ISSN: 0974-5572
IJCTA
International Journal of
CONTROL THEORY
AND APPLICATIONS
UGC APPROVED JOURNAL
ज्ञान-विज्ञान विमुक्तये
INTERNATIONAL SCIENCE PRESS
Gurgaon, Haryana (India)

International Journal of Control Theory and Applications

ISSN : 0974-5572

© **International Science Press**

Volume 10 • Number 35 • 2017

Research Challenges in Multimodal Biometrics – A Critical Review

Ayesha Tarannum[a], Srinivasulu Tadisetty[b] and Md. Zia Ur Rahman[c]

[a]Research scholar Department of E.C.E., K.L. University, Vaddeswaram, Guntur DT, A.P., 522502, India. Email: ayeshabad14@gmail.com
[b]Corresponding author, Professor, Department of E.C.E., Kakatiya University College of Engineering and Technology, Kakatiya University, Warangal-506009, India. Email: drstadisetty@gmail.com
[c]Professor, Department of EC.E., K.L. University, Green Fields, Vaddeswaram, Guntur. A.P., 522502, India. Email: mdzr55@gmail.com

Abstract: There are many evolving changes with the era of information security in terms of new technology. The advent of biometric system is one among them. The biometric system brings a sophisticated authentication to every individual in the social era. The biometric system and most of its characteristics facilitate a unique original signature of an individual which is broadly accepted. Therefore, the Biometric systems usage in most of the applications is become a mandatory to achieve better authenticity. This paper encapsulates the latest research trends in multimodal biometric as per meticulous literature survey and also review the impact on various applications

Keywords: Unimodal biometrics, multimodal biometrics, authentication, authorization, cryptography, secret keys, fusion metrics, performance and quality metrics.

1. INTRODUCTION

The biometric system facilitates an accuracy and standard consistency over many other traditional approaches. The term biometric revels the fact aboutthe certain biological phenomena and constituent parts under various observations. The biometric system expeditiously makes use of both behavioral and physical attributes such as hand geometry, finger prints, iris, palm, retina and face for the identification of individuals [1, 2].The system completely depends upon "whom the person is" and "what he has got to do". In short, it specifies the authorized personnel and specific imposter [3]. Any behavioral and physiological specification can be read as biometric until and unless it fulfills the below mentioned facts [4].

Universality: Each and every individual must possess unique characteristic.

Uniqueness: Either of any two individuals must not have similar characteristics.

Immutability/performance: The existing characteristics of any individual should be invariant from time to time.

Togetherness: The attributes are quantitatively measured and can also be related as per the needs and requirements with utmost priority.

Circumvention: Fraudulent systems are growing at a speed pace and can be easily circumvented.

Performance: It pinpoints the precision levels after identification.

Acceptability: The probabilistic ratio which defines the accepatace of the users for the usage of the biometric system.

The usage of the biometric technology primarily relies on its application domain. Any biometric system cannot meet its requirements to maximum extent, for example- its cost, acceptability, and accuracy. This clearly shows that biometric is purely optional and completely optimal [5]. The biometric characteristic “Finger print” plays a vital role in presenting enormous advantages over many other biometrics. The finger print characteristics include uniqueness, relative temporal invariance and acquisition ease. The following below mentioned Table 1 entails the biometric techniques with respect to seven factors. Several myths revealed that the usage of biometrics are very advangateous over the traditional voice print techniques. Most usually Finger scan and Iris scan are the modest technologies in the era of biometrics. Finger and iris scan proved themselves in delivering high performance, fast processing and accuracy. The Table 1 clearly depicted the performance aspects of finger prints and has shown the metrics that stated the measures are better compared to other biometric techniques. The biometric technique of finger print has been using since several years because of its distinctiveness for personal identification. Finger print biometric system works with basic two principles.

1. **Individuality:** Each and every individual is identified with unique finger print. No two persons in this universe possess the similar finger prints. Thus the biometrics can be operated in two ways. They are identification and verification method

   A. *The identification method:* The method initially determines an unknown individual as primary task through finger print.

   B. *The verification method:* The method on the other hand verifies whether the already taken finger print is either rejected or accepted. The method plays a crucial role in authenticating and authorizing an individual.

2. **Persistence:** All the characteristics of biometrics do not change with time variance.

The finger print biometric methodology is being extensively used to many multitasking applications in the fast growing era. Some of them include security breaches at national and international airports, defense and in many other government sectors. Therefore at the current scenario for enhaced security aspects, all advanced personal and enterprise applications tend to use the latest multimodal biometric systems. Though biometric systems are advancing interms of safety, security and authentication, it still holds few limitations for data being stolen or shared to unauthorized access. Inspite of many security approaches, the biometric system always proved itself as best with various algorithmic approaches and resulted in user friendly with enhancingsecurity and improving the authenticity.

