ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 2, pp: (381-389), Month: April-June 2014, Available at: www.researchpublish.com

Application of Biometrics in Commercial Security

V.S. Swarna Lakshmi[1]

[1]Student, Department of Computer Science Engineering, Saveetha School of Engineering

Saveetha University, Chennai– 602 105, India

Abstract: **Biometrics is the science and technology of measuring and analyzing of biological data. It has been used to uniquely identify individuals by their physical characteristics or personal behavior traits. It is used to allow employees access to concerned areas and for general ID purposes. A biometrics system goes through three basic steps: 1. acquiring of data, 2. Encrypting data 3. Analysis of data. Biometrics is being used in ATMs, computers, security installations, mobile phones, credit cards, health and social services. The future in biometrics seems to belong to the multimodal biometrics (a biometric system using more than one biometric feature) as a unimodal biometric system (biometric system using single biometric feature) has to contend with a number of problems. In this paper, of some of the biometrics will be presented that are currently in use across a different range of environments or those which are still in limited use or under development, or still in the research .This paper will give us a clear view of biometrics.**

Keywords: **Biometrics, Biological data analysis.**

1. INTRODUCTION

The purpose of biometrics is to uniquely identify or verify an individual through the Characteristics of the human body Biometrics uses characteristics that can be physical such hand shape, a fingerprint, facial characteristics, voice, or DNA. Biometrics can also use Characteristics that are learned or acquired, behavioral traits such our signature, they way we Speak or use a computer. Biometric technology must first gather Information into a computer database, for Example, a database of fingerprints. The Computer will compare the fingerprints in the Database to any new sample and recognize when there is a match. The matches can be Used for both identification and verification Purposes.

1.1 HISTORY

The earliest cataloging of fingerprints dates back to 1891 when Juan Vucetich started a collection of fingerprints of criminals in Argentina.

2. METHODOLOGY

2.1 FACIAL RECOGNITION

Generalized Matching Face Detection Method (GMFD) .NEC's face recognition technology utilizes the GMFD method that provides high speed and high accuracy for facial detection and facial features extraction. The main logic for facial recognition within GMFD is a modified Generalized Learning Vector Quantization (GLVQ) algorithm, which searches and selects face area candidates after the generation of potential eye pairs. GLVQ is based on a neural network and is not easily fooled by attempts to conceal identity via the usage of caps, hats, sunglasses, etc. Perturbation Space Method (PSM)NEC has developed the PSM algorithm that converts two-dimensional images (e.g., photographs) into three-dimensions (such a process is called "Morphing"). The three-dimensional representations of the head are then rotated in both the left-to-right and up-and-down directions. Further processing applies differing illumination across the face, which greatly enhanced the chances of a query "faceprint" for matching against its true mate from the database. Adaptive Regional Blend Matching (ARBM) Method.

Thanks to the PSM algorithm, the general range of facial poses and illumination has ceased to present major problems. However, the range of variation of different facial parts is still a challenge. To reduce the impact of adverse local changes (e.g., varying facial expression caused by smiling and blinking eyes, and intentional changes caused by the wearing of caps, hats and glasses), NEC's face recognition technology utilizes the ABRM algorithm, which reduces the impact of such local changes during the matching process. The minimization of the local changes guarantees the overall face recognition accuracy.

2.2 FINGER PRINT

A fingerprint scanner system has two Basic jobs -- it needs to get an image of your finger, and it needs to determine whether the pattern of ridges and valleys in this image matches the pattern of ridges and valleys in pre-scanned images.

Only specific characteristics, which are unique to every fingerprint, are filtered and saved as an encrypted biometric key or mathematical representation. No image of a fingerprint is ever saved, only a series of numbers (a binary code), which is used for verification. The algorithm cannot be reconverted to an image, so no one can duplicate your fingerprints. It is important to note that Easy Clocking's biometric time clocks do not actually collect and store fingerprints. Instead, it saves a mathematical representation of the employee's biometric data. When the biometric time clock scans a hand or finger during a supervised enrollment process, only an encrypted mathematical representation of the fingerprint is stored. As a result, it's virtually impossible to duplicate the original image from that mathematical representation. Additionally, if employees question cleanliness, this concern should not be dismissed. Instead, you should assure employees that the time clock's finger zone is not a hot zone for germs. In fact, it will be touched far less frequently than restroom door handles, water cooler spigots, or chairs in the break room. The advantage of finger print biometrics is Fingerprints are much harder to fake than identity cards. You can't guess a fingerprint pattern like you can guess a password. You can't misplace your fingerprint, like you can misplace an access card. You can't forget your fingerprints like you can forget a password.

