Journal of Applied Mathematics & Bioinformatics, vol.3, no.4, 2013, 141-161
ISSN: 1792-6602 (print), 1792-6939 (online)
Scienpress Ltd, 2013

Encryption and Biometrics:Context, methodologies and perspectives of biological data

K. Havenetidis[1]

Abstract

The majority of the authentication systems found today can be broken or stolen and generally are characterized by reduced security. Therefore, numerous efforts have been made in developing effective methods in the areas of cryptography, data hiding and biometrics in order to achieve an enhanced level of information security. Biometrics or Biometric authentication uses subjects' biological (DNA, ear, face, fingerprint, gait-body motion, hand geometry-vein pattern, iris-retina and odor) and behavioural data (keystroke dynamics, signature, smell and voice) in order to improve security and convenience. However, there are important technological challenges such as accuracy, reliability, data security, user acceptance, cost, and interoperability, as well as challenges associated with ensuring effective privacy protections. Although iris-retina scan and face thermogram gather most of the characteristics of an ideal biometric system the final biometric selection should be based on application's purpose. Recently, novel approaches for the development of practical biometric identification systems have led to security enhancement of biometrics and cryptography. One of the most

[1] Faculty of Military Sciences, Hellenic Military Academy, Vari - 16673, Greece.
E-mail: havenetidisk@sse.gr

Article Info: *Received* : August 1, 2013. *Revised* : October 20, 2013.
Published online : December 10, 2013.

efficient methodologies towards security maximization of biometrics and cryptography seems to be the use of multimodality biometrics data since each biometric modality separately has its weaknesses. Other promising methods include cancellable biometrics via atrifacts which seems to overcome most of the risks and vulnerabilities related to security and privacy.

Mathematics Subject Classification: 92C55; 94A08; 92C10

Keywords: Encryption; Multimodal Biometrics; Unimodal Biometrics; Cancellable Biometrics

1 Introduction

Personal identification systems that rely on knowledge are subject to loss, counterfeiting, and theft. Such systems suffer from the inability to identify the genuine user (usually based on passwords) if the information is borrowed on permission of the user. The development of an identification system based on biometrics has attracted a great deal of interest as it obviates the requirement for physical possession or memorization of a security code and has the potential to differentiate individuals with high accuracy [1-4].

In all biometric systems the basic steps are i) Enrollment: recording of biological-behavioral data ii) Storage: Analysis of the specific trait and translation to a code or graph and iii) Comparison: Collation of the current with the stored biological data and acceptance or rejection of the user. When ccombining biometrics and cryptography there is a replacement of security code with biometric data in order encryption-decryption process to be efficient and secure (Figure 1).

