards as in debit and credit cards. The technology for **smart cards** is ever increasing and is being used in personal identification and authentication, as in **biometrics**. Current and future uses of smart cards will be seen in *citizen cards*, *driver's licenses*, *patient cards* & *passports*.

Contact smart cards have a contact area containing a small gold plated contact pad. When inserted into a reader, the contact pad or chip makes contact with electrical connectors that can read data from the chip and write information back. The cards do not contain batteries; the power is supplied by the reader.**Smart card** *readers* are used as communication device or medium between the host and the smart card as in a computer, point of sale terminal or mobile phone. Since the *chips in smart cards are the same as in mobile phones*, the SIM cards in mobile phones are programmed differently and embedded in different shaped PVC.Contactless **smart cards** use the chip to communicate with the card reader through RFID (*radio frequency identification*) induction technology. These cards require only close proximity to an *antenna* to complete the transaction. These are used when a transaction needs to be completed quickly or hands free such as a mass transit system.**Smart card** chips are capable of many kinds of transactions. Besides making purchases from your credit account, debit account or from a stored account value that's reloadable. The enhanced memory and processing capabilities can far exceed the technology of a magnetic stripe card and can perform many tasks at once.**Smart cards** are mostly used in financial applications as in credit cards, debit cards, fuel cards, SIM cards in cell phones, authorization cards for pay television, households pre pay utilities, high security identification, access control cards, public transportation and public phone payment cards.Smart cards can also be used as *electronic wallets*. The smart card can be loaded with funds that can be used at various public locations as in parking lots, vending machines or retail outlets. The cryptographic algorithms protect the exchange of money from the card and the merchant. There is no contact with the bank and no exchange of banking info to the accepting machine.Health cards and other **biometrics** applications that have been outfitted with a **smart card** chip can protect a patient's medical history, provide a secure avenue for their medical records and provide secure access to emergency medical information as well as reducing health care fraud.Techniques are being developed to provide greater security measures to prevent the tampering of **smart cards** (which are much safer than traditional swipe cards), and are emerging as the favourite choice of the banking, health care and **biometrics** industry for storing secured data.If you are looking for a **biometrics smart cards** application for your business or institution, please contact one of the solution providers below.

Digital Signature / Keystroke Biometrics

A *digital* **biometrics signature** is equivalent to a traditional *handwritten* signature in many respects since if the signature is properly implemented is more difficult to forge then the traditional type.Digital signature schemes are *cryptographically* based and must be implemented properly to be effective. Digital signatures can be used for electronic mail, contracts, or any message sent via some other *cryptographic protocol*.Although messages include information about the person sending the message, that information may or may not be accurate. A *digital* **signature** may be used to authenticate the source of the message.Each **signature** has a secret key. That secret key is used to validate the signature was indeed sent by the user that it implies has sent it. Many applications can appreciate the importance of high confidence in sender authenticity from government applications to financial institutions

In certain instances the sender and receiver of a message with a *digital* signature need to be confident that the message and signature has not been altered in any way during transmission.The use of *encryption* can be used to hide the contents of a message without changing the signature. It is possible though to change an encrypted message without understanding it.However, if a message has been digitally signed, any changes to the message after signature will invalidate the signature. Also, there is no efficient way to modify a message and its signature to produce a new message with a valid signature because it is considered to be computationally infeasible.A secret/private key can be stored on a user's computer and protected by a password but this has some disadvantages. The user can only use that particular computer to use the signature secret key and the security of the secret key must depend on the security of that computer. A more secure solution is to store the secret key for the digital signature onto a smart card. Many smart cards have been designed to be tamper resistant.In a typical *digital* signature implementation, the hash calculated from the document is sent to the smart card, whose CPU encrypts the hash using the stored private key of the user, and then returns the encrypted hash.The user must activate the smart card by entering a PIN code. It can be implemented that the secret key never leaves the smart card. If for some reason the smart card is stolen, the thief must also have the PIN code in order to generate a digital signature.This system of using the smart cards makes the *digital* signature very difficult to copy and the loss of such a card can be detected by the owner and those cards' privileges can be revoked.Secret/private keys stored and protected by computer alone are much easier to copy and these compromises are much more difficult to detect and can go on for some time before security devices have been alerted.Another process to computer security uses keystroke dynamics. It is possible to enhance a computer's security by using a special algorithm which when used in addition to the security password, checks if the keyboards' keys have been pressed in the user's pre-recorded and unique way of typing that particular password. *Authenticating* this way of typing can be very difficult.It is easy for someone to copy the user's keystroke patterns and the algorithm may *authenticate* a similar pattern to keystrokes that are slightly different. The use of keystroke biometrics with other processes makes it more difficult to copy.Biometric keystroke *authenticating* does not require any expensive hardware. It is virtually just an algorithm that can be implemented and run on any computer. When this algorithm is used in combination with a password and/or a smart card, the authentication scheme greatly enhances security.