2. BIOMETRIC SYSTEMS

The word biometric hailed from two latin words ‘bios’ and ‘measure’. ‘Bios’stands for bio and ‘measure’ stands for metrics. The biometric approach kindle pattern recognition system to mark and authenticate specific individual impressions through biological and physiological characteristics [2]. The Figure 1-1 depicts the biometric system as five categories of subsystems. They are as (1) Data collection, (2) Transmission, (3) Data storage, (4) Signal processing, (5) Decision systems.

Table 1
Resemblances between various biometrics, as per the extracts of A. Jain [2], Uldag [5], on the basis of (High = 100, Medium = 75, Low = 50)

Biometrics	*Universality*	*Uniqueness*	*Permanence*	*Collectability*	*Performance*	*Acceptability*	*circumvention*	*Average*
Face	100	50	75	100	50	100	50	75
Fingerprint	75	100	100	75	100	75	100	89.3
Hand geometry	75	75	75	100	75	75	75	78.6
Keystrokes	50	50	50	75	50	75	75	60.7
Hand veins	75	75	75	75	75	75	100	78.6
Iris	100	100	100	75	100	50	100	89.3
Retinal scan	100	100	75	50	100	50	100	82.1
Signature	50	50	50	100	50	100	50	64.3
voice	75	50	50	75	50	100	50	64.3
Gait	75	50	50	100	50	100	75	71.4

Pattern: A sensor which is duly equipped in an electronic gadget is used to collect preliminary biometric samples of a respective individual which is also called as Data collection.

Transmission: In this system, the sampled data in the Data collection module is further compressed, processes the signal and is further transmitted to the storage.

Data storage: All the gathered templates of the biometric sampled images are stored successfully.

Signal processing: The features of the image is clearly extracted by using varioius pattern recognition systems, pattern matching techniques and image processing systems.

Decision systems: Decision making is the crucial role in signaling the right decision. The decision system performs the verification process by matching the scores obtained from images.

The Figure 1 depicts the Biometric system, with an acquisition box which acquires the preliminary data from the individual. Then the collected and sampled is being validated through quality accesor to improve performance.

The latest bio-crypto systems are gaining popularity, which is the latest development. The bio-crypt systems and their performance vary accordingly with the standards of the Bio-metric. If the quality of bio-metric is extreme, then the Bio-crypt is better choice. The bio-cryptography will provide better authentic solutions. The latest review and discussions are as follows

3. CRYPTOGRAPHY

The word cryptography is termed as the science of hiding the original content of data and tracing back the original information when required. Cryptography almost relates to encryption methodologies. It stands with the conversion of a plain text in to another format of data called cipher text [7]. The alternative source of methodology to retrieve source information from cipher text is the “Decryption”. A logical algorithm serves for both decrypting and encrypting the biometric process. The complete operation modes of cipher can be solely controlled and monitored by a ‘key’. The key is said to be the key parameter which is acknowledged only by the message to the sender and the receiver. The key may be used for both encryption and decryption during the passage of information. Keys are so vital, since, all ciphers without protection of keys are easily breakable and information may be stolen by the third party in a quicker pace.

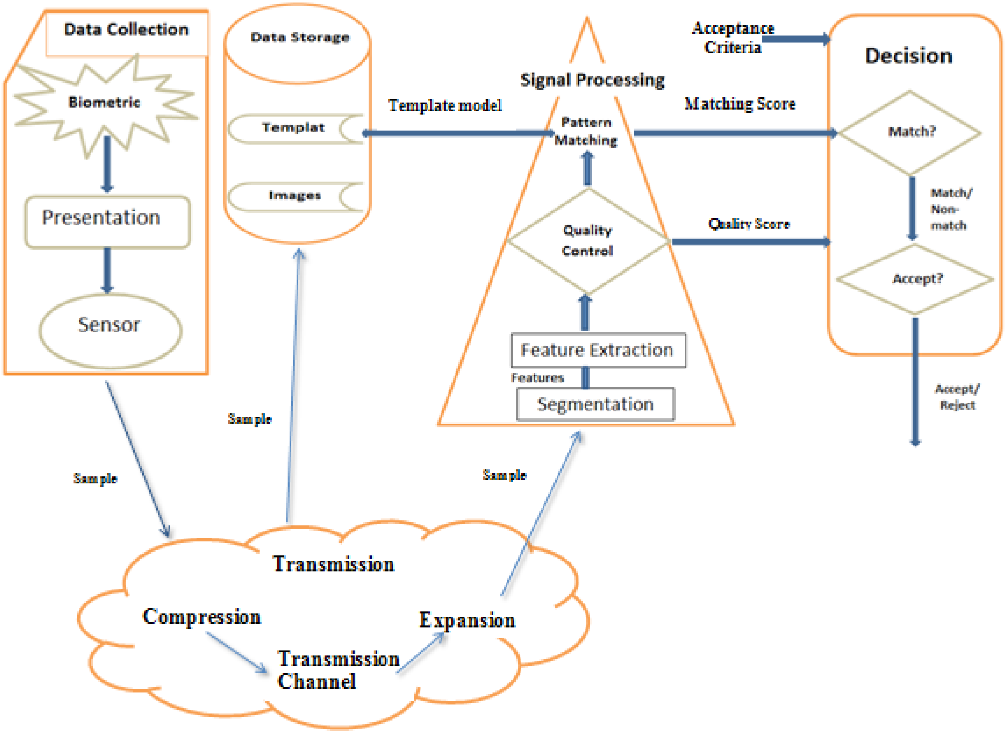


Figure 1: Block diagram of a generic biometric system [6]