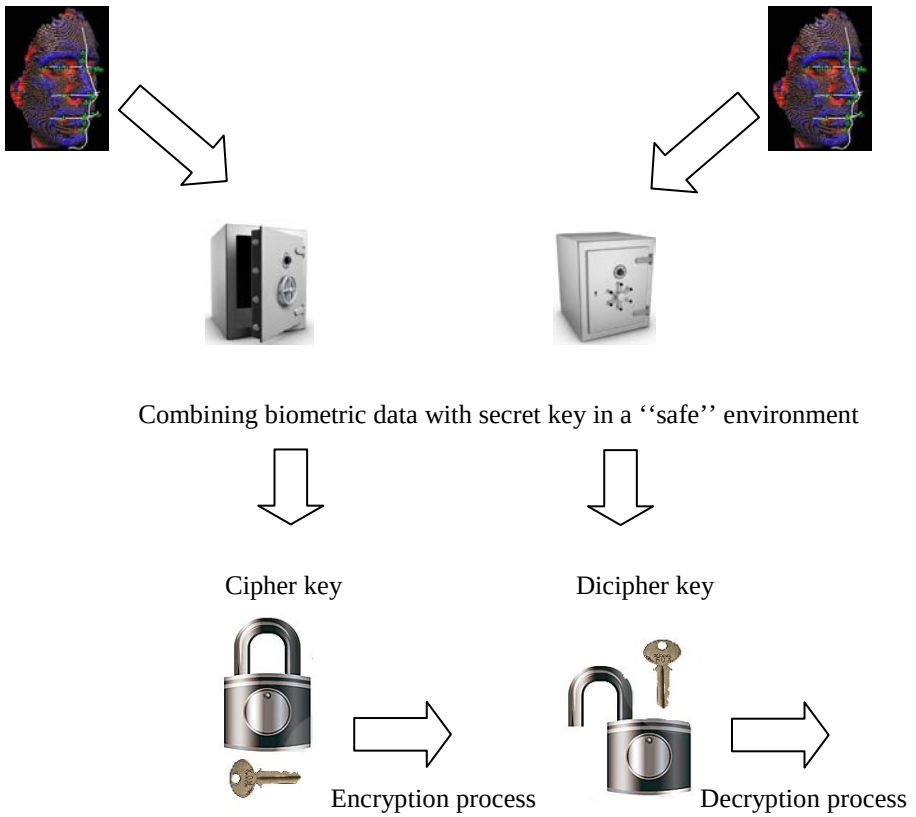

Figure 1: Integration of biometrics with cryptography

The significance of biometric usage on global security is recognized by the increasing number of countries which apply biometrics for various purposes. Specifically, the U.S.A. was a pioneer in biometrics in the 1970s with the development of automated systems for physical access control, time-attendance and personal identification. In the 1990s Australia, Canada and Brazil implemented biometrics for border security, immigration and passports issue. With the dawn of the 20th century an explosion of biometric systems was evident for many countries (India, Gambia, Israel, New Zealand, all European Union countries) [5] for other ‘‘non-traditional’’ various purposes such as voting, school accounts and athletes’ security. Currently biometrics’ everyday applications are classified in three main categories: i) Commercial **(**cellular phone, computer network login, electronic data security, internet access, ATM, credit card, physical

access control, medical records management, distance learning) ii) Government **(**correctional facility, driver's license, social security, border-passport control, national ID card.) and iii) Law enforcement (forensic applications, computer access, immigration, national identity, physical access, prisons, telecommunications). In military, biometrics' applications are not well known but it is likely to include i) use of vehicles with integrated biometrics that would proceed to human or object recognition (forward observation; ambulance; convoy support) during military operations in hostile environment, ii) access control in military bases iii) aircraft or riffle equipped with user identification systems iv) personal portable or stationary devices that help soldiers identifying friendly population following occupation and v) detection of health deterioration in time.

Biometrics includes various sources of biological and behavioral data. The former covers a wide range of sources such as DNA, ear, face, fingerprint, gait-body motion, hand geometry-vein pattern, iris-retina and odor [6,7], whilst the latter only keystroke dynamics, signature and voice. The present paper will briefly present the biological data as it provides a rosy prospect for accurately identifying a persons' identity.

2 Sources of biological data used in biometrics

2.1 Deoxyribo Nucleic Acid (DNA)- Genes

Every cell in a human body contains a copy of DNA which does not differ from person to person, but 0.1% would be unique to each individual [8]. The chance of two individuals sharing the same DNA profile is less than one in a hundred billion. The procedure of determining DNA can only accomplished in a laboratory and comprises four phases:

- Isolation (blood, saliva, hair, urine, semen, tissue)
- Cutting into shorter fragments

- Sort fragments by size
- Comparison of fragments in different samples

The above procedure used to last (completion time) 3-7 hours but recently, it has been reduced to 30-50 minutes with the increasing power of modern computers. DNA is digital, increasing the accuracy and allowing true recall to be gained for the process of authentication [9].

2.2 Ear

Identification by ear biometrics is promising because it is passive like face recognition, but instead of the difficulties to extract face biometrics, it uses robust and simply extracted biometrics like those in fingerprinting [10]. Amongst the numerous methods of ear identification, the common ones are: (i) taking a photo-video of an ear (comparison with previous entries, anatomical sites, distances, skin texture), (ii) taking "earmarks" via pressure against a flat glass and (iii) taking thermogram pictures of the ear [11, 12]. There is also a new experimental method [optoacoustic emissions (OAEs)] where the presence of the subject is not necessary, as ears' morphology is determined by the reflection of sounds emitted from the ear (via telephone) to an ultralow-noise microphone [13].

2.3 Facial recognition

Face recognition is accomplished with the use of an ordinary video camera and a computer and includes four techniques: Facial geometry, skin pattern recognition, facial thermogram (requires an infrared camera) and skin deformation (dynamic instead of static facial features). Facial geometry detect subjects' facial features (Eyebrow, wrinkles, shadows, lip shape) and use these as patterns. 3D systems create a model of the users face and matching is conducted between the

subjects bone and facial structure. The matching process uses a set of features are stored as vectors where

$$x = \left[a_1(x),\ a_2(x), \ldots,\ a_n(x) \right],$$

see in [14].