Vein Recognition Biometrics

Biometrics, such as with **vein recognition**, refers to methods for recognizing individual people based on unique physical and behavioral traits. hysiological biometrics is one class of biometrics that deals with physical characteristics and attributes that are unique to individuals. **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.Of the many new biometric technologies such as DNA, Iris recognition, ear and body odor recognition, **vein recognition**, with its own unique characteristics and advantages is now emerging as one of the fastest growing technologies. Vein recognition is the newest type of biometric technology and is quickly moving from labs to widespread commercial development

One reason that **vein recognition** has such great potential for explosive growth, and may one day be the leading biometric technology in the world is its potential to be applied in several unique forms. There is a wide selection of great companies that have all developed different kinds of **vein recognition** biometric technologies.There are a variety of methods for **vein recognition biometric technology.** Some companies have developed devices that scan the vein structure pattern in the index finger, or more than one finger at a time. Others have developed vein recognition devices designed for reading the vein patterns located under the palm and at the back of the hand. The variety of devices available gives a wide selection of choices for consumers to meet different needs and demands.Another reason for the fast emergence of **vein recognition** biometrics is very, very low False Rejection and False Acceptance Rates. Vein patterns are unique to each individual and they do not change over time except in size so it is hardly possible to fool the technology. **Vein recognition** technology has a False Rejection Rate of 0.01% and a False Acceptance Rate of 0.0001% and so it is arguably the most suitable for high-security deployment.The potential for **vein recognition** biometric technologies is very promising for many reasons. Vein recognition biometric devices are often small, portable and affordable because they often use a single-chip design. It often takes less than two seconds for a vein recognition biometric device to authenticate the user, and contact is not necessary.

Other promising facts about **vein recognition** biometric technologies include their capability to fuse with existing biometric technologies. Vein recognition can be used along with fingerprint and hand geometric technology, provide one-to-many matching and also enhance security and decrease vulnerability for fraud.Today **vein recognition** biometric technology is most commonly found in the Asia Pacific region. Due to some controversy surrounding fingerprint biometrics, **vein recognition** has found widespread acceptance in the Asian Pacific.Adoption of **vein recognition** technologies has been highest among financial institutions and it is used commonly for ATM identity verification and PC login authentication where high security is a necessity.

Multimodal Biometrics

Multimodal Biometrics are systems that are capable of using more than one physiological or behavioral characteristic for enrollment, verification or *identification*. For biometric identification to be ultra-secure and provide above average accuracy, more than one type must be used as only one form of it may not be accurate enough. One example of this inaccuracy is in the area of fingerprints where at least 10% of people have worn, cut or unrecognizable prints.

Some forms of behavioral *biometric identification* include the following:

- Keystroke or Typing Recognition and Speaker identification or Recognition

Some forms of *physical* biometric identification include the following:

- Fingerprint,Iris,Retina,Finger Geometry,Signature/Handwriting,Voice,Facial Proportions and Hand Geometry

Multimodal biometrics will use a combination of the above *recognition* technologies, up to three of them, to compare the *identity* of a person therefore providing the best security available to you. If one of the technologies fails for any reason, your system can still use another one or two of them to provide accurate identification of a person.The benefits of multimodal biometrics is that by using more than one means of *identification*, your system can retain a high threshold *recognition* setting and your system administrator can decide the level of security that is needed. For a very high security site, you may need to use up to three biometric identifiers and for a lower security site, you may only need one or two of them. This greatly reduces the probability of admitting an imposter.There is a great need for **multimodal biometrics** as most biometric systems used in real applications are unimodal, which means they rely on only one area of identification. Some examples of these are fingerprints, faces and voices and these systems are quite vulnerable to many problems such as noisy data, non-universality and spoofing. This leads to a high false acceptance rate and false rejection rate, limited discrimination capability, and lack of permanence.