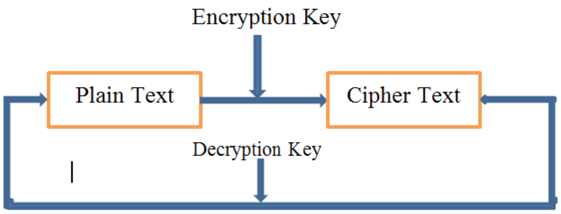


Figure 2: Block diagram of a generic cryptography

Cryptography is also an important methodology to protect and secure confidential data. Cryptography can be applied for the security of e-commerce, e-mails, computer passwords, kiosks and ATM cards. Cryptography is deployed not only for the sake of protection of authenticated information but also it serves confidential information from theft or hacking from any intruders across the communication channels.

The schemes of the cryptography are primarily categorized into three types. They are

(a) The symmetric key or the secret key cryptography.

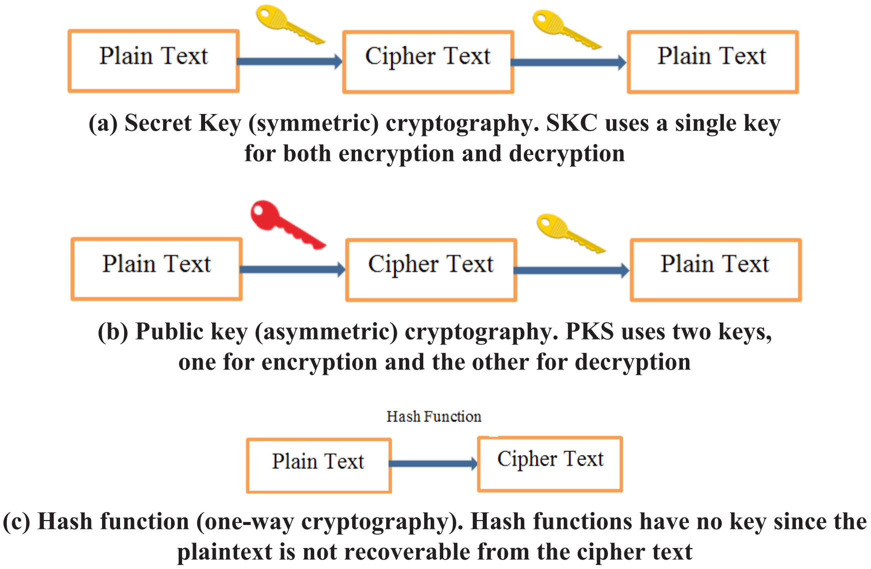
(b) The asymmetric key or the public key cryptography.

(c) The hash functions of the cryptography.

The above mentioned three types of cryptography are clearly shown in figure 1-3. In particular, the general information is called as simple or plain text. Later it is encrypted in to cipher text either by using any of the above mentioned three types.

1. A standard unique key is generally employed for encrypting and decrypting the original source biometric samples.
2. The alternate approach is the usage of two keys called the public key generally employed for encrypting and decryping the sources.
3. The Hash function methodology for cryptography deploys a fixed length value.

All the schemes in the cryptography are optimized for some specific use and application. The hash function cryptography is best known for data integrity because any change made in the source is immediately affected at the receiver. All the contents of the message also change. Besides, the secret key cryptography is ideally best for encrypting the messages. In this process, the sender, who wishes to send messages, shall generate a session key per each message aimed to the receiver. The receiver on the other hand uses the same session key (key used for encryption) to decrypt the message context. The public key cryptography is a process of exchanging of key application.



(a) Secret Key (symmetric) cryptography. SKC uses a single key for both encryption and decryption

(b) Public key (asymmetric) cryptography. PKS uses two keys, one for encryption and the other for decryption

(c) Hash function (one-way cryptography). Hash functions have no key since the plaintext is not recoverable from the cipher text

Figure 3. Cryptography types a) secret key b) public key and c) hash function

The generalized classification and verification system of the unimodal fingerprint system is entailed in [11]. The complete projection system is dependent on a feedback for feature extraction stage. Further feature extraction stage moves with feature refinement mode to rapidly increase quality metrics. The quality measures and improvement characteristics are passed through a finger print verification system such that the Gabor filter is imposed at the input stage of the image to further enhance image quality. Ratha et. al., [11] came forward with Graphical representation for unimodal Biometric system using “distortion – tolerant “finger print authentication technique. Under their supervision and implementation, a weighted graph is employed for both the reference finger print and the query finger print. The proposed methodology has undergone much supervision across various databases with an optical biometric sensor and resulted better.