Fig.1 Typical finger print

2.3 VOICE RECOGNITION:

Voice recognition is the process of taking the spoken word as an input to a computer program. This process is important to virtual reality because it provides a fairly natural and intuitive way of controlling the simulation while allowing the user's hands to remain free. This article will delve into the uses of voice recognition in the field of virtual reality, examine how voice recognition is accomplished, and list the academic disciplines that are central to the understanding and advancement of voice recognition technology.

Auditory Biometric: Identification is the task of determining an unknown speaker's identity. Speaker identification is a 1:N (many) match where the voice is compared against N templates. Speaker identification systems can also be implemented covertly without the user's knowledge to identify talkers in a discussion, alert automated systems of speaker changes, check if a user is already enrolled in a system, etc.

For example, a police officer compares a sketch of an assailant against a database of previously documented criminals to find the closest match (es).

In forensic applications, it is common to first perform a speaker identification process to create a list of "best matches" and then perform a series of verification processes to determine a conclusive match. Note: There is a difference between speaker recognition (recognising who is speaking) and speech recognition (recognising what is being said). These two terms are frequently confused, as is voice recognition. Voice recognition is a synonym for speaker, and thus not speech, recognition. In addition, there is a difference between the act of authentication (commonly referred to as speaker verification or speaker authentication) and identification.

2.4 IRIS RECOGNITION:

The iris is the most unique feature visible on the human body. No two irises are the same - even identical twins have different iris patterns. The abundance of detail in the iris, its variability and lack of genetic dependence, and its accessibility for imaging without physical contact all make the iris an excellent personal identifier. Each of the three main biometrics has applications where it excels. However, for patient identification, iris has the edge. Iris recognition is more accurate than either fingerprints or facial, which is important where the standard is a zero error rate. Fingerprint identification uses a contact sensor, a non-sterile pad that all persons must touch to be identified. In a clinical environment, it's likely that some users will have transmissible diseases, so non-contact technologies are a better choice. Our comparison chart on selected technology features highlights advantages of the iris technology in this application. Iris recognition technology uses a digital camera in combination with software that performs the following functions:

a) Acquires an image of the eye, which includes the iris

b) Defines the boundaries of the iris

c) Analyzes image data

d) Generates pattern data

e) Stores the pattern data

f) When recognition is desired, another image is taken, and pattern data from that image is matched to the stored data.

Retinal scanning:

Retinal scanning is an older biometric technology that maps the blood vessels in the retina (optic nerve head) in the back of your eye using lights aimed into the eye. The iris, in contrast, is on the outside and visible without any invasive lighting. Iris identification systems merely take a digital picture of the outside of your eye and do not provide any other health information; retinal scanning is more like getting an eye exam and can be used to diagnose various medical conditions.