The Euclidean distance is computed between the features for 2 sets giving an indication of how similar the sets of features are [10]. A sum is made over the squared difference between all the features, the square root of which is used to give an overall variation between the two sets,

$$d(x_i, x_j) = \sqrt{\sum_{r=1}^{n} \left(a_r(x_i) - a_r(x_j) \right)^2}$$

see in [14].

This is compared to a threshold, if it is below the threshold the two subjects are considered to match, otherwise they are different subjects.

Infrared imaging uses temperature data from different regions of the face, such as nose and mouth, in order to detect differences and authenticate a subject. However, infrared sensors are prohibitively expensive which is a factor inhibiting wide spread use of the thermograms.

2.4 Fingerprint

The fingerprint biometric is a method used for more than a century for identification, primarily by law enforcement agencies. In the 1970s the old ink-and-paper procedure was replaced by an automated system which recently became digital [15]. The basic patterns of fingerprints are loops, whorls and arches that can be found in fingerprints [16]. Fingerprints are categorized in Latent (2D, by chance, perspiration-oil-powder print), known (intentional, chemical print-digital scan), and plastic (left in a malleable substrate, wax-putty impressions). The standard methodology used by fingerprint experts to conduct friction ridge

examinations is called ACE-V, for analysis, comparison, evaluation, and verification, which are the four fundamental phases utilized in this process [16]. Fingerprint recognition is considered a ‘‘balanced’’ biometric tool regarding accuracy, validity, cost and rapidity [17].

2.5 Gait-body motion

Motion analysis is relatively new biometric method and its instrumentation comprises one camera (2D), or 3-4 high speed cameras (3D) (Figure 1), or 6-12 cameras for optoreflective systems (6-20 known points; Figure 2) (3D) alongside with the appropriate software. The last set of cameras are used to solve the direct linear transformation equations employed for reconstruction of 3-D displacement data. There are many variables measured through theses systems such as joint forces, speed-acceleration, derived measures (angular speed), kinematics, inverse dynamics, body segment and joint angles, electromyography (optional), ground reaction forces, movement simulation [18] (Figure 3).

In gait analysis there is no need for camera use since the subject walks over a pad (force platform; Figure 4) which measures contact time, plantar pressure (Mean, Peak), center of pressure, pressure per pixel, and displacement. However, gait can be altered throughout time (gain in body weight) therefore, preliminary results on gait analysis need to confirm its potential.