The IRIS recognition systems [12], on the other hand along with the 2Dimension wavelet filters and the Gabor filters are used exclusively for extraction of feature from the image. The method is obviously non-reactive to rotation and translation of the image and is perfectly tolerant to high level illumination. This method which uses Gabor filter generated 98.3 % accuracy and 82.51 % with wavelet. The complete observations and experiment was carried at CASIA database. The Gabor filters and several multi channels had been implemented to record the local texture and information of theIRIS. The result set implementations gave better improvement in performance as FRR = 2.17 % and FAR = 0.01 % in the CASIA databases [13].

In general, the unimodal biometric system prevail many disadvantages due to its dependency on its uniqueness in biometric feature. Some of the instances of this type are processing errors, acquisition of features, distinctiveness among features and temporarily unavailability of features. All these may affect the accuracy of the system. A multi model biometric system is another source to improve the performance aspects by combining one or more biometric systems. Hence, there is a definite need to raise the concept of multi model biometric approach to this fast growing technology market.

As per research [14], Conti et. al., introduced a multi model biometric system with the integration of acquisition to two different finger prints. He came up with the usage of fuggy logic approach for matching up of the score fusion. Various experiment set ups have been conducted on this approach for both the matching scores fusions and the decision level fusion. The experiment resulted better performance with 6.7% for matching –score level fusion.

On the other hand yang and ma [10] used hand generated palm prints and finger prints to generate identification of individual. The characteristics are obtained from the same image unlike as other multi model systems. Their matching score fusion is considered successively from one characteristic to another. To say, primarily palm prints, secondly finger prints and so on. The complete system under testing environment produced better outputs with 98 subjects.

Besbes et. al., [15] stepped forward with another multi model biometric system with the integration of IRIS and finger prints. They followed a hybrid methodology based on IRIS template and finger print minutiae extraction through various mathematical notations with the extracted fragments in the IRIS region. This methodology uses the unimodal decision specifying with 'AND' operator. Further, no experimental setup has been carried out to analyze the performance.

Acquiler et. al., [16] introduced the multi model biometric method with the extraction of Gabor filter and Fourier transformations [FFT] for finger prints. Statistical metrics and other local features were taken in to consideration for novel stage recognition. This methodology undergoes usage of left and right hand thumbs. Each thumb finger print is processed successively and the experimental setup have resulted FRR = 1.4% and FAR = 0.2% with consideration of 50 subjects. Prasad and Subbarayudu [17], produced their experimental result sets of multi modal biometric system (both palm print and IRIS), unimodal palm print system and unimodal IRIS system. The feature fusion compares all of their fusion scores with the template vector to test the performance issues. The experiment was carried out with above 600 images from about 100 different subjects.

The biometric system which is dependent on cryptography generates the corresponding cryptographic keys for standard detection and usual authentication. Lifang Wu et. al.[18], generated Bio-metric cryptosystem depending on the face detection called face biometrics. An examination is conducted on the context basis by Rathgab and uhl [19] for creating keys from binary biometric template. They used IRIS Biometric vectors which are especially distinguished with the fuzzy logic availed from the biometric data.

Optionally, a secure and more realistic approach is proposed by Hao et. al., [20] to indigenously present cryptographic applications. Here they implemented Bi-layered error correction method which is duly merged with Reed Solomon and Hadamard codes. From this, a key is generated from the image of IRIS with minutia error corrections. These corrections are redefined through image vectors and finally saved within the smart card. This approach gave better reliability with a success ratio of about 99.5%. Now, this is aimed to produce about 140 bits biometric key which is more suitable for 128 bit AES. Usage of AES also facilitates better enhancements in biometrics.

Yazhuo Gorg et. al., [21] featured a pseudo random number key generate approach to produce cryptographic keys. This also termed as PKI key generation method. This methodology is more suitable to produce appropriate PKI keys with lengthy and supplementary bits. The biometric system also suffered from non-revocability. To handle the problem, connie et. al., [22], stepped forward with a method called palm hashing. In this method, all the templates of palm prints are definitely hashed with a group of pseudo code keys to obtain a new palm hash.

Ross et. al., during 2007 gave the proposal for several stages of information formation with respect to the original finger print. They claimed that the stages of information are included from the minutiae of templates. The levels can be categorized as the class of information, the orientation field and the friction ridge structure. The localized ridge orientation is formed with the template of the minutiae. The formed template is used to analyze the original template's class[23].

Capelli et. al., during 2007 described their proposal in reconstructing the existing finger print images with the standards of ISO templates. Gabor filters played vital role in their approach to generate master finger print. They carried out the experiment with nine various systems and generated successful ratio of 81% with accurate precision security levels, [24]. Monrose et. al., [25] developed a methodology based on password strengthening with the key stroke biometrics. His approach revealed less security since, many of the entropy attributes are associateed to the passwords. The method cumulatively extracted the binary bits from the typing patterns which are duly clubbed with passwords. This limitation is very severe and thus proved unsuccessful. To strengthen the approach, again in 2001, Monrose et. al., improved the methodology with supplement stuff on the basis of voice biometrics.