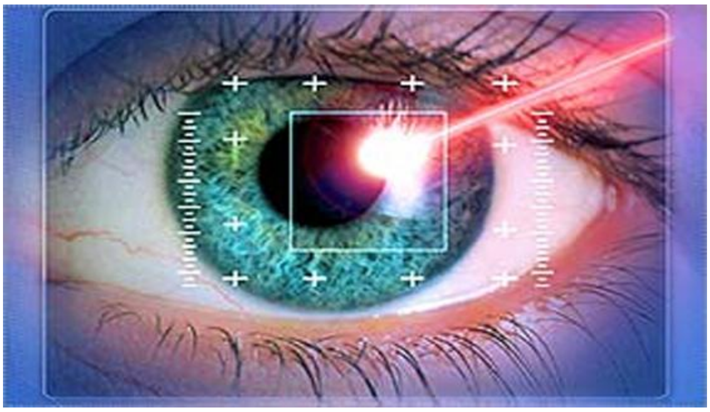

Fig. 2 Iris recognition

2.5 GAIT:

Gait recognition is an emerging biometric technology which involves people being identified purely through the analysis of the way they walk. While research is still underway, it has attracted interest as a method of identification because it is non-invasive and does not require the subject's cooperation. Gait recognition could also be used from a distance, making it well-suited to identifying perpetrators at a crime scene. But gait recognition technology is not limited to security applications – researchers also envision medical applications for the technology. For example, recognizing changes in walking patterns early on can help to identify conditions such as Parkinson's disease and multiple sclerosis in their earliest stages.

Gait recognition technology is, however, still in its developing stages. No model has, as of yet, been developed that is sufficiently accurate and marketable. The technology is moving ahead at a rapid pace, however, with government-sponsored projects supporting research such as that going on at the Georgia Institute of Technology, MIT, the Lappeenranta University of Technology, and others academic institutions.

There are two main types of gait recognition techniques currently in development. The first, gait recognition based on the automatic analysis of video imagery, is the more widely studied and attempted of the two. Video samples of the subject's walk are taken and the trajectories of the joints and angles over time are analyzed. A mathematical model of the motion is created, and is subsequently compared against any other samples in order to determine their identity.

The second method uses a radar system much like that used by police officers to identify speeding cars. The radar records the *gait cycle* that the various body parts of the subject create as he or she walks. This data is then compared to other samples to identify them.

Efforts are being made to make gait recognition as accurate and usable as possible, and while it may never be as reliable as other biometrics such as fingerprint or iris recognition, it is predicted that gait recognition technology will be released in a functional state within the next five years, and will be used in conjunction with other biometrics as a method of identification and authentication.

2.6 ODOR DETECTION:

Odor detection and identification by machines is currently being done to evaluate perfumes, wine, olive, oil, and even find people buried in rubble. Extending body odor detection to authentication may seem far-fetched and unrealistic. Yet such an application is plausible, given that like a fingerprint or iris, the human body odor is unique. Although such technology still has strides to make before being applicable as either a stand-alone or supplemental technology to existing biometric tools, it still warrants research, especially in how the technology is perceived. Numerous studies have addressed the public perception of biometric technologies, although odor scanning is one that has been under-addressed. This exploratory study addresses perceptions and attitudes of odor scanning and recommends directions for future research and practice. This study has found that odor scanning is little understood, and its benefit to security and privacy are perceived as low. Should body odor scanning develop into a viable method of biometric authentication, issues of perception and acceptance will need further attention by both research and practice.

2.7 EAR RECOGNITION:

Ear biometrics is a relatively unexplored biometric field, but has received a growing amount of attention over the past few years. There are three modes of ear biometrics: ear photographs, ear prints obtained by pressing the ear against a flat plane, and thermograph pictures of the ear. The most common implementation of ear biometrics is via photographs for automated identification applications, the most common implementation of ear biometrics is via photographs for automated identification applications. In practice, and we discuss some worked done on ear recognition. One of the first Ear recognition systems is the Iannarelli‘s system which was originally developed in 1949. This is a manual system based upon 12 measurements. Each photograph of the ear is aligned such that the lower tip of a standardized vertical guide on the development easel touches the upper flesh line of the cocha area, while the upper tip touches the outline of the ant tragus. Then the crus of helix is detected and used as a centre point. Vertical, horizontal, diagonal, and anti-diagonal lines are drawn from that centre point to intersect the internal and external curves on the surface of the pinna. The 12 measurements are derived from these intersections and used to represent the ear[15]. Mark Burge and Wilhelm Burger reported the first attempt to automate the ear recognition process in 1997, they used a mathematical graph model to represent and match the curves and edges in a 2D ear image. Some years later, Belén Moreno, Ángel Sanchez, and José Vélez described a fully automated ear recognition system based on various features such as ear shape and wrinkles. Since then, researchers have proposed numerous feature extraction and matching schemes, based on computer vision and image processing algorithms, for ear recognition [2]. Chen and Bhanu developed another shape model-based technique for locating human ears in side face range images where presented a 3D ear recognition system that exploited the depth and structure of the ear‘s morphological components They started by locating the edge segments and grouping them into different clusters that are potential ear candidates. For each cluster, they register the ear shape model with the edges[16].The use of 2D or 3D ear images for human recognition differs from the use of ear prints: marks left by secretions from the outer ear when someone presses up against a wall, or some platform . Ear prints have been introduced as physical evidence in several criminal cases in the many countries, although some convictions that relied on ear prints have been overturned. Ear prints haven‘t been widely accepted in court due to a lack of scientific consensus as to their individuality. In addition, the use of ear thermo grams could help mitigate the problem of occlusion due to hair and accessories. As the technology matures, both forensic and biometric domain.