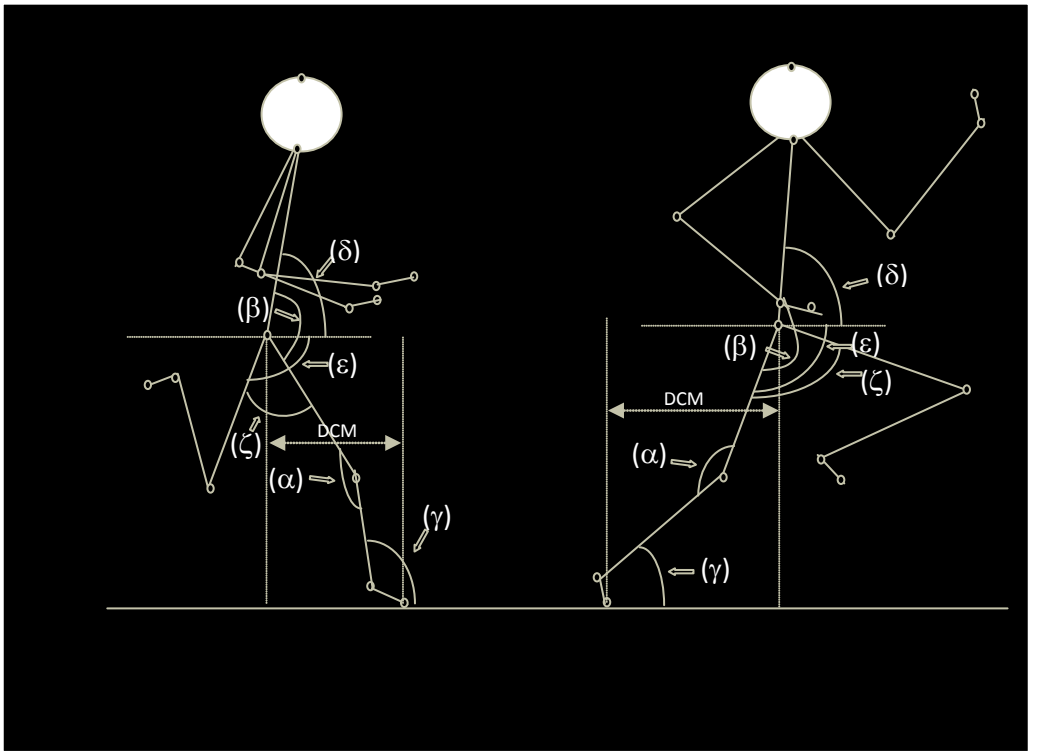

Figure 1: Variables measured during motion 3D analysis

Figure 2: Optoreflective system

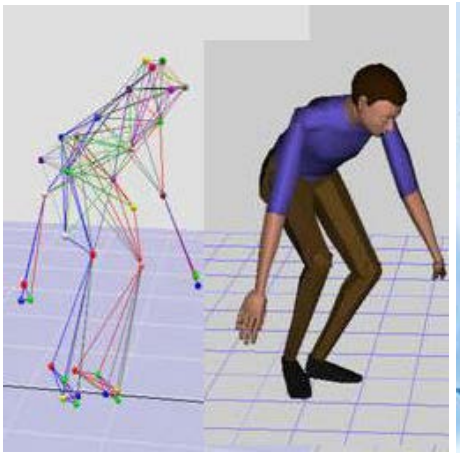

Figure 3: Movement simulation

Figure 4: Pressure pad

2.6 Hand-palm geometry

Hand-palm geometry uses automated systems equipped with digital camera and light and predetermined position for fingers scan various characteristics of hand-palm such as length, width, thickness, surface area and curvature.

The geometry of the hand is not known to be very distinctive and hand geometry-based recognition systems cannot be scaled up for systems requiring identification of an individual from a large population (19). However, more sophisticated systems determine the palm-vein pattern using infrared light where absorption of hemoglobin in the blood produces a black appearance of veins in the picture. In both systems there is no use of radioactive particles and all information can be on the server or an ID card.

2.7 Iris-retina identification

Iris-retina are visible but protected structures, which do not usually change over time, thus, making them ideal for biometric identification. The canning system uses a CCD digital camera under both visible and near-infrared light to take a clear, high-contrast picture of a person's iris. With near-infrared light, a person's pupil is very black, making it easy for the computer to isolate the pupil and iris. Usually, the eye is placed 3 to 10 inches from the camera. When the camera takes a picture, the computer locates the center-edge of the pupil, the edge of the iris and the eyelids and eyelashes. Eyeglasses and contact lenses typically do not interfere or cause inaccurate readings. Although, the early iris-based recognition systems required considerable user participation and were expensive, the newer systems have become more user-friendly and cost-effective [19].

2.8 Odor

Olfaction process is a difficult task as different people have different perception of the same odor as there is no physical continuum as sound frequency in hearing or Newton's circle in colour vision [20]. The human olfaction comprises four stages: Sniffing, Reception, Detection and Cleansing [21]. The respective electronic sensing system uses various sensors (conductivity, piezoelectric, optical fiber and Spectrometry-Based sensors) [22-25] whilst the pattern recognition system uses statistical and neuromorphic methods to detect and classify each odor [26-27]. Currently, there is limited information regarding the accuracy of the methods used in the electronic sense devices and exactly numerical algorithms.

In Table 1 are presented most of the advantages and disadvantages associated with biological data used in biometrics.

Table 1: Advantages and disadvantages

Biological data	**Advantages**	**Disadvantages**
	High precision (all data are digital) and convenience	High cost
DNA	It is extremely hard to forge or imitate	Influence on manipulators' objectivity (a realistic portrait easily identifies the subject in question)
	A large amount of research & money has been invested on DNA processing	Identical twins share the same DNA
		Lack of computational power to perform DNA sequencing in 'real-time' conditions

Table 1 continues		
	Unique	Various sources affect data (camera light-angle, gravity, oil-wax
Ear	Non-intrusive	built up, pose)
	Convenient (OAEs)	Low quality images will be rejected by the computer
		Subject must cooperate with reader (remove hat-hair-jewelry)
	Unique data (combined with 3D modelling)	Alcohol influence
Face recognition *with thermogram*	High precision (high number of reference points 19,000 vs 80 for finger)	Influence on manipulators' objectivity (a realistic portrait easily identifies the subject in question)
	Non-intrusive	
	Input is stable	
	Subjects can be evaluated covertly, without their knowledge	
	Easy set-up (setting an ordinary camera)	Can be fooled by identical twins
Face recognition *without thermogram*	No age effects	Effect of various sources (makeup, pose, illumination, camera angle and distance)
	Non-intrusive	Difficulty in data interpretation
	The EER for facial recognition algorithms can be very high	
	Non-invasive technique	Scanners can be fooled with fake fingers
	Unique data	Low quality images will be rejected by the computer
	Impossible to re-construct	The system is secure at the time of enrolment
	Replay attacks are hard to implement	Slow database search

