Securing system access using multi-model biometrics for authorization

***Sneha Kurhekar*[1], *Harshvardhan Upadhyay*[2]**

[1,2]Department of Electronics and Telecommunication Engineering, SRCOE, Pune, Maharashtra, India

Abstract

Today, the security requirements of society have placed biometrics at the center of a large debate as it is becoming a key aspect in a multitude of applications. Proposed system is the implementation of the embedded system for the online signature, finger print and key pattern verification. And providesecured authentication system. The work describes the complete biometric algorithm for enrollment phase and evaluation phase. In proposed system, android phone and finger print module R305 are used for data acquisition process. Subsequently, signature and fingerprint images are aligned by applying HMM and DTW algorithm respectively. Proposed system provide extra layer of security as both the characteristics of biometrics are used in it, as well knowledge factor and inherence factor of authentication are included. This work implements securing system access using multi-sensor biometrics for authorization.

Keywords: Biometrics, Embedded system, FPGA, Dynamic Time Wrapping and HMM model

I. INTRODUCTION

Biometric is related to the human characteristics and traits. Biometric authentication is the realistic authentication form of identification and access control. Multimodal biometric systems use more than one biometrics to overcome the limitations of unimodal biometric systems. As we know, from the beginning Fingerprint and signature play very vital role in the process of identification. Fingerprint and signature are needed in many places for personal identification. It is widelyused in the field of finance, access control and security. Today, the security requirements ofsociety have placed biometrics at the center of a large debate as it is becoming a key aspect ina multitude of applications [1]. There are many more other personal authentication techniques as well. Some of them uses the possession of the token (i.e ID cards) and some of them are knowledge based (i.e password, key-phase etc). But, the token based technique whose attributes can be stolen or lost whereas knowledge based approaches whose attributes can be forgotten, which become major drawback of such techniques. But the biometrics attributes, do not suffer from such disadvantages.

Biometrics identifiers are the measurable characteristics. It can be classified into two type's i.e 'Physiological and Behavioral'. The type which is based on the biological traits of user such as fingerprint, hand geometry, face etc is known as Physiological Biometrics and the trait which shows the pattern of behavior of a person such as, voice and signature are known as Behavioral Biometrics [2]. To the best of our knowledge, proposed biometric model gives the proper authentication with extra layer of security. In this proposed system, we are using both traits of biometrics physiological trait fingerprint and behavioral trait signature. So, we say proposed system is a multi-model biometric system. Toward these direction the contribution of these paper is three fold: First we are using signature (behavioral trait), secondly fingerprint(biological trait) and lastly key pattern. When all these three parameters matches then and only then user get authorized.This paper is organized as follows. Section II describes the basic theory of the multimodal biometric system. Section III presents the DTW and HMM algorithm. Section IV shows the experimental setup with result and finally Section V presents the conclusions.

II. MULTIMODEL BIOMETRIC SYSTEM

Fig. 1 shows the architecture adopted by proposed system which having generic architecture as a basic platform with some additional advantages features. As shown in Fig. 1 system having three inputs i.e signature, finger print and key pattern.

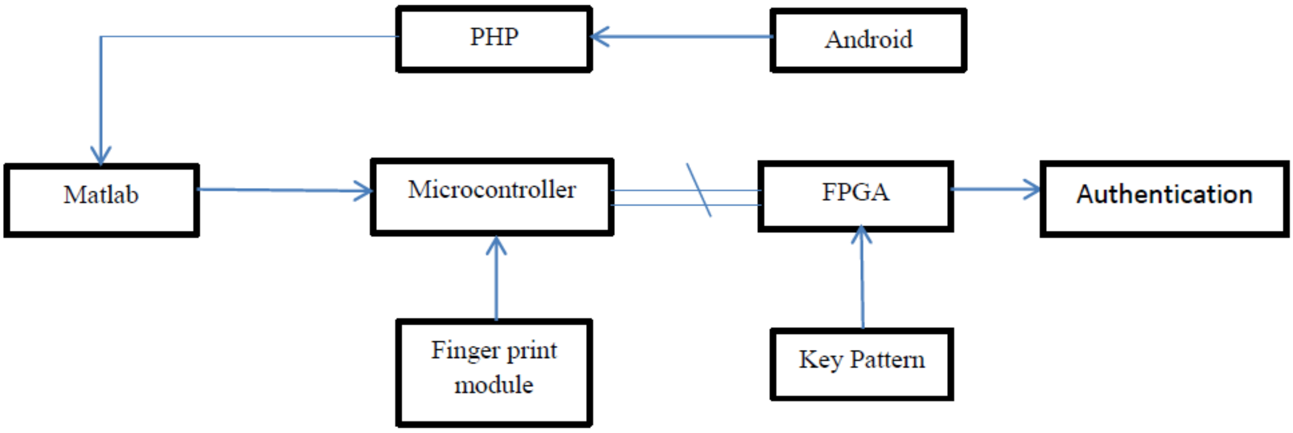


Fig. 1 Architecture of proposed Multimodal biometric system

Working of proposed system can be sub divided into following stages-

- Data Acquisition
- Image pre-processing
- Feature Extraction
- Classification

1. Data Acquisition- Data acquisition is the process of collecting input data from input devices. So signatures are collected using android mobile phone whereas finger prints are collected from the Finger Print Sensor R305.

