International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 04 | Apr-2016 www.irjet.net p-ISSN: 2395-0072

Multi Modal Biometric Systems: A State of the Art Survey

G. Angeline Prasanna[1], K. Anandakumar[2], A. Bharathi [3]

[1] Research Scholar, Bharathiar University, Coimbatore - 641 046, Tamil Nadu, India

[2]Department of MCA, BannariAmman Institute of Technology, Erode - 638401, Tamil Nadu, India

[3] Department of IT, BannariAmman Institute of Technology, Erode - 638401, Tamil Nadu, India

---

Abstract - *In its most general definition, Biometrics refers to the science of automatic recognition of individuals based on some specific physiological and/or behavioral features. A biometric system that is based on one single biometric identifier does not always come to meet the desired performance requirements; multimodal biometric systems come to be an emergent trend. In this paper, we discuss the most commonly used unimodal biometric systems ranging from signature identification, facial recognition, DNA identification, speech authentication, hand geometry recognition, iris recognition and fingerprint identification. However, performances of such unimodal biometric recognition systems can degrade quickly when the input biometric traits suffer extensive variations; the importance of multimodal biometric systems is hence highlighted. Recent advances and application of multimodal biometric systems are then presented.*

***KeyWords*: multimodal biometric systems, iris recognition, facial recognition, gait identification, fusion**

1.INTRODUCTION

The design of multimodal interfacing systems has been growing substantially over the last few decades, and their applications have grown dramatically in functionalities in many fields. Some of these multimodal systems are human computer dialog interaction based systems where the user interacts with the PC through voice or vision or any other pointing device in order to complete a specific task. These kinds of systems seem to be very powerful and effective due to the fact that they allow the user to interact differently with the computer.

Other multimodal systems are less based on human computer dialog interaction, such as multimodal biometrics systems. They are used for identification purposes to provide more secure environments.

The use of biometric systems has grown quickly over the past decade. They are mostly used for identification systems implemented to provide a more secure environment, and authenticate the identity of people, while minimizing the chance of false positive or false negative (in terms of authentication). At the same time, the system should be fast enough to deal with possible real time traffics, as at physical checkpoints.

Photographs and fingerprints have been used as personal identification tools for many decades. More recently some more advanced biometrics tools have been developed, such as the case of measuring the geometry of the palm or hand; recognizing the pattern of blood vessels in a retina or the flecks of colour in an iris; or making the pattern in a person's DNA; as well as recognizing voices or faces, or the way people walk. Multimodal biometric systems that infer personal identification based on multiple physiological or behavioral characteristics are preferred. Consider, for example, a network logon application where a biometric system is used for user authentication. If a user cannot provide good fingerprint image due to a cut in the finger for example, then face and voice or other biometric identifiers can be used instead (or in conjunction). Voice identification as well cannot operate efficiently in a noisy environment or in the case where the user has some illness affecting his

voice. Facial recognition is not suitable if the background is cluttered, or if the person's stored information are several years old. For these reasons among others, multimodal biometric systems found their way to emerge in the recent and advanced authentication and security applications.

The remainder of the paper is organized as follow: Section 2 presents an overview on biometrics. Biometric techniques including unimodal and multimodal biometrics are presented in section 3. Section 4 then presents the most recent applications of unimodal and multimodal biometric systems. Section 5 concludes the paper with some suggestions for further investigations.

2. OVERVIEW ON BIOMETRICS

As later demonstrated in this paper, there are many different biometrics that could be utilized in a given system. However, despite the wide variety of possible biometrics, the key high-level structure of a biometrics system is the same [2]. First of all, the system has to develop a representation describing the discriminating features extracted from the biometric sample. These discriminating features could, for instance, be the relative locations of minutiae points extracted from a fingerprint [3] or an iris code from an iris. Each sample's representation is referred to as a template.

Clearly, a system has to allow for the addition or registration of new templates. This process is called enrolment. The templates are stored in a database and may be linked to particular information about the corresponding individual depending on the specific application [2].

Biometrics systems are usually used to accomplish one of two related objectives: identification or verification [4]. Identification refers to the process of trying to find a match between a query biometric sample and one stored in the database. For instance, to obtain access to a restricted area, one may go through an iris scan. A corresponding template describing the discriminating features is built for the scanned iris. Then the new template is compared to all those stored in the database. One is then granted or denied access depending on the existence of a database template similar to the query template. Verification, on the other hand, refers to the process of checking whether a query biometric sample belongs to a claimed identity. For instance, one may have to enter an ID number or use a particular card, then have one's iris scanned. The biometric system then has to only check whether the constructed query template is similar enough to the database template associated with the given ID number or card. From these descriptions, it should be obvious that verification is less computationally expensive and more robust than identification. However, identification is more convenient, less obtrusive, and is the only option when it comes to applications that attempt to find security threats. After all, criminals are unlikely to put forward their correct identities willingly.

As with any field, it is very important to have a widely used metric to measure performance of biometric system, so that systems could be compared, real-world performance can be estimated, and progress could be motivated. In biometrics, performance is ultimately based on the probability of accepting impostor users, referred to as False Acceptance Rate (FAR); and the probability of rejecting genuine users, referred to as False Rejection Rate (FRR). Plotting the value of (1 - FRR) against FAR produces what is known as the Receiver Operating Curve, which could be used for a graphical comparison of performance between different systems. For a simple empirical measure, the Equal Error Rate (EER) is usually used in biometrics, which refers to the point at which FRR and FAR are equal [5].