The protection of biometric templates is an important aspect in the technological era. Hence, shielding functions are developed by Linnartz and Tuyls in 2003 [26]. For this protection system, the researchers dedicatedly made use of epsilon revealing functions and delta- contraction techniques to process the biometric finger prints and images obtained from the individual. These functions are very essential in estimating and computing the originality of the data from the databases.

Dodis et. al., [27] used fuzzy logic method to extract biometric data and to generate cryptographic keys. The primitives used by them are advanced. A secure sketch and fuzzy extractor primitives are deployed to recover the shared secret keys in the biometrics. This method is very stable in tolerating an error. The same approach and methodology is given as trial for 3D face and finger prints which produced the satisfactory remark.

Vetro et. al., (2009) and Draper et. al., (2007) [28,29] explained distributing the source code and gave protection for biometric template using finger print and iris. The variations existing in the finger print minutiae like deletions, insertions and other movements have overcome with a statistical model. The extracts of binary feature vectors and templates from minutiae are safely secured with the help of LDPC code. However, this method generated more complex computational approach for performance. Hence, a pre-alignment of fingerprint requisite is essential to overcome the complex issues for performance calculations.

The approach of Sundan and Juels (2002) [30] became very popular in the mile stones of the technological era. Their scheme encodes the complete secret keys in the form of the coefficients of a polynomial. This enhanced the additional security to the biometrics. The encoded secret keys are either unlocked or unlocked only the features of the biometrics. Since, this approach is proved to the robust one, and applied to the fingerprints. A multi model fuzzy vaults on the basis of iris and finger prints by Jain and Nanda kumar (2008) [31], voice and finger print by camlikaya et. al., (2008), and many multiple finger prints by kholmatov-Yanikoglu (2004) [32] are extensively proposed. After the proposals, in 2008, kholmatov and yanikoglu drastically observed and estimated the probable vulnerability by the fuzzy vault scheme in the biometrics. They claimed that the decoding and encoding secrets of the biometrics can be easily breakable with the minutiae positions in the biometrics. However, many of the scientific reasons challenged to overcome this limitation. In this connection Verbauwhede and Yang in 2005, proposed a fantastic methodology in determining the reference point of the minutiae of the finger prints. Under this, a minutiae under the polar coordinates is specifically locked or unlocked in the fuzzy logic scheme. This added additional security to the fuzzy vault scheme. During 2006, Jain and Uldag[33], proposed the alignment and friction ridge orientation schemes. Their enhancements are carried by Cheng et. al., with an automatic finger print alignment using geometric hash tables. On the other hand, Nagar et. al., (2008) and Li et. al., (2009) brought advancements in the fuzzy vault scheme to provide additional security to biometric systems.

Many several approaches have been developed for multimodal biometric system with various modalities. M. Nagesh et. al., [34] introduced an authentication system using both the palm print andface. The evolutions were made by using fusion score and matching issues. Jain and Ross [35] used linear dimensional classifiers and decision tree for merging of fusion scores duly obtained for biometric systems on hand geometry, finger print and face modalities. T.Wang et. al [38] also created a multi model biometric system on iris and face using the fusion scores and involving weighted and unweighted sum rules. This gained an accuracy level of about 96.6%. AsimBAig et. al., [36] also developed a multimodel biometric system which is purely based on hamming distance vector. The hamming distance vector method for the multimodal biometric has gained a precision of ERR 2.66%. Reddy.Srinivas [37] also defined a multimodal biometric system which purely secures the templates using password hardened fuzzy vault. Many research investigations are still under survey to carry out the FAR and FRR to bring down to zero, so as to increase the security levels for the rapidly increasing attention for biometric systems[9].

Jain and Rose introduced the approach for the multimodal biometric system [39]. The multimodalities have also been presented[40,41,42,49] with various fusion strategies. Finger prints and iris fusion strategies have greatly attracted the generosity of the researchers in literature [43,44,45,46,47]. Baig et. al., during 2009 raised a frame work with the usage of single match implementation for both the finger print and the iris. Their experimental setup has been conducted with west Virginia university database containing 400 images with an EER (equal error rate) set to threshold levels. Jameerbasha et. al., during 2011 developed an approach with merging of logistic regression method, highest rank method and Borda count method for development of multimodal biometric system. Their approach generated highest yielding in terms of execution time to match with optimal FRR and FAR. Their result set produced 0.25% FRR and 0% FAR. The matching scores obtained from the modalities of both the IRIS and FINGER prints are referred as MS Iris and MS Finger. These matching scores are obtained by using the min-max rule. The normalization technique drags both Iris and Finger matching scores between 0 and 1[23]. There are many normalization techniques, to name a few- Tan H, Z score and sigmoid resulted best output. The result of Tan H proved better with many parameters involved in the algorithm. Min-Max and Z score algorithms are very insensitive to the occurrence of outliers [17] but easy to implement.