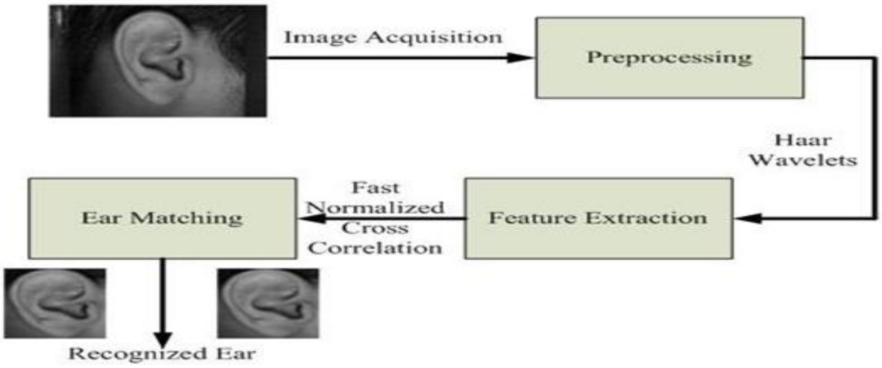

Fig. 3 Ear recognition

2.8 VEIN RECOGNITION:

Blood veins are formed during the first eight weeks of gestation in a chaotic manner, influenced by environment in a mother’s womb. This is why vein pattern is unique to each individual, even to twins. Veins grow with a person’s skeleton, and while capillary structures continue to grow and change, vascular patterns are set at birth and do not change over the course of one’s life time. To scan the veins, an individual’s hand is placed on the hand guide (the plastic casing of the scanner device) and the vein pattern is captured by lighting the hand with near-infrared light. Veins contain deoxidized hemoglobin, an iron-containing pigment in the blood that carried oxygen through the body. These pigments absorb the near-infrared light and reduce the reflection rate causing the veins to appear as a black pattern. An individual’s scanned palm vein data (biometric template) is encrypted for a protection and registered along with the other details in his/her profile as a reference for future comparison.

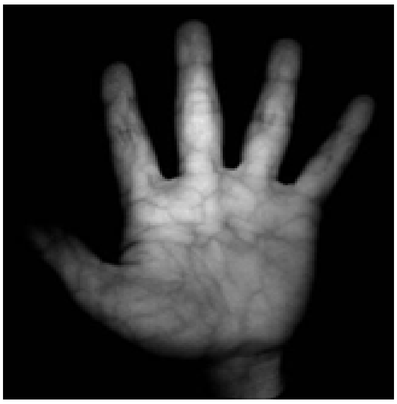

Fig. 4 VEIN RECOGNITION

3. WORKING

Patient *Security* has been adopted primarily with palm vein recognition technology, which provides highly accurate patient identification that works by scanning the vein pattern of a patient's palm. The technology works by capturing vein pattern in a patient's palm with a near-infrared light wave scanner. This scan produces a unique biometric template that is a digital representation of the vein pattern

3.1 SIGNATURE RECOGNITION:

Biometric technology can be generally classified as either physiological recognition or behavioral recognition. Previous articles (fingerprint, iris, retinal, voice, facial, and hand geometry recognition) have reviewed physiological recognition, in that some sort of biological feature has been examined in order to verify or identify an individual. Behavioral recognition examines the mannerisms of an individual. This includes Signature Recognition and Keyboard Typing Recognition, in that the way an individual signs his signature or types on the keyboard can be used for verification purposes.