Table 1 continues		
Fingerprint	The EER for fingerprint match algorithms can be low	The size of a fingerprint template is relatively large
	Stable input	Various sources (scar, bruises, dry skin) affect image quality
	Huge databases are already in existence	Scanning device can be by-passed
Gait	Convenient	Data alterations throughout lifetime (injuries, training, footwear)
	Subjects can be evaluated covertly, without their knowledge	Specialized personnel for data processing
	Non-intrusive (2D)	Large data template
Body motion	Unique data	High cost (3D)
	Various sources of data	Time consuming
		Subject must cooperate with reader
		Specialized personnel for data processing
	Small template size	No open search (1:N) capability
Geometry	Non-intrusive	Readers are relatively large, easily damaged
	1:1 match accuracy	Readers are expensive
Vein pattern	Input is stable through lifetime Highly accurate Easily taken sample	Lack of proven reliability
		Enrolment is highly intrusive
		Specialised personnel
Iris	Unique data, Input is stable through lifetime, Non-intrusive	Large data template, Frequent improperly focused image, Single-source High cost , Has not been proven a 1:N match capability

Table 1 continues		
Retina	Input is stable, except in the case of certain degenerative retinal diseases Fast verification Small template size	Intrusive with high discomfort level, Subject must cooperate with reader; refusal to cooperate is not apparent to the tester, Single source, No proven ability to carry out 1:N searching
	Non-intrusive Unique data	No available commercial applications for person authentication
		High cost
Odor		Use of many sensors each one for specific odor
		Inability to detect mixtures
		Various sources of error (diet, environment, fatigue)
		Information processing mechanisms of human olfaction entirely is still unknown

The above Table clearly shows that each single biometric modality has its weakness. However, the selection of the appropriate biometric source should be based on prioritization of the following characteristics in order to form the ‘‘perfect’’ human identification system. This system ought to be unique (e.g. Odor), permanent (e.g. Iris), universal (e.g. Retina), precise (e.g. DNA), storable (e.g. Motion analysis), eexclusive (e.g. Vein pattern), cost-effective (e.g. Fingerprint), convenient (e.g. Ear), simple (e.g. Gait analysis) and socially acceptable (e.g. Face geometry). A classification of each biometric tool according to the mentioned characteristics is shown in Figure 2. In general, a score above 2.5 or below 1.5 is considered optimal and inadequate respectively.

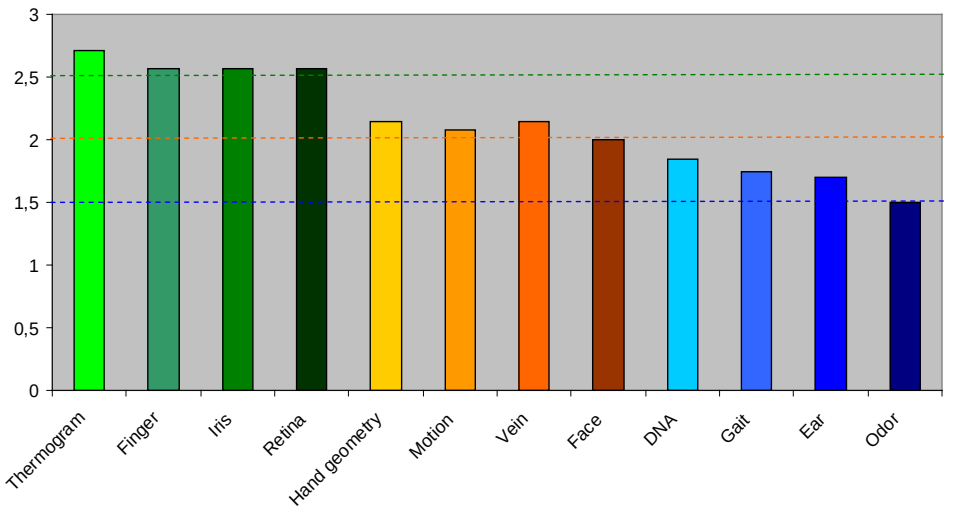

Figure 2: Classification of biometrics (biological sources) based on performances in various characteristics

The above Figure indicates that face recognition using thermogram, fingerprint and iris-retina scan gather most of the characteristics that could determine the ideal biometric system. Alternatively, ear and odor are not considered promising methods on subject identification. However, the determinative factor for selecting a biometric source seems to depend on the application's purpose.