A multi model biometric system in 2013 was introduced by Abdolahi et. al., used the weighted code and fuzzy logic vault. He used the conversion of the iris and finger print images in to binary codes. After combining the images, the decision level fusion is inherited to merge the results. This approach finally weighted 20% for finger print code and 80% weight for iris code. The total work gained an achievement of FAR with 2% and 98.3% of FRR in terms of accuracy.

Multimodal biometrics as shown in the above figure reveals the functional approach of the multiple traits of biometrics (Iris, finger prints, palm etc). The enhancements can be enraged with the above architecture to far extent. The depicted figure may be useful to simplify the inner contexts of multimodal biometric system.

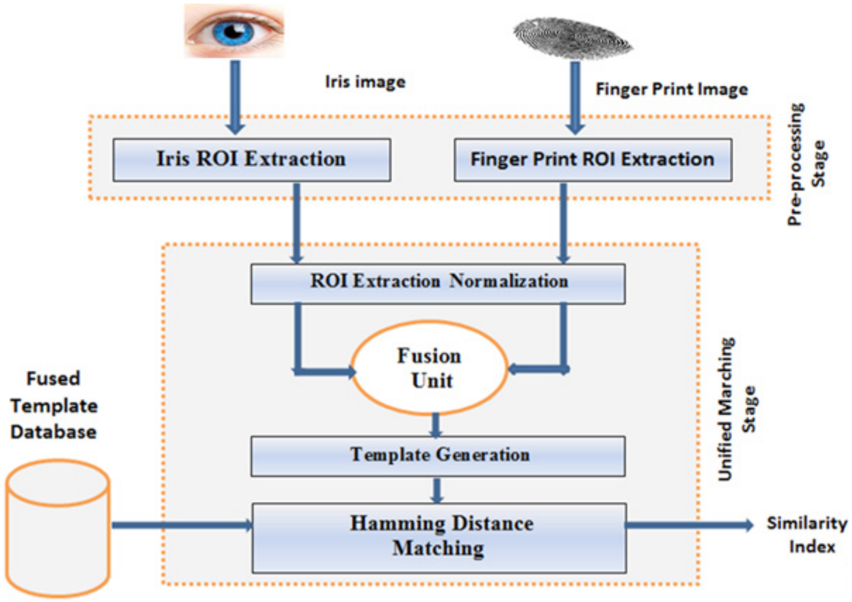


Figure 4: Functional approach of the multiple traits of biometrics

4. CESSATION

Security is a major concern in this vast world of digital authentication and authorization. The traditional approach uses the technique of user ids and passwords. As technology is advancing, this approach is damped with the rise of latest methodologies in authentication, authorization and security systems. The passwords are easily breakable with the breaking algorithms over online. Hence, biometric system as a standalone technique with unique processing system as id and password is useful. But the limitation is that if once the biometric image is stolen, the same image is applicable to many numbers of applications and can be accessed without the notice of original authorized personnel. Hence, it is preferred to go with multimodal biometric to enrich the security aspects. Multimodal approach enriches and strengthens the security essentials as part of online threats. . It is also very precise that unimodal biometrics alone cannot with stand for all the security circumstances with huge collection of data in the storage databases.

5. FUTURE DIRECTIONS

On behalf of this survey, it is withdrawn that multimodal biometrics are most vital at present generation to safeguard the user identification and authorization. It is clearly understood to enhance adaptive methods to safeguard the primitive data. Many protective algorithms with advanced detective systems must be designed and implemented so as to supplement succesive protection to information sources.

REFERENCES

[1] S. Pankanti, S. Prabhakar, and A. K. Jain, “On the Individuality of Fingerprints,” IEEE Transactions on PAMI, Vol. Vol. 24,, pp. 1010-1025, 2002.

[2] A. K. Jain and D. Maltoni, Handbook of Fingerprint Recognition: Springer-Verlag New York, Inc., 2003.

[3] A. K. Jain, R. Bolle, and S. Pankanti, Biometrics: Personal Identification in Networked Society: Kluwer Academic Publishers, 1998.

[4] D. D. Zhang, Automated Biometrics: Technologies and Systems: Kluwer Academic Publishers, 2000.

[5] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric cryptosystems: issues and challenges," Proceedings of the IEEE, Vol. 92, pp. 948-960, 2004.

[6] A. C. Leniski, R. C. Skinner, S. F. McGann, and S. J. Elliott, "Securing the biometric model," presented at Security Technology.Proceedings of the 37th IEEE Annual 2003 International Carnahan Conference, 2003.

[7] B. Scheneier, Applied Cryptography, 2nd ed: John Wiley & Sons, New York, 1996.

[8] P. Reid, Biometrics and Network Security: Prentice Hall PTR, 2003.