3 BIOMETRICS TECHNIQUES

Various behavioural and physical attributes could be used to identify an individual. We will visit briefly some of the most commonly used biometrics and present the advantages and disadvantages of using each one on its own. Then, we will move on to describe multimodal systems that consult more than one biometric before making an identification decision.

3.1 Unimodal Biometric systems

Numerous systems have been built that make use of one biometric for identification purposes. The biometric used can be especially suitable or inappropriate for a given application depending on its characteristic strengths and weaknesses. We carry out a brief survey to contrast the different commonly used biometrics outlining the basics of how they work and the motivations behind the use of each one.

3.1.1 Iris Recognition

The iris begins to form in the third month of gestation, and its patterns become unchangeable by the age of two or three. Furthermore, the iris pattern depends on the initial environment of the embryo, hence making the iris a unique feature and highly distinct from one person to another. In fact, even the left and the right irises for the same person are not identical.

The iris is isolated and protected from external environment and it is impossible to surgically modify the iris without unacceptable risk to vision. Additionally, its physiological response to light provides one of several natural tests against artifice [6]. Thus, given its uniqueness and permanence, iris recognition comes to be a popular biometric identification technology for personal identification.

Iris recognition identifies a person by analyzing the "unique" random patterns that are visible within the iris of an eye to form an iris code that is compared to iris templates in an existing database. The iris recognition process has six main steps [7]:

1. Image acquisition, as shown in figure 1, is one of the major challenges of automated iris recognition, because we need to capture a high-quality image of the iris while remaining non-invasive to the human operator.
2. Iris localization in which the edges of the iris and the pupil are detected to extract the iris region.
3. Normalization of the size of the iris region to ensure consistency between eye images despite the stretching of the iris induced by the pupil's dilation.
4. Unwrapping of the normalized iris region into a rectangular region.
5. Extraction of discrimination features in the iris pattern, so that a comparison between templates can be done.
6. Encoding of iris features using wavelets to construct the iris code to which input templates are compared in the matching step.

Although exhibiting a number of strong points, discussed above, iris recognition suffers from a few problems as well. For one thing, it is very difficult to perform at a distance larger than a few meters or if the person to be identified is not cooperating by holding the head still and looking into the camera. Iris recognition is susceptible to poor image quality, with associated failure to enrol rates [8]. Besides the iris is located behind a curved, wet, and reflecting surface and obscured by eyelashes, lenses, and reflections. It is partially occluded by eyelids. Also, it deforms non-elastically as pupil changes size [9]. All these reasons make image acquisition a critical operation to perform.

Figure 1: Iris scanner used to identify Baghdadi city council members [10]

3.1.2 Facial Recognition

Facial recognition is usually thought of as the primary way in which people recognize one another. After all, given a search through one's wallet, it becomes clear that

identification based on facial recognition is used by many organizations, such as universities, government agencies, and banks, although the recognition is usually carried out by a human. Many of these organizations will, of course, have these photos stored in large databases making many commercial and law-enforcement applications feasible given a reliable facial recognition system. Additionally, facial images of a person can usually be collected without necessarily requiring much co-operation from that person. Thus, it is no surprise that facial recognition is a key part of the DARPA-funded Human ID at a Distance Project aimed at developing the technology to identify terrorists from a distance [11].

Despite the aforementioned advantages of using facial recognition, it may perform very poorly when deployed in the real world, especially for recognition at a distance. A facial recognition system deployed in Logan International Airport to detect terrorists failed in 38 percent of the cases to match the identities of a test group of employees, according to a study by the American Civil Liberties Union [12]. A face-recognition system deployed on the streets of Tampa, Florida to identify criminals was scrapped two years later having not identified, alerted of, or caught any criminals, according to a spokesman for the Tampa Police Department [13].

There are many approaches that exist for tackling face recognition. Some of these approaches use the whole face as raw input, such as eigenfaces (figure 2) and fisherfaces, which are based on principal component analysis. Other approaches depend on extracting and matching certain features from the face, such the mouth and eyes. Lastly, some approaches are a mix of the two using data from the whole face as well as specific features to carry out the recognition [14].

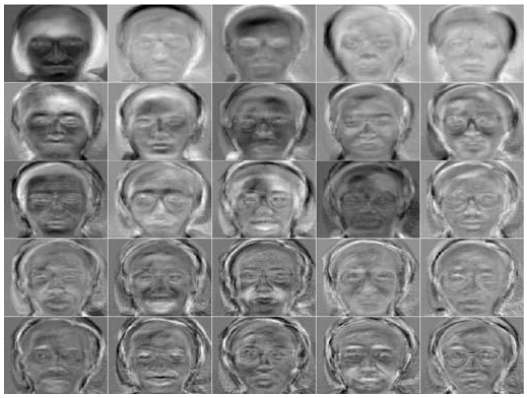

Figure 2: Images generated by Eigenfaces approach. [15]

3.1.3 Fingerprint Identification

According to the glossary of the Scientific Working Group on Friction Ridge Analysis, Study and Technology (SWGFAST) [16], "a fingerprint is an impression of the friction ridges of any part of the finger". The uniqueness of friction ridges tells us that no two fingers or palm prints are ever exactly alike; even two recorded successive impressions from the same finger are no identical [17].