You can overcome the limitations of uni modal biometric systems by using multimodal biometrics where you use *two or more sources* to validate identity. Multimodal systems are more reliable because you are using many independent biometrics that meet very high performance requirements and they counteract the problems listed above. They also effectively deter spoofing because it is near impossible to spoof *multiple biometric traits* and the system can request the user to present random traits that only a live person can do.

Multimodal biometrics are driven by various factors such as: risk and viability of spoofing, *universal enrollment* requirements, *accuracy/integrity requirements*, suitability for the environment and transaction time flexibility.

Some of the **multimodal biometrics** target applications are shown below with the potential needed:

Strong Potential: Physical access Civil ID *Criminal ID*
Moderate Potential: *Network/PC access* Kiosk/ATM
Modest Potential: Retail/POS *Surveillance* eCommerce telephony

REFERENCES

[1] J. Daugman. High confidence visual recognition of persons by a test of statistica independence. IEEE Trans.PAMI,15(11):1148–1161, November1993.

[2] J. Daugman. The importance of being random: Statistical principles of iris recognition. Pattern Recognition,36(2):279–291, 2003.

[3] J. Daugman. Anatomy and physiology of the iris. [htlm-doc.], [retrieved 15.10.2003].

[4] R.Wildes. Iris recognition: An emerging biometric technology.Proceedings of the IEEE, 85(9):1348–1363, September 1997.

[5] W. Boles and B. Boashash. A human identification technique using images of the iris and wavelet transform. IEEE Trans. Signal Processing, 46(4):1185 1188, April 1998.

[6] S. Lim, K. Lee, O. Byeon, and T. Kim. Efficient iris recognition through improvement of feature vector and classifier. ETRI Journal, 23(2):61–70,2001.

[7] S. Noh, K. Pae, C. Lee, and J. Kim. Multiresolution independent component analysis for iris identification. In Proceedings of ITC-CSCC'02, pages 1674-1678, 2002.

[8] C. Tisse, L.Martin, L. Torres, and M. Robert. Person identification technique using human iris recognition. In Proceedings of ICVI'02, pages 294–299, 2002.

[9] L. Ma, T. Tan, Y. Wang, D. Zhang. Personal Recognition Based on Iris Texture Analysis. IEEE Trans.PAMI, 25(12):1519–1533, 2003.

[10] W. Kong and D. Zhang. Accurate iris segmentation based on novel reflection and eyelash detection model. In Proceedings of ISIMVSP, pages 263–266, 2001.

[11] P. Kovesi. Image features from phase congruency. Videre: Journal of Computer Vision Research, 1(3):1–26, 1999.

[12] P. Kovesi. Phase congruency detects corners and edges. In Proceedings DICTA'03, pages 309–318, 2003.

[13] E.Wolff. Anatomy of the Eye and Orbit. 7th edition. H. K. Lewis & Co. LTD, 1976.

[14] A. Oppenheim, J. Lim. The importance of phase in signals. Proceedings of the IEEE 69, 529-541, 1981.

[15] Chinese Academy of Sciences – Institute of Automation. Database of 756 Greyscale Eye Images

[16] C. Barry, N. Ritter. Database of 120 Greyscale Eye Images. Lions Eye Institute, Perth Western Australia

[17] J. Canny, A computational approach to edge detection, IEEE Trans.Pattern Anal. Mach. Intell. 8 (6) (1986) 679–698.

[18] Junzhou Huang, Li Ma, Yunhong Wang, Tieniu Tan, "Iris Model Based on Local Orientation Description", Proc.of Asian Conference on Computer Vision, 2004, pp.954-959.

[19] Ya-Ping Huang, Si-Wei Luo, En-Yi Chen, "An Efficient Iris Recognition System", Proceedings of the First International Conference on Machine Learning and Cybernatics, Nov.2002

[20] A, Oppenheim, J.Lim, "The importance of Phase in Signal", Proceedings of the IEEE 69, 1981, pp.529-541.

[21] Hugo Proenca,Luis A Alexandre ”iris recognition:Analysis of error rates regarding the accracy of the segmentation stage” Image and Vision computing 28 2009

[22] UK Passport Service page http://www.passport.gov.uk/index.asp.

[23] US Department of Homeland Security page http://www.dhs.gov/dhspublic/.

[24] Morrone, M.C., Ross, J.R., Burr, D.C., Owens, R.A.: Mach bands are phase dependent. Nature 324 (1986) 250{253

[25] Li Ma, T. Tan, “Efficient Iris Recognition by Characterizing Key Local Variations”, IEEE Trans. on Image Processing, Vol.13, no.6, 2004.