2. Image pre-processing- Preprocessing stage is used to reduce the noise and normalized the images obtained from input devices. The preprocessing stage is enclosed by normalization, segmentation, filtering like processes. Binarization and thinning process are carried out over the finger print image in the preprocessing stage.

3. Feature Extraction - Feature extraction is the efficiency measure tool for the signature verification process. Proposed system, deals with the dynamic features and used function based features as signature is characterized in terms of time function. Dynamic features are extracted from signatures that are acquired in real time which make the signature more unique [5] [6].

In proposed system, we are going to deal with the some features like thinning of images, perimeter, area, orientation, eccentricity etc. Pattern of interleaved ridges and valleys lines can be described by a fingerprint image. Minutia is the unique feature of the ridges. Minutia points occur at ridges bifurcation. Bifurcation is the process where a ridge split into two lines at specific points. For the proposed system for that purpose we are using dynamic time wrapping technique. This technique aims to minimize the effects of distortion and time-shift between two signatures collected in different sessions.

4. Classification:

In verification process, authentication of signature, fingerprint and key pattern are done. In these, the features of signature and finger print and key pattern which stored in dada based during enrolment stage are matched with test signature, fingerprint and key pattern.K nearest neighbors(KNN) classifier used for the classification stage.

III. EXPERIMENTAL SETUP& IMPLEMENTATION

1. Pre saving of segmentation on android:In gesture builder library emulator save the gesture file. It provide extra layer of security.
2. User Registration:User draw the sign on the android phone it followed by fingerprint scan on the module R302. Both the input saves to the data base. Key pattern also generated by the user. All these three data are saved by user name on knowledge base.
3. User evaluation:As we know, authentication process consists of two phase, enrollment phase and verification phase. We finish enrollment phase through the user registration. Now whatever data we are needed for evaluation i.e signature, fingerprint and key pattern is already stored in data base. Here we compare previously stored user data with newly enrolled if all the parameters matches then we get the proper authentication result.

A.Signature process:

For thesignature, we are using android phone as a input. Wireless connection should be created between Android phone and Matlab. The gesture file which is created when user touches the screen and it gets stored in Matlab. Touch gesture occurs when a user places one or more fingers on the touch screen, and application interprets that pattern of touches as a particular gesture. The gesture starts when the user first touches the screen, continues as the system tracks the position of the user's finger(s), and ends by capturing the final event of the user's fingers leaving the screen. Android provides the Gesture Detector class for detecting common gestures.

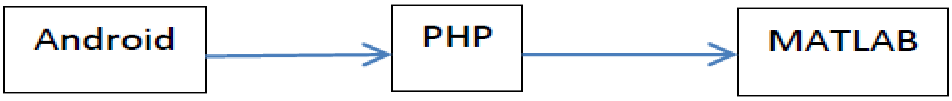


Fig. 2 Signature process

A Hidden Markov Modeling (HMM) is used with the signature process. HMM process consist of two processes, they are an underlying process and an observable process. So HMM is called as a doubly stochastic process. The process which is hidden from observation is known as an underlying process and the process which is determined by the underlying process is called as an observable process.Knn classifier is used for classification. K nearest neighbors is a simple algorithm that stores all available cases and classifies new cases based on a similarity measure. A case is classified by a majority vote of its neighbors, with the case being assigned to the class most commonamongst its K nearest neighbors measured by a distance function. If K = 1, then the case is simply assigned to the class of its nearest neighbor.

B. Fingerprint process:

For fingerprint in proposed system we are using finger print sensor module R305.This module is with TTL UART interface for direct connections to microcontroller UART or to PC through MAX232 / USB-Serial adapter. The user can store the finger print data in the module and can configure it in 1:1 or 1: N mode for identifying the person.

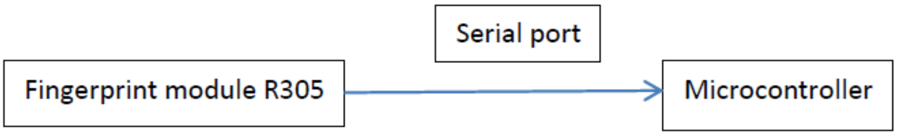


Fig3. Fingerprint process

Dynamic timing wrapping is implemented on fingerprint for the feature extraction. Dynamic time warping (DTW) is an algorithm for measuring similarity between two temporal sequences which may vary in time. DTW is a method that calculates an optimal match between two given sequences (e.g. time series).