Fingerprint identification is the process of comparing two or more friction skin ridge to determine if they are originated from the same finger (or palm, toe, etc.) under some threshold scoring rules.

One main shortcoming for fingerprint identification systems is that small injuries and burns highly affect the fingerprint. In fact, injury, whether temporary or permanent, can interfere with the scanning process. For example, bandaging a finger for a short period of time can impact the fingerprint scanning process. Something as simple as a burn to the identifying finger could make the fingerprint identification process fail [18]. Also add to this that the type of work that a person performs can also affect and sometimes damage some of fingerprint ridges as well.

Figure 3: Fingerprint ridges showing a loop pattern [19]

3.1.4 Voice Identification

A biometric system could be built based on the extraction and modelling of specific features from speech. This voice authentication process is based on an analysis of the vibrations created in the human vocal tract. The shape of a person's vocal tract determines the resonance of the voice which is fairly different from one to another due to the fact that everyone has a unique vocal tract in shape and size.

One advantage about the voice identification process is that it does not have to require a specific grammar and can be language independent; hence allowing callers to speak any phrase in any language they choose [20]. However, Human voice is generated though a complex process that involves the interactions of several body parts, especially the lungs, larynx and mouth. And hence, any small temporarily or permanent damage to any of these body parts can lead to a voice problem, and therefore highly affecting the identification process [21]. Besides, it would be possible that a tape recording is used to hack into a system.

3.1.5 DNA Identification

DNA (deoxyribonucleic acid), shown in figure 4, is the well-known double helix structure present in every human cell, and is used to produce a DNA fingerprint which is the same for every single cell of a person. A DNA fingerprint is robust and is impossible to be changed by surgery or any other known treatment. It is widely used in the diagnosis of disorders, paternity tests, criminal identification. Statistics show that that the chance of having two people with the same DNA profile is one to billion, making DNA testing at a very high degree of accuracy.

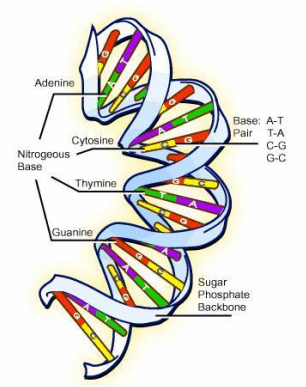

Figure 4: DNA double Helix [22]

On the other hand, DNA techniques are not able to distinguish between monozygotic twins which are formed when one fertilized egg splits, because they are the only people in the world with identical DNA profile. DNA faces several other challenges as well; several hours are required in order to obtain a fingerprint and the test is quite expensive to perform. Besides, DNA includes sensitive information related to genetic and medical aspects of individuals, and hence any misuse of DNA information can disclose the user's privacy. This is why people are fairly hostile to DNA usage [23].

3.1.6 Hand Geometry Recognition

While it does not occur to humans, in everyday life, to observe one's hand geometry to identify who they may be, primitive biometric systems that do just that have been in existence since the 1960s. Use of hand geometry has several advantages as shown by a survey of 129 users of a hand geometry biometric system at Purdue University's Recreation Centre. Out of the survey participants, 93% liked using the technology, 98% found it easy to use, and no one found the technology invasive of privacy [24].

Similar to other technologies, hand geometry's ease of use and acceptably amongst users does come at a cost. For one thing, hand geometry is not especially distinctive, especially when applied to a large population. Thus, it is most suitable for purposes of verification rather than

identification. Additionally, hand geometry may not be an ideal biometric to use if users include children whose hand-geometry template may vary during their growth period [25].

Figure 5: Hand Geometry Recognition system [27]

Hand geometry recognition can be done based on the measurement and matching of various features, such as the finger width, finger length, hand size, and hand contour. Most hand-geometry systems determine the different parts of the hand based on pins between fingers, restricting the position in which one can place one's hand [26]. Figure 5 shows one of such hand geometry recognition systems.

3.1.7 Gait Recognition

One's walk can be observed well from a distance or from security-camera video and checked against a database for a possible match. This ability to identify a person from a distance is gait's biggest asset, because it helps in building non-obtrusive authentications systems as well as helping to meet today's heightened security concerns. Alongside facial recognition, the Human ID at a Distance Project uses gait to help identify terrorists from a distance [11]. Additionally, it is difficult for one to deliberately copy someone else's way of walking [28]. Having said all of this, gait recognition is still in its infancy and has not faced many tests, especially for potential attacks [29].

Most of current approaches to gait recognition are based on silhouette analysis. Given video input of one's walk, a corresponding silhouette is formed, which is analyzed to produce a gait signature. The production of the signature and the matching process can be done using a variety of techniques, such as hidden Markov models and eigen analysis [30]. Recently, a very different type of approach to gait recognition has emerged that relies on having a physical device, such as an accelerometer, attached to one's physical body to collect data about one's gait. The new sensor- based approaches, however, give up gait's potential to identify from a distance [31].

3.1.8 Signature Verification

Signatures are composed of special characters and flourishes, which make them most of the time unreadable. Besides, intrapersonal variations and differences make the analysis of these signatures as complete images and not as letters and words important and unique [32]. That is why signatures have been accepted in government, legal, and commercial transactions as a method of verification.