However, a distinction must be made at this point. We are all familiar with signing our signature on an electronic Point of Sale system. This electronically captured signature is then compared to the signature on our driver's license (or another type of ID) in order to verify whom we are. This is not Signature Recognition in the truest form. This example can be classified as a "simple signature comparison." Signature Recognition in its truest form can be further defined as "dynamic signature recognition." In this case, it is not the way a signature looks that is important, but it is the *behavioral patterns* in which the signature is signed that becomes important. These behavioral characteristics include the changes in the timing, pressure, and speed during the course of signing. While it may be very easy to duplicate the visual appearance of the signature, it is very difficult to duplicate the behavioral characteristics when you sign your signature. Signature Recognition technology consists primarily of a pen and a specialized writing tablet, which are then connected to a local or central computer for template processing and verification. In order to start the data acquisition phase of the enrollment process, the individual must sign their name multiple times on the writing tablet. The robustness of the Signature Recognition enrollment template is a direct function of the quality of the writing tablet that is utilized A high quality writing tablet will be able to capture all of the behavioral variables (timing, pressure, and speed) of the signature, whereas a lower end writing tablet may not be able to capture all of the variables. However, there are a number of constraints in the data acquisition phase. First, a signature cannot be too long or too short. If a signature is too long, there will be too much behavioral data presented, and as a result, it will be difficult for the Signature Recognition system to identify consistent and unique data points. If a signature is too short, there will not be enough data present, and as a result, this will lead to a higher False Accept Rate (for example, an impostor being authorized by the Signature Recognition system). Second, the individual must complete the enrollment and verification processes in the same type of environment and conditions. For example, if the individual was standing in the enrollment phase, but sitting in the verification phase, and resting their arm in one phase and not in the other phase while signing, can cause the enrollment and verification templates to be substantially different from each other. This constraint of a consistent environment is also faced by another biometric technology-Facial Recognition. .After the data acquisition phase, the Signature Recognition system then extracts the unique features from the behavioral characteristics, which includes the time utilized by the individual to sign their name; the pressure applied from the pen to the writing tablet; the rate of speed in signing the signature; the overall size of the signature; and the quantity and the various directions of the strokes in the signature.Since Signature Recognition is classified as a "behavioral recognition" biometric, there are no actual images of the signature used in the template creation phase. With the other biometric technologies examined in previous articles, an actual image is used to create the enrollment and verification templates. With Signature Recognition templates, different values or "weights" are assigned to the unique features described. These templates can be as large as 3 Kilobyte .

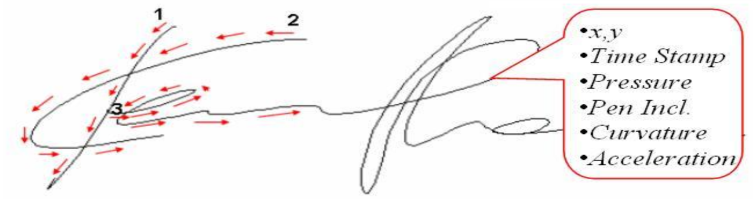

Fig. 5 Signature recognition

3.2 DNA RECOGNITION:

Deoxyribonucleic acid (DNA) is the genetic material found in most organisms, including humans. Each individual human is identifiable by hereditary traits found in their DNA, which is located in the nucleus of the cells as well as the mitochondria. DNA serves as a genetic code that is unique to every organism, no two being exactly alike; only identical twins are an exact DNA match. An organism's DNA code is comprised of four bases: adenine (A), guanine (G), cytosine (C), and thymine (T). These bases combine in a specific sequence to form base pairs that determine the anatomy and physiology of the organism. Each base pair is attached to a sugar and phosphate molecule creating a nucleotide. Nucleotides compose two long strands connected by the base pairs in a ladder-like formation that form the common spiral known as the double helix. n the case of human beings, there are about 3 million bases, 99% of which are the same from person to person. The variations found in the final 1% are the means by which DNA becomes unique to each individual. The final 1% also serves as the foundation for DNA biometrics, being the location of the unique traits by which DNA recognition can identify or verify the identification of an individual person.