[9] A. J. Menezes, S. A. Vanstone, and P. C. V. Oorschot, *Handbook of Applied Cryptography*: CRC Press, Inc., 1996.

[10] F. Yang and B. Ma, "A new mixed-mode biometrics information fusion based-on fingerprint, hand-geometry and palm-print," in Proc. 4th Int. IEEE Conf. Image Graph., 2007, pp. 689–693. DOI:10.1109/ICIG.2007.39.

[11] N. K. Ratha, R. M. Bolle, V. D. Pandit, and V. Vaish, "Robust fingerprint authentication using local structural similarity," in Proc. 5thIEEE Workshop Appl. Comput. Vis., Dec. 4–6, 2000, pp. 29–34. DOI: 10.1109/WACV.2000.895399.

[12] Y. Zhu, T. Tan, and Y. Wang, "Biometric personal identification on iris patterns," in Proc. 15th Int. Conf. Pattern Recogn., 2000, Vol. 2, pp. 805–808.

[13] L. Ma,Y.Wang, andD. Zhang, "Efficient iris recognition by characterizing key local variations," *IEEE Trans. Image Process.*, Vol. 13, No. 6, pp. 739–750, Jun. 2004.

[14] V. Conti, G. Milici, P. Ribino, S. Vitabile, and F. Sorbello, "Fuzzy fusion in multimodal biometric systems," in Proc. 11th LNAI Int. Conf. Knowl.- Based Intell. Inf. Eng. Syst. (KES 2007/WIRN 2007), Part I LNAI 4692. B. Apolloni et. al., Eds. Berlin, Germany: Springer-Verlag, 2010, pp. 108–115.\

[15] F. Besbes, H. Trichili, and B. Solaiman, "Multimodal biometric system based on fingerprint identification and Iris recognition," in Proc. 3rd Int. IEEE Conf. Inf. Commun. Technol.: From Theory to Applications (ICTTA 2008), pp. 1–5. DOI: 10.1109/ICTTA.2008.4530129.

[16] G. Aguilar, G. Sanchez, K. Toscano, M. Nakano, and H. Perez, "Multimodal biometric system using fingerprint," in Proc. Int. Conf. Intell. Adv. Syst. 2007, pp. 145–150. DOI: 10.1109/ICIAS.2007.4658364.

[17] V. C. Subbarayudu and M. V. N. K. Prasad, "Multimodal biometric system," in Proc. 1st Int. IEEE Conf. Emerging Trends Eng. Technol., 2008, pp. 635–640. DOI 10.1109/ICETET.2008.93.

[18] Lifang Wu, Xingsheng Liu, Songlong Yuan and Peng Xiao, "A novel key generation cryptosystem based on face features", IEEE 10th International Conference on Signal Processing (ICSP), pp. 1675 – 1678, 2010.

[19] C. Rathgeb and A. Uhl, "Context-based biometric key generation for Iris", IET Computer Vision, Vol. 5, No. 6, pp. 389 – 397, 2011.

[20] F. Hao, R. Anderson and J. Daugman, "Combining crypto with biometrics effectively", IEEE Transactions on Computers, Vol. 55, pp. 1081-1088,2006.

[21] Yazhuo Gong, Kaifa Deng and Pengfei Shi, "PKI Key Generation Based on Iris Features", International Conference on Computer Science and Software Engineering, Vol. 6, pp. 166 – 169, 2008.

[22] T. Connie, A. Teoh, M. Goh and D. Ngo, "Palm hashing: A novel approach for cancellable biometrics", Information processing letters, Vol. 93, No. 1, pp. 1-5, 2005.

[23] Ross A, Shah J, Jain AK. From template to image: reconstructing fingerprints from minutiae points. IEEE Transactions on Pattern Analysis and Machine Intelligence, Special Issue on Biometrics 2007;29(4):544–60.

[24] Cappelli R, Lumini A, Maio D, Maltoni D. Fingerprint image reconstruction from standard templates. IEEE Transactions on Pattern Analysis and Machine Intelligence 2007;29(9):1489–503.

[25] Monrose F, Reiter MK, Wetzel S. Password hardening based on keystroke dynamics. In: Proceedings of the sixth ACM conference computer and communication security, 1999. p. 73–82.

[26] Linnartz J-P, Tuyls P. New shielding functions to enhance privacy and prevent misuse of biometric templates, audio-and video-based biometrie person authentication. In: Fourth international conference, AVBPA 2003, Guildford, UK, June 2003.

[27] Dodis Y, Ostrovsky R, Reyzin L, Smith A. Fuzzy extractors: how to generate strong keys from biometrics and other noisy data. SIAM Journal of Computing 2004;38(1):97–139.

[28] Vetro A, Draper S, Rane S, Yedidia J. securing biometric data. Technical report, TR2009-002, Mitsubishi Electric Research Laboratories (MERL), 2009.