There are two different types of signature verification: offline and online. The former takes only a signature's image and analyses it, and then compares it to the stored template to measure similarity (figure 6). The latter goes a step further and various features that are determined by the signing method are evaluated. Such features include the number of strokes used, the amount of pressure at a given point, and the writing speed. Online signature verification is more robust against forgery as it requires the forger to not only copy the signature's shape, but also copy the way it is written. However, online techniques cannot be applied for verifying signatures on documents or bank cheques [33].

The major problem faced with this technology is that a person’s signature changes with time and is highly affected by the physical and emotional conditions of the signatories. As a matter of fact, even successive signatures by the same person can be significantly different.

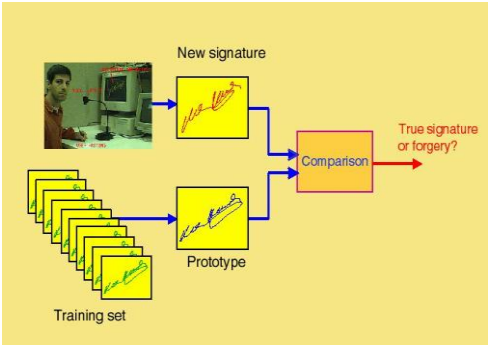

Figure 6: Signature Verification Process [34]

3.2 Multimodal Biometric Systems

As emphasized above, none of the biometrics can guarantee perfect recognition rates. Also, different biometrics has different strengths and weakness. Thus, conditions that may cause one biometric to fail may have no influence on another. For instance, if one's voice had changed because of a cold, speech identification may no longer be reliable, but the cold is unlikely to affect the reliability of fingerprint recognition. Alternatively, if one's finger incurred an injury, fingerprint identification may become less reliable than that of voice identification. This realization leads one to consider the possibility of using multiple biometrics together for the purpose of identification. A fusion module could be added that takes in output from multiple unimodal recognizers and attempts to make a conclusion based on the combined evidence.

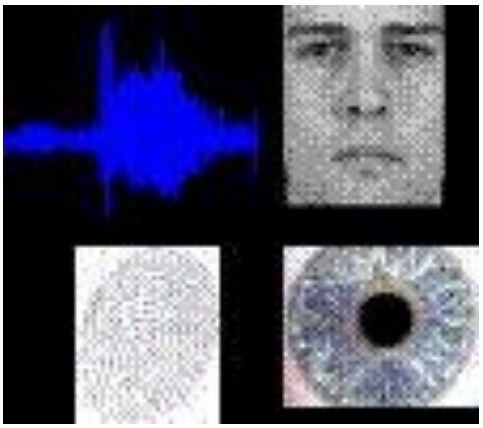

Figure 7: Multimodal Biometrics [35]

Many approaches exist for integrating multiple modalities. Fusion approaches can be distinguished in two ways. First of all, fusion could be carried out at different levels. Modalities could be combined at the feature level, the matching level, or the decision level. Secondly, fusion could be based on rules or based on machine-learning approaches [36]. Rule-based approaches include simple sum, max score, and min score [37]. Machine-learning approaches include support vector machines, minimum cost Bayesian classifier, Fisher's linear discriminant, decision trees, and multilayer perceptron [38].

3.2.1 Fusion at Feature Level

Fusion at the feature level may be most useful for closely-related modalities or for integrating input from multiple sensors of same modality. It normalizes features from multiple channels and includes all in one vector, and then it selects features using some specific mechanisms, such as sequential forward selection.

It calculates distance scores between a query vector and one in the database based on a measure, such as Euclidean distance. Feature Fusion produced best results when modalities are related (e.g. LDA-Red, LDA-Green, LDA-Blue) than when they were unrelated (e.g., hand and face) [39].

3.2.2 Fusion at Matching Level

Fusion at matching level normalizes scores of matchers to same domain using mechanisms such as Min Max, which maps score values to [0, 1], or Quadric-Line-Quadric function, which tries to separate the genuine and impostor score distributions [37]. Then it may use one or more of following approaches for the actual classification [37]

- Fixed rules, such as simple sum, maximum unimodal score, and minimum unimodal score
- Trained rules, such as Support Vector Machines, Fisher's Linear Discriminant, Bayesian Classifier, Multi-Layer Perceptron, and Decision Trees [40].
- Adaptive rules, such as assigning less weight to modalities that are disadvantaged by the current environment (e.g. too much background noise).

3.2.3 Fusion at Decision Level

Fusion of multiple biometrics can be also done at the decision level where each classifier provides its decision as "accept" or "reject". Then the Borda count method can be used for combining the classifiers' outputs. The Borda count is a winner election method in which voters rank candidates in order of preference. Candidates will receive a certain number of points depending on the position they hold. Finally, the winner of an election is the candidate with highest number of points.

One problem that appears with decision level fusion is the possibility of having a tie. Therefore it is necessary to have more classifiers than classes. Hence, for verification applications, at least three classifiers are needed because only two classes exist in a verification process ("yes" or "no"). But for identification cases, it is not practical and even sometimes not feasible to have more classifiers than classes; this is why combination level is usually applied to verification scenarios. Important combination schemes at this level are the serial and parallel combination ("AND" and "OR" combinations); where AND combination improves the False Acceptance Ratio (FAR) while the OR combination improves the False Rejection Ratio (FRR) [36].