3 Maximizing biometrics' efficiency

Apart from the security threats that reduce biometrics' reliability, there are also a number of specific privacy concerns risks which threaten user confidence and lead to a lack of acceptance and trust in biometric systems.

Biometric Encryption is a process that securely binds a digital key to a biometric or generates a key from the biometric. In essence, the key is ''encrypted'' with the biometric, and the resulting biometrically encrypted key,

also called BE template or helper data, is stored. The digital key can be ‘‘decrypted’’ on verification if a correct biometric sample is presented. This ‘‘encryption/decryption’’ process is fuzzy by nature, because the biometric sample is different each time, unlike an encryption key in conventional cryptography. However, various approaches have been followed such as Fuzzy vault, secure sketches, extract phase information through Fourier transform and error correction codes in order to resolve these problems [28-29]. A major technological challenge is to have the same digital key recreated despite the natural variations in the input biometrics [30].

Another method that can also improve biometrics' recognition accuracy and strengthen the resistance against spoof attacks [31-33] is the use of multimodal biometric systems. In multimodal biometric systems data from at least two single modalities can be utilised by an individual system or independent systems which can function separately and their decisions may be combined [34]. Possible schemes of combining various biometric cues in multimodal biometrics include the fusion of 2D and 3D face images [35]; 3D facial shape and infrared facial heat pattern image [36], faces and fingerprints [37] and face and gait [38]. Another version of multimodal biometrics is the combination of ‘‘hard’’ with ‘‘soft’’ biometrics. The former refers to biological-behavioural characteristics (primary information) for personal identification whilst, the latter to personal ancillary information (age, gender, ethnicity, height). It has been reported [39] that this combination can lead to an increased recognition rate by 6% using hydrid biometric system (Figure 3) that uses face and fingerprint as the primary biometrics and integrated with secondary biometrics (gender, ethnicity, and height).

Finally, a novel method of cancelable biometrics (Hashing template) which combines biological data with the use of an artifact has shown a greater control of the security level, convenience in biological registration and resistance to spoofing. In this method [40] the artifact (a transparent sticker with two dots)

attached to source of biological data (finger) is used during enrollment phase. In the identification phase, additional data, apart from the one obtained during e.g. finger geometry can be provided such as the position and direction of the artifact in relation to the biological source. Once the artifact is altered or removed from the biological source, re-enrolment is required which upgrades the system to a higher security level.

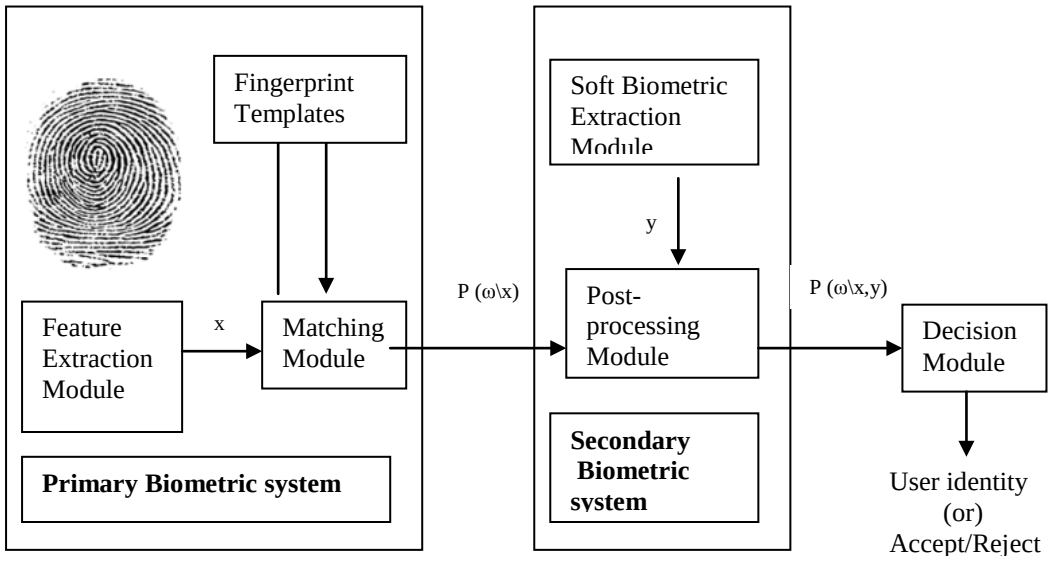

Figure 3: General framework for soft biometric integration with hard biometrics [39]