3.3 HOW DNA RECOGNITION WORKS:

The cells that contain DNA share genetic material (information) through chromosomes. Humans have 23 chromosomes that house a person's DNA and their genes. Of the 46 total chromosomes, 23 come from each parent of an offspring. 99.7% of an offspring's DNA is shared with their parents. The remaining .3% of an individuals DNA is variable repetitive coding unique to an individual. This repetitive coding is the basis of DNA biometrics. DNA recognition uses genetic profiling, also called genetic fingerprinting, to isolate and identify these repetitive DNA regions that are unique to each individual to either identify or verify a person's identity.

The basic steps of DNA profiling include:

1. Isolate the DNA (sample can originate from blood, saliva, hair, semen, or tissue)
2. Section the DNA sample into shorter segments containing known variable number tandem repeats (VNTRs), identical repeat sequences of DNA
3. Organize the DNA segments by size
4. Compare the DNA segments from various samples

The more repeats of sequences there are for a given sample, the more accurate the DNA comparison will be, thus decreasing the likelihood of the sample matching multiple individuals. In other words, the more detailed the sample is, the more precise the comparison is in identifying the individual who possesses the DNA from the sample. A few drawbacks of this technique are the depth of the procedure, the physical invasiveness of obtaining the DNA sample, and the time required to perform a DNA comparison. Also contamination of the sample renders the comparison impossible. Most often, DNA biometrics is used for identification purposes as opposed to verification because the technique has yet to automate through technological advances. DNA sequencing, the process of generating a DNA profile, is compared to DNA samples previously acquired and catalogued in a database. The most common DNA database in existence is the CODIS System used by the Federal Bureau of Investigation. DNA biometrics technology is not advanced enough for universal use. Current DNA biometrics is far from that depicted in the movies.

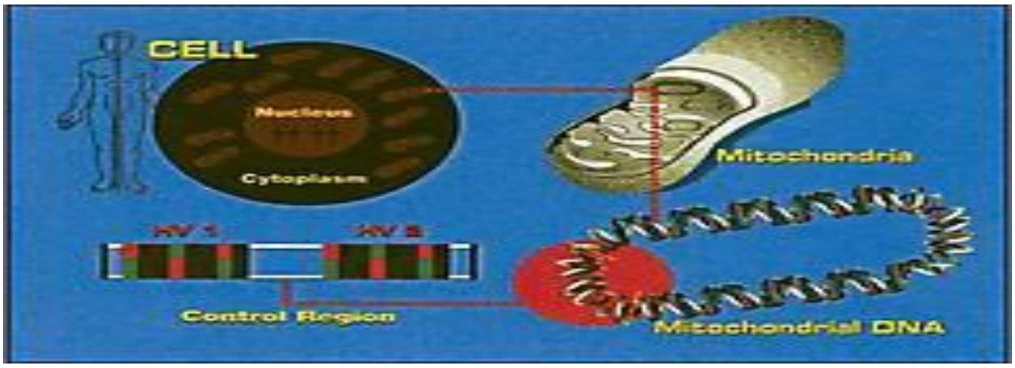

Fig. 6 DNA matching

3.4 HAND GEOMETRY RECOGNITION:

The hand geometry scanner looks for unique features in the structure of the hand. These unique features include the finger thickness, length, and width, the distances between finger joints, the hand's overall bone structure, etc. It should be noted here that with iris and fingerprint recognition, the primary goal is to look for extremely distinctive features. However, this is not the case with hand geometry recognition, as it is looking for moderately unique features. Thus, hand geometry recognition would not be the biometric tool of choice for high security applications or identification purposes where iris recognition or fingerprint recognition would be, respectively.

The user first places his or her hand onto a platen. This platen consists of 5 pegs which help the user position their fingers properly in order to insure quality enrollment and verification templates. The hand geometry scanner consists of a charged couple device camera (CCD), as well as various reflectors and mirrors in order to capture various black and white pictures of the hand. Two basic types of pictures of the hand are captured: (1) An image of the top of the hand; and (2) An image of the side of the hand.