4 Applications

Biometrics has been used in a wide range of applications. First, we categorize and present specific application examples based on the primary benefit of biometrics that they make use of. Then, we provide detailed descriptions of several interesting biometric applications.

4.1 Benefit and Examples

There are a wide variety of applications for biometrics in existence today. Of course, these applications have sprung up because of the benefits biometrics provides as an identification solution. Depending on the application, a particular benefit is usually emphasized, such as security, convenience or privacy.

4.1.1 Security

The uniqueness of biometric signals and the difficulty in forging them makes biometrics an attractive solution for enhancing security. The Republic of the Maldives, with the support of BioLink, introduced passports that come with microchips storing fingerprint and face templates. This technology allows for quick and reliable identification of citizens [41]. Mexico City International Airport installed Bioscrypt's V-Smart authentication system to provide access control to high-security areas of its terminals. The system requires use of a smart card that stores one's fingerprint template [42].

4.1.2 Convenience

Biometrics provide a very convenient solution that allows one to quickly authenticate into a system without necessarily having to carry anything, take the time to type anything, nor remember any secret strings. This convenience factor has attracted many manufacturers. Axxis Biometrics makes fingerprint-based door locks, such their 1Touch [43]. Also, mainstream Lenovo notebooks, such as the R Series come with an integrated fingerprint reader that lets users simply swipe their finger, rather than enter passwords to log in [44]. NCR, on the other hand, provides point-of-sale biometric terminals used to quickly authenticate sports bar employees to enter orders [45]. Columbia's Bancafe Bank incorporated NCR's fingerprint readers across all of its ATM network, so that users no longer need to carry an ATM card to make transactions [46].

4.1.3 Privacy Enhancement

Biometrics can be used as unique identifiers without revealing any personal information about the person they are identifying. Opposite to what many believe, biometrics could in fact enhance privacy. Thus, biometrics could be the ideal solution for social benefit programs where it is important to keep track of usage; but privacy is a major concern. On the Pakistan-Afghanistan border, the United Nations High Commission on Refugees (UNHCR) uses an iris recognition solution to ensure that each Afghani refugee obtains only one refugee package. To obtain a package, refugees have to authenticate via the iris recognition system.

If they are already in the database, then they are identified as having already received their package. If they are not in the database, then they are added to it and are given a package. The biometric database stores nothing but iris templates that are not linked with any personal information to the refugees [47].

4.2 Case Studies

In this section, four most recent applications of multimodal biometric systems are presented. Then one advanced application of unimodal biometric systems is highlighted.

4.2.1 E-passport in the European Union

The European Union's e-passport is one important security application of multimodal biometric systems. E-passport is an advanced smart card that holds digitized multi biometric features of its associated holder (figure 8). This card will substitute both the national identity card and the conventional passport and possibly other cards (e.g. driving license). It will be used for enhanced security of personal authentication.

The smart card uses a systematic cryptographic and public key infrastructure (PKI) and a number of private keys for each cardholder, as well as a visual identity that is a requirement for a travel document in EU.

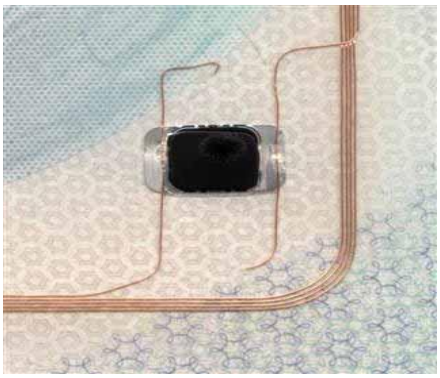

Figure 8: E-passport Chip [48]

The EU is studying the people's acceptance to e-passports Negative respondents in fact see that e-Passport has significant negative privacy consequences. The e-passport, with biometric identifiers, requires the disclosure of personal information which is stored on the smart card. However surveys show that fingerprint and iris identifiers received the highest preference from the respondents with 57% and 53% each. Therefore these types of biometrics should be taken into account first when implementing the e-passport. Another clear preference was noticed in the favour of applications related to Banking and Government (e.g. driving license, national ID and passport) [49].

4.2.2 BioID

Another notable multimodal biometric technology is HumanScan's BioID technology [50], which combines face, voice and lip movement information to identify users (see figure 9). It has a number of positive features. First of all, it costs little to set up and install. A standard USB camera and a microphone are all that is needed in terms of input devices. Also, it is fairly unobtrusive requiring one little more than to look at the camera and say something. Lastly, BioID can be configured to use any single one or combination of face, voice and lip movement biometrics. BioID is not tied to any specific application, but simply provides an Application Programming Interface (API) that makes it integratable into existing applications. In fact, the API used is BioAPI [51] compliant. BioAPI is an international standard for biometric APIs allowing applications to be developed independently of the biometrics systems they may use. [52] claims that BioID could be used for controlling access to physical locations, as well as access to technical systems and that BioID had demonstrated reliability in many installations around the world. However, no specific examples are provided, nor performance evaluations are published.