5 Conclusion

Biometric systems may add a new level of authentication and identification to applications, but are not, however, without their risks and challenges. From the unimodal biometric systems there is not one biometric modality that is best for all implementations and no biometric technique is foolproof. Although significant progress has been made in security enhancement of biometrics and cryptography over the past decade, much remains to be done. Evolution in biometric technology

has led to the use of multimodality biometrics data, novel bioencryption methods and cancellable biometrics via artifacts. These promising methods will definitely have a profound influence on global security and privacy.

References

[1] A.K. Jain, R. Bolle and S. Pankanti, *Biometrics: Personal identification in networked society*, Norwell, MA: Kluwer, 1999.

[2] A. Ross and A. K. Jain, Multimodal Biometrics: An Overview, *Proceedings of the 12th European Signal Processing Conference*, (2004), 1221-1224.

[3] N. K. Ratha, A. Senior and R. M. Bolle, Automated Biometrics, *Proceedings of the International Conference on Advances in Pattern Recognition*, (2001).

[4] B. Moreno, A. Sánchez and J. F. Vélez, On the Use of Outer Ear Images for Personal Identification in Security Applications, *Proceedings of the 33rd Annual International Carnahan Conference on Security Technology*, (1999), 469-476.

[5] J.H. Hoepman, E. Hubbers, B. Jacobs, M. Oostdijk and R. Wichers Schreur Advances in Information and Computer Security Crossing Borders: Security and Privacy Issues of the European e-Passport Lecture Notes, *Computer Science*, **4266**, (2006), 152-167.

[6] K. Rabuzin, M. Baca and M. Malekovic, A Multimodal Biometric System Implemented within an Active Database Management System, *Journal of Software*, **2**(4), (2007), 24-31.

[7] M. Baca, and K. Rabuzin, Biometrics in Network Security, *Proceedings of the XXVIII International Convention MIPRO,* (2005), 205-210.

[8] http://www.genomenewsnetwork.org/resources/whats_a_genome/Chp1_1_1.shtml, 2003.

[9] S.Z. Li, *Encyclopedia of Biometrics*, Springer publications, 2009.

[10] M. Rahman, R. Islam, N. Islam, B. Ahmed and A. Islam, Person Identification Using Ear Biometrics, *International Journal of The Computer, the Internet and Management*, **15**(2), (May - August, 2007), 1-8.

[11] M. Burge and W. Burger, Ear Biometrics in Computer Vision, *Proceedings of the 15th International Conference of Pattern Recognition*, ICPR 2000, (2000), 826-830.

[12] H.M. El-Bakry and N. Mastorakis, Ear recognition by using neural networks, *Proceedings of the 11th International Conference on Mathematical methods and computational techniques in Electrical engineering*, (2009), 770-804.

[13] M.A. Swabey, S.P. Beeby, A.D. Brown and J.E. Chad, Using Otoacoustic Emissions as a Biometric, *Biometric Authentication Lecture Notes in Computer Science*, **3072**, (2004), 600-606.

[14] T. Zhang, X. Li, D. Tao and J. Yang, Multi-modal biometrics using geometry preserving projections, *Pattern Recognition*, **41**(3), (2008), 805-813.

[15] J.D. Woodward, N.M. Orland and P.T. Higgins, *Biometrics*, New York, McGraw Hill Osborne, 2003.

[16] N. Kaushal and P. Kaushal, Human Identification and Fingerprints: A Review, *Journal of Biometrics and Biostatistics*, **2**(123), (November, 2011), doi:10.4172/2155-6180.1000123.

[17] I. Maghiros, Y. Punie, S. Delaitre, E. Lignos, C. Rodriguez, M. Ulbrich, M. Cabrera, B. Clements, L. Beslay and R. VanBavel, Biometrics at the Frontiers: Assessing the Impact on Society, (2005), http://trid.trb.org/view.aspx?id=767172.