In the enrollment phase, the user is prompted by the hand geometry scanner to place their hand on the platen three different times, so that three images can be captured and then averaged. The resulting image forms the basis for the enrollment template, which is then stored in the database of the hand geometry scanner. The enrollment phase can be accomplished in just five seconds.In the verification phase, the user is prompted to place their hand only once on the platen. An image is captured, and forms the basis for the verification template. The verification template is compared against the enrollment template, in the exact same fashion as fingerprint recognition. The verification phase can be accomplished in just under one second.

In the enrollment and verification phases, the hand geometry scanner takes 96 measurements of the hand. The enrollment and verification templates are only 9 bytes.

4. APPLICATIONS OF HAND GEOMETRY RECOGNITION

There are numerous types of applications for which hand geometry recognition is utilized. The most recognized use for this technology is in physical access entry applications, because the system is user-friendly to configure. In fact, this was the first application that this technology was used for when it first came out onto the market. Another application gaining popularity for hand geometry recognition is time and attendance. There are hand geometry scanners today that are just designed for this, as discussed previously. The advantage is that the use of timecards, identification badges, and Social Security numbers is eliminated. Also, the costly problem of "buddy punching" (associated with time clocks) is non-existent. Hand geometry recognition is also used for point of sale applications. Examples of this include subsidized school lunch programs and luxury hotels. All of these involve the use of the hand geometry scanner to deduct or debit money from a user's fund account when a purchase is made. Hand geometry recognition is also utilized in the Immigration and Naturalization Service Passenger Accelerated Service System (INSPASS). With this system, frequent international business travelers can simply use their hand geometry to enter the United States, rather than waiting in long immigration lines at the airport. Finally, hand geometry recognition is making a presence in the financial sector; a number of banks (in particular the Bank of America and the Nevada State Bank) are planning to adopt this technology to give customers easier and timely access to their safe deposit vaults.

5. CONCLUSIONS

Biobiometrics has been used effectively for more than a decade for time and attendance and workforce management. Despite widespread use, confusion and misconceptions about the technology and its capabilities persist. These concerns are easily dispelled when the facts about biometrics are established. · *Biobiometric*s offers unparalleled ability to quickly and accurately capture real-time, labor data and provide a nonrepudiated audit trail. *Biobiometrics* has undergone intense scrutiny and the results are in - when properly deployed, biometrics work well and are safe, secure, and accurate. · Biometrics offers organizations a broader range of direct and indirect time, cost, and operational benefits than alternative time and attendance methods.· Today over one hundred thousand thriving organizations rely on Easy Clocking's time & attendance systems to automate their employee attendance and as a result they are seeing a significant reduction in direct and indirect labor costs.

Biometrics refers to an automatic authentication of a person based on his physiological and/or behavioral characteristics. The usage of biometrics as a reliable means of authentication is currently gaining momentum, thou the industry is still evolving and emerging. The unimodal biometric recognition systems have to contend with a variety of problems and thus presently the amount of applications employing unimodal biometric systems is quite limited. Some limitations of the unimodal biometric systems can be alleviated by using multimodal biometric systems, which integrate information at various levels to improve performance. The future of biometrics can thus be envisaged to perhaps belong to multimodal biometric systems.

ACKNOWLEDGMENT

The author would like to thank Mrs. Anusiya for her guidance and support.

REFERENCES

[1] http://www.biometricsinstitute.org/pages/types-of-biometrics.html

[2] http://www.eye-controls.com/technology

[3] http://globalseci.com/?page_id=44

[4] http://dl.acm.org/citation.cfm?id=1929612

[5] http://www.ijarcsse.com/docs/papers/Volume_3/6_June2013/V3I6-0660.pdf

[6] http://www.patientsecure.com/palm-vein-recognition.html

[7] http://www.technologyexecutivesclub.com/Articles/security/artBiometricsSignatureRecognition.php

[8] http://misbiometrics.wikidot.com/dna

[9] http://www.technologyexecutivesclub.com/Articles/security/artBiometricsHandGeometryRecognition.php

[10] Dr. Stewart Hefferman, TSSI, Swindon, UK, Role of biometrics with document security.