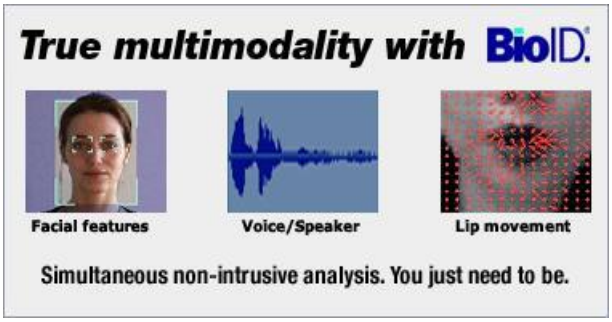

Figure 9: Bio-ID System [53]

4.2.3 Human ID

The Defense Advanced Research Projects Agency (DARPA) in USA is currently developing a program called Human Identification at a Distance (HumanID). The program aims at developing automated biometric identification technologies to detect, recognize and identify humans at great distances (25-150 feet) [11].

Techniques being investigated are face recognition; recognition from body dynamics in video including gait; recognition from infrared, multi-spectral, and hyperspectral imagery. Methods for fusing biometric technologies into advanced human identification systems will be developed to enable faster, more accurate and unconstrained identification of humans.

Program manager, Jonathon Philips holds good future ideas for the HumanID project. Despite all the tough challenges the program faces, he has faith in newer techniques that will be emerging to enhance the proficiency and accuracy of this project that will be of great help and use to the Intelligence, Information Access Division, and the security organizations [54].

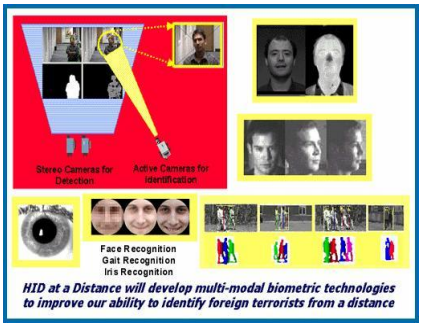

Figure 10: Poster on "Human ID" system [55]

4.2.4 Restricted Area Identity Card

Another interesting recent application for multimodal biometric systems is the biometric ID card (also called as the Restricted Area Identity Card) that will be introduced by the federal Canadian government for workers at 29 major airports by the end of the year 2007. This card uses both fingerprint and iris biometrics in order to identify 120,000 workers who have permission to access restricted areas at the airport. The card has a small computer chip that stores the cardholder's fingerprint and iris templates. The biometric reader at the airport will scan the individual and the card, and compare the information presented by the individual with the data stored on the card in order to test if that individual is indeed the cardholder, then it checks if the cardholder has access to the particular restricted area or not. The government hopes to finish implementing the system at the airports and issuing the cards by December 31, 2007 [56].

4.2.5 ATM Vein Authentication

Most ATMs today in Europe and North America require customer to authenticate using a card and a PIN. However, fraudsters have found ways to obtain such information. A fraudster can install a skimming device that reads a card's magnetic strip and a mini-camera to capture the entry of a PIN [57]. When Japan faced a dramatic rise in card fraud in 2003, authorities forced banks to adopt new more secure methods of authentications. Since then, most Japanese banks have adopted finger vein technology offered by Hitachi (figure 11). The biometric system works by emitting near-infrared rays that pass through the finger and are absorbed by the haemoglobin. Since haemoglobin is present only within the veins, dark areas will appear only wherever veins exist. The resulting image can be captured by a camera and used for matching against templates that were collected in the same manner [58].

Figure 11: Hitachi Finger Vein Authentication [59]

This new method of ATM authentication was not used to replace any of the existing cards or PIN security layers, but was added as an additional layer making it surely

more difficult to commit fraud [60]. As for the reliability of the vein biometric layer on its own, its false acceptance rate is extremely low at 0.0001% with a verification time of less than 0.5 seconds. Additionally, vein biometric is not externally visible making it more difficult to forge and is not affected by injuries or common sickness [58]. Thus, it should not be surprising to find that the International Biometric Group ranked vein biometric as the best biometric in both aspects: effectiveness and usability [60].

5. CONCLUSIONS

In this paper, we have highlighted the most commonly used unimodel biometric systems. We also presented the importance of multimodal biometrics systems for providing a more secure environment with higher authentication accuracy by overcoming the limitations of individual biometrics. Some recent applications of these types of systems were then presented.

It can be concluded that multimodal biometric systems that infer personal identification based on multiple physiological or behavioral characteristics are preferred because of their robustness against the failure of one specific biometric identifier.

REFERENCES

[1] A. Ross and A.K. Jain, "Multimodal biometrics: an overview", *Proceedings of 12th European Signal Processing Conference (EUSIPCO)*, Vienna, Austria, pp 1221-1224 (2004).

[2] A.C. Weaver, "Biometric authentication", *Computer*, 39(2), pp 96-97 (2006).

[3] S. Prabhakar and A. Jain, "Fingerprint identification", http://biometrics.cse.msu.edu/fingerprint.html, visited on 15/10/2007.

[4] J. Ortega-Garcia, J. Bigun, D. Reynolds and J. Gonzalez-Rodriguez, "Authentication gets personal with biometrics", *Signal Processing Magazine, IEEE*, 21(2), pp 50-62 (2004).