[18] J.A. Alderson and B.C. Elliot, *Image analysis in sport performance*, in Applied anatomy and biomechanics in sport, T. R. Ackland, B. C. Elliot, and J. Bloomfield, Human Kinetics Publishers, 2009.

[19] A.K. Jain, A. Ross and S. Prabhakar, An Introduction to Biometric, *IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics*, **14**(1), (2004), 4-20.

[20] G. Wyszecki and W. Stiles, *Color science: concepts and methods, quantitative data and formulae*, Wiley press, 1982.

[21] P. Keller, Overview of Electronic Nose Algorithms, *International Joint Conference of Neural Networks*, (1999).

[22] T. Nakamoto, A. Fukunda and T. Moriizumi, Perfume and Flavor Identification by Odor-Sensing System Using Quartz-Resonator Sensor Array and Neural Network Pattern Recognition, *Actuator B*, **18/19**, (1994), 282-290.

[23] Y. Okahata and O. Shimizu, Olfactory Reception on a Multibilayer-Coated Piezoelectric Crtstal in a Gas Phase, *Langmuir*, **3**(6), (1987), 1171-1172.

[24] H. Sundgren, F. Winquist and I. Lundstrom, Artificial Neural Network and Statistical Pattern Recognition Improve MOSFET Gas Sensor Array Calibration, *Proceedings of the International conference on Transducers, Solid-State Sensors and Actuators, Digest of Technical Papers*, (1991), 574-577.

[25] G.F. Fernando, D.J. Webb and P. Ferdinand, Optical-Fiber Sensors, *MRS Bulletin*, **27**(5), (May, 2002), 359-364.

[26] C. Linster, F. Grasso and W. Getz, Olfactory Coding: Myths, Models and Data, *Proceedings of the Neural Information Processing Systems Post-Conference Workshop*, (1998).

[27] J. Jackson, *Principal Component Analysis*, John Wiley & Sons press, 1991.

[28] A. Juels, and M, Sudan, A fuzzy vault scheme, in Lapidoth, A., Teletar, E. (eds.) *Proceedings of IEEE International Symposium on Information Theory*, (2002), 402-420.

[29] Y. Dodis, R. Ostrovsky, L. Reyzin and A. Smith, *Fuzzy Extractors: How to Generate Strong Keys from Biometrics and other Noisy Data*, Springer-Verlag Press, 2007.

[30] A. Cavoukian and A. Stoianov, *Biometric Encryption Encyclopedia of Biometrics*, Springer, pp. 1-14, 2009.

[31] L. Hong, A.K. Jain and S. Pankanti, Can multibiometrics improve performance?, *Proceedings of IEEE Workshop on Automatic Identification Advanced Technologies*, (1999), 59-64.

[32] A.K. Jain, K. Nandakumar and A.A. Ross, Score normalization in multimodal biometric systems, *Pattern Recognition*, **38**, (2005), 2270- 2285.

[33] A. K. Jain, K. Nandakumar, U. Uludag and X. Lu, *Multimodal Biometrics: Augmenting Face With Other Cues*, in Face Processing: Advanced Modelling and Methods, Zhao, W. Chellappa, R. (Eds.), Elsevier Press, 2006.

[34] E. Camlikaya, A. Kholmatov and B. Yanikoglu, Multi-biometric Templates Using Fingerprint and Voice, *Biometric technology for human identification*, **6944**(5), (2008), 1-9.

[35] K.I. Chang, K.W. Bowyer and P.J. Flynn, An Evaluation of Multimodal 2D+3D Face Biometrics, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, **27**, (2005), 619-624.

[36] K.I. Chang, K.W. Bowyer, P.J. Flynn and X. Chen, Multi-biometrics using facial appearance, shape and temperature, *Proceedings of the IEEE International Conference on Automatic Face and Gesture Recognition*, (2004).

[37] H. Lin and J. Anil, Integrating faces and fingerprints for personal identification, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, **20**, (1998), 1295-1307.

[38] G. Shakhnarovich, L. Lee and T. Darrell, Integrated face and gait recognition from multiple views, *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, **1**, (2001), 439-446.

[39] A.K. Jain, S.C. Dass and K. Nandaumar, Can Soft Biometric Traits Assist User Recognition?, *Proceedings of SPIE on Biometric Technology for Human Identification*, (2004), 1-12.

[40] N. Nishiuchi and H. Soya, Cancelable Biometric Identification by Combining Biological Data with Artifacts, *Proceedings of the International Conference on Biometrics and Kansei Engineering*, (2011), 125-142.