[29] Draper SC, Khisti A, Martinian E, Vetro A, Yedidia JS. Using distributed source coding to secure fingerprint biometrics. In: IEEE international conference on acoustics, speech and signal processing (ICASSP2007), Vol. 2, April 2007. p. II.129–32.\

[30] Juels A, Sundan M. A fuzzy vault scheme. In: Proceedings of the IEEE internation symposium on information theory, Lausanne, Switzerland, 2002. 408 pp.

[31] Nandakumar K, Jain AK. Multibiometric template security using fuzzy vault, biometrics: theory, applications and systems (BTAS08), Crystal City, Septem- ber 29–October 1, 2008.

[32] Yanikoglu B, Kholmatov A. Combining multiple biometrics to protect privacy. In: Proceedings of the ICPR workshop on biometrics: challenges arising from theory to practice, Cambridge, UK, August 2004.

[33] Uludag U, Jain AK. Securing fingerprint template: fuzzy vault with helper data. In: Proceedings of the IEEE workshop on privacy research in vision, June 22, 2006. p. 163–70.

[34] Nageshkumar.M, Mahesh.PK and M.N. Shanmukha Swamy, "An Efficient Secure Multimodal Biometric Fusion Using Palmprint and Face Image", IJCSI International Journal of Computer Science Issues, Vol. 2, 2009.

[35] A. Ross and A. K. Jain, "Information Fusion in Biometrics" Pattern Recognition Letters, Special Issue on Multimodal Biometrics, 24(13):2115–2125, 2003.

[36] Asim Baig, Ahmed Bouridane, Fatih Kurugollu, and Gang Qu, "Fingerprint – Iris Fusion based Identification System using a Single Hamming Distance Matcher", International Journal of Bio-Science and Bio- Technology, Vol. 1, No. 1, December, 2009.

[37] E. Srinivasa Reddy, I. Ramesh Babu, "Performance of Iris Based Hard Fuzzy Vault", Proceedings of IEEE 8th International conference on computers and Information technology workshops, 2008.

[38] T. Wang, T. Tan, and A.K. Jain, "Combining face and iris iris biometrics for identity verification," in Proc. 4th Int. Conf. Audio-Video-Based Biometric Person Authentication, J. Kittler and M. Nixon, Eds., 2003, Vol. LNCS 2688, pp. 805–813.

[39] A. Ross and A. Jain, "Information fusion in biometrics," Pattern Recognition Letters, Vol. 24, No. 13, pp. 2115–2125, 2003.

[40] J. Zhou, G. Su, C. Jiang, Y. Deng, and C. Li, "A face and fingerprint identity authentication system based on multi-route detection," Neurocomputing, Vol. 70, No. 4–6, pp. 922–931, 2007.

[41] H. Ailisto, E. Vildjiounaite, M. Lindholm, S.-M. M¨akel¨a, and J. Peltola, "Soft biometrics-combining body weight and fat measurements with fingerprint biometrics," Pattern Recognition Letters, Vol. 27, No. 5, pp. 325–334, 2006.

[42] J. Yang and X. Zhang, "Feature-level fusion of fingerprint and finger-vein for personal identification," Pattern Recognition Letters, Vol. 33, No. 5, pp. 623–628, 2012.

[43] M. Abdolahi, M. Mohamadi, and M. Jafari, "Multimodal biometric system fusion using fingerprint and iris with fuzzy logic," International Journal of Soft Computing and Engineering, Vol. 2, No. 6, pp. 504–510, 2013.

[44] A. Baig, A. Bouridane, F. Kurugollu, and G. Qu, "Fingerprint—iris fusion based identification system using a single hamming distance matcher," International Journal of Bio-Science and Bio-Technology, Vol. 1, No. 1, pp. 47–58, 2009.

[45] A. Jagadeesan, T. Thillaikkarasi, and K. Duraiswamy, "Cryptographic key generation from multiple biometric modalities: fusing minutiae with iris feature," International Journal of Computer Applications, Vol. 2, No. 6, pp. 16–26, 2010.

[46] A. JameerBasha, V. Palanisamy, and T. Purusothaman, "Efficient multimodal biometric authentication using fast fingerprint verification and enhanced iris features," Journal of Computer Science, Vol. 7, No. 5, pp. 698–706, 2011.

[47] N. Radha and A. Kavitha, "Rank level fusion using fingerprint and iris biometrics," Indian Journal of Computer Science and Engineering, Vol. 2, No. 6, pp. 917–923, 2012.

[48] S.J. Xie, J. Yang, D.S. Park, S. Yoon, and J. Shin, "State of the art in biometrics," in Iris Biometric Cryptosystems, J. Yang and L. Nanni, Eds., InTech, 2011.

[49] A.K. Jain and A. Ross, "Multibiometric systems," Communications of the ACM, Vol. 47, No. 1, pp. 34–40, 2004.

[50] U. Gawande, S.R. Nair, H. Balani, N. Pawar, and M. Kotpalliwar, "A high speed frequency based multimodal biometric system using iris and fingerprint," International Journal on Advanced Computer Engineering and Communication Technology, Vol. 1, No. 2, pp. 66–73, 2012.