[5] R. Tronci, G. Giacinto and F. Roli, "Selection of experts for the design of multiple biometric systems", *Lecture Notes in Computer Science*, 4571, pp 795-809 (2007).

[6] Y.P. Huang, S.W. Luo and E.Y. Chen, "An efficient iris recognition system", *Proceedings of First International Conference on Machine Learning and Cybernetics*, Beijing, pp 4-5 (2002).

[7] J. Daugman, "How iris recognition works", *IEEE Transactions on Circuits and Systems for Video Technology*, 14(1), pp 21-30 (2004).

[8] J. Daugman, "The importance of being random: statistical principles of iris recognition", *Pattern Recognition*, 36(2), pp 279-291 (2003).

[9] P. Blythe and J. Fridrich, "Secure digital camera", *Digital Forensic Research Workshop*, Baltimore, Maryland, (2004).

[10] Wikimedia,"Image",http://upload.wikimedia.org/ wikipedia/commons/c/cf/Retinal_scan _securimetrics .jpg , visited on 15/10/2007.

[11] Electronic Frontier Foundation, "Human ID at a distance(HumanID)", http://w2.eff.org/Privacy/TIA/ hid.php, visited on 15/10/2007.

[12] S. Murphy and H. Bray, "Face recognition devices failed in test at Logan", http://www.boston.com/news/local /articles/2003/ 09/03/face_ recognition_ devices_ failed _in_test_a t_logan/, visited on 15/10/2007.

[13] L.M. Bowman, "Tampa drops face-recognition system", http://www.news.com/Tampa-drops-face-recognition-system/2100-1029_3-5066795.html, visited on 15/10/2007.

[14] W. Zhao, R. Chellappa, P. Phillips and A. Rosenfeld, "Face recognition: a literature survey", *ACM Computing Surveys*, 35(4), pp 399-458 (2003).

[15] Christopher DeCoro's Website at Computer Science Department of Princeton University, "Face recognition using Eigenfaces", http://www.cs. princeton. edu/ ~ cdecoro/eigenfaces /eigenfaces.jpg, visited on 15/10/2007.

[16] SWGFAST, "Glossary", http://www.swgfast.org/ Glossary_Consolidated_ ver_1.pdf, visited on

15/10/2007.

[17] D.R. Ashbaugh, "Ridgeology", *Journal of Forensic Identification*, 41(1), pp 16-64 (1991).

[18] R. Jamieson, G. Stephen and S. Kuma, "Fingerprint identification: an aid to the authentication process", *Information Systems Audit and Control Association*, 1, (2005).

[19] Department of Electrical and Computer Engineering at University of Delaware, "Image taken from course number: eleg675", http://www.ee.udel.edu/~barner/courses/eleg675/ Images/Fingerprint.jpg, visited on 15/10/2007.

[20] Voice Recognition and Speech Recognition Software and Vendors Guide, "Biometric identification", http://www.voice-commands.com/510.htm, visited on 15/10/2007.

[21] Yahoo Health, "Voice problems", http://health. yahoo.com/topic/other/other/article/ healthwise/ty7247, visited on 15/10/2007.

[22] D. Secko, "A monk's flourishing garden: the basics of molecular biology explained", http://www.scq. ubc. ca/a-monks-flourishing-garden-the-basics-of-molecular-biology-explained/, visited on 15/10/2007.

[23] I. Maghiros, Y. Punie, S. Delaitre, E. Lignos, C. Rodríguez, M. Ulbrich, M. Cabrera, B. Clements, L. Beslay and R. Van-Bavel, "Biometrics at the frontiers: assessing the impact on society - for the European parliament committee on citizens freedoms and rights, justice and home affairs (LIBE)", *Institute for Prospective Technological Studies*, (2005).

[24] E. Kukula and S. Elliott, "Implementation of hand geometry: an analysis of user perspectives and system performance", *Aerospace and Electronic Systems Magazine, IEEE*, 21(3), pp 3-9 (2006).

[25] K. Delac and M. Grgic, "A survey of biometric recognition methods", *Electronics in Marine, 2004, Proceedings Elmar 2004, 46th International Symposium*, pp 184-193 (2004).

[26] G. Boreki and A. Zimmer, "Hand geometry: a new approach for feature extraction", *Proceedings of the Fourth IEEE Workshop on Automatic Identification Advanced Technologies*, pp 149-154 (2005).

[27] Sandia Control Systems Inc., "Products", http:// sandiacontrolsystems.com/img/HGU.jpg, visited on 15/10/2007.

[28] L. Wang, H. Ning, T. Tan and W. Hu, "Fusion of static and dynamic body biometrics for gait recognition", *IEEE Transactions on Circuits and Systems for Video Technology*, 14(2), pp 149-158 (2004).

[29] D. Gafurov, E. Snekkenes and P. Bours, "Spoof attacks on gait authentication system", *IEEE Transactions on Information Forensics and Security*, 2(3), pp 491-502 (2007).

[30] M. Nixon and J. Carter, "Advances in automatic gait recognition", *Proceedings of the Sixth IEEE International Conference on Automatic Face and Gesture Recognition 2004*, pp 139-144 (2004).

[31] D. Gafurov, K. Helkala and T. Søndrol, "Biometric gait authentication using accelerometer sensor", *Journal of Computers*, 1(7), pp 51-59 (2006). J.F. Vélez, Á. Sánchez and A.B. Moreno, "Robust off-line signature verification using compression networks and positional cuttings", *Proceedings of the 2003 IEEE Workshop on Neural Networks for Signal Processing*, pp 627-636 (2003).

[32] A. Kholmatov and B. Yanikoglu, "Identity authentication using improved online signature verification method", *Pattern Recognition Letters*, 26(15), pp 2400-2408 (2005).

[33] M.E. Munich Website, "Camera-based ID verification by signature tracking", http://www.vision.caltech.edu / mariomu/research/ sigverif/sv.gif, visited on 15/10/2007.

[34] Electrical and Computer Engineering Department of Carnegie Mellon University, "Advanced multimedia processing lab projects", http://amp.ece.cmu. edu/

projects/images/image00 8.gif, visited on 15/10/2007.

[35] M. Faundez-Zanuy, "2004, Data fusion in biometrics", *IEEE Aerospace and Electronic Systems Magazine*, 20(1), pp 34-38 (2005).

[36] M. Indovina, U. Uludag, R. Snelick, A. Mink and A. Jain, "Multimodal biometric authentication methods: a COTS approach", *Proceeding of the MMUA 2003, Workshop on Multimodal User Authentication*, Santa Barbara, California, pp 99-106 (2003).

[37] S. Ben-Yacoub, Y. Abdeljaoued and E. Mayoraz, "Fusion of face and speech data for person identity verification", *IEEE Transactions on Neural Networks*, 10(5), pp 1065-1074 (1999).

[38] A. Ross and R. Govindarajan, "Feature level fusion using hand and face biometrics", *Proceedings of the SPIE Conference on Biometric Technology for Human Identification II*, 5779, pp 196–204 (2005).

[39] K.A. Toh, X. Jiang and W.Y. Yau, "Exploiting global and local decisions for multimodal biometrics verification", *IEEE Transactions on Signal Processing*, 52(10), pp 3059-3072 (2004).

[40] BioLink, "BioLink fingerprint biometrics in Maldivian passports", http://www.biolinksolutions.com / print.asp?nItem ID=162, visited on 15/10/2007.

[41] Bioscrypt, "Mexico City International Airport Uses Bioscrypt's Identity and Access Management Solution in New State-of-the-Art Terminal", http://www.bioscrypt .com/news/press/item-845/, visited on 15/10/2007.

[42] Axis Biometrics, "Products", http://www.axxisbiometrics. com/products/index. cfm, visited on 15/10/2007.

[43] Lenovo, "Security, fingerprint reader, overview", http://www.pc.ibm.com/ca/security/fingerprintre ader.html, visited on 15/10/2007.

[45] NCR, "Smooth's sports grille deploys POS with fingerprint recognition for employee use", http://www.ncr.com /about_ncr/media_informatio n/news_releases/2007/may/051707b.jsp?lang=E N, visited on 15/10/2007.

[46] ATM Market Place, "Columbia's Bancafe Bank introduces ATM finger-scanning technology", http://www.atmmarketplace.com/article.php?id= 5253, visited on 15/10/2007.

[47] C.M. Most, "Towards privacy enhancing applications of biometrics", *Digital ID World Magazine*, June/July 2004 Issue, pp 18-20 (2004).

[48] The New York City Independent Media Centre, "Image archives of 08/2006", http://nyc.indymedia.org/ images/2006/08/74861. jpg, visited on 15/10/2007.

[49] G. Ng-Kruelle, P.A. Swatman, J.F. Hampe and D.S. Rebne, "Biometrics and e-Identity (e-Passport) in the European Union: end-user perspectives on the adoption of a controversial innovation", *Journal of Theoretical and Applied Electronic Commerce Research*, 1(2), pp 12-35 (2006).

[50] HumanScan: Boid, "Home page", http://www.bioid.com, visited on 15/10/2007.

[51] BioAPI Consortium, "Home page", http://www.bioapi.org, visited on 15/10/2007.

[52] R. Frischholz and U. Dieckmann, "BiolD: a multimodal biometric identification system", *Computer*, 33(2), pp 64-68 (2000).

[53] Secure Systems, "ControlSphere biometric extension", http://www.securesystems.lv/images/bioid.png, visited on 15/10/2007.

[54] P. Wallich, "Getting the message", *IEEE Spectrum*, 40(4), pp 38-42 (2003).

[55] 21C Magazine, "Human ID at a distance", http://www.21cmagazine.com/issue2/iao_remix/ humanid.html, visited on 15/10/2007.

[56] CBC News, "Biometric ID cards coming for airport workers", http://www.cbc.ca/technology/story/2006/11/10/ airports-card.html, visited on 15/10/2007.

[57] BBC News, "Cash machine fraud up, say banks", http://news.bbc.co.uk/2/hi/uk_news/6115974.stm , visited on 15/10/2007.

[58] P. Jones, "Banking on vein at the ATM", *Biometric Technology Today*, 14(5), pp 8-9 (2006).

[59] S. Vickers, "Could this be the end of Chip and PIN?", http://www.info4security.com/pictures/thumb/r/o /p/FINGER.jpg, visited on 15/10/2007.

[60] R. Condon, "New biometrics see right through you", *Infosecurity*, Jan/Feb 2007 Issue, pp 24-25 (2007).