- Two time series Q & C.

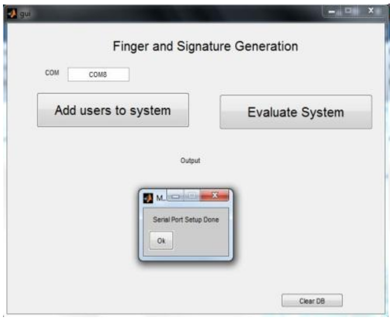
  $Q = q_1, q_2, \ldots\ldots\ldots\ldots q_n$

  $C = c_1, c_2, \ldots\ldots\ldots\ldots c_n$
- Construct m×n matrix D with distances $D_{ij} = d\ (q_i\ , c_j\ )$
- Warping path W is a contiguous set of matrix elements $W_k = (\ i, j\ )_k$
- Find : DTW (Q , C) = min $\sqrt{\sum Wk}$

IV. RESULT AND DISCUSSION

The complete embedded system works in two phases of authentication i.eenrollment phase and evaluation phase. In enrollment phase signature, fingerprint and user name are stored on database. In evaluation phase, system compares the user's signature, fingerprint and key pattern with previously stored one and according to that evaluation phase give its output. This system gives the correct authentication when all three parameters are correct. If system found that any among three is not matching with the previous one then we are not getting any authentication. System display the message "match not found".

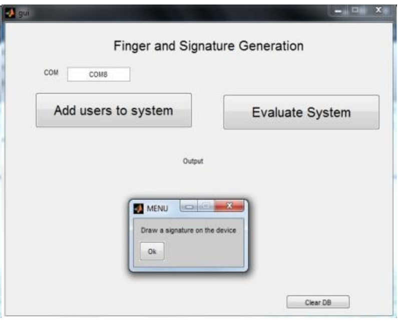
We can observe the evaluation phase and enrollment phase in following fig. As all setups are done, firstly our set up check whether serial port connections is done or not and it displays as shown in Fig.4.



COM COM8

Serial Port Setup Done

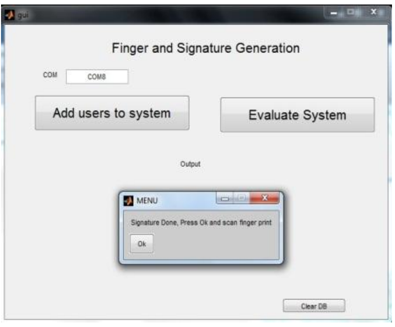
Fig. 4 Serial port connection



COM COM8

Draw a signature on the device

Fig. 5(a) Signature enrollment Fig.

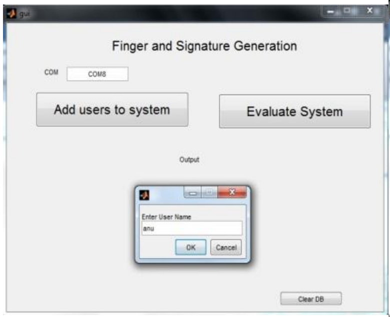


COM COM8

Signature Done, Press Ok and scan finger print

5(b) Fingerprint enrollment

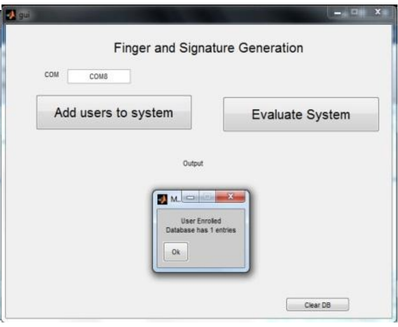
Fig. 5(a) and Fig. 5(b) shows enrollment phase, in which user must enroll signature and finger print respectively. Fig 5(c) shows how to user save his data by his name. Fig 5(d) shows the result of enrollment process. User information is stored in data base.



COM COM8

Enter User Name: anu

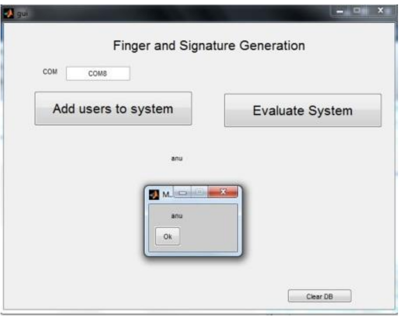
Fig 5(c) Enrollment of user name



COM COM8

User Enrolled
Database has 1 entries

Fig. 5(d) Enrollment phase result



COM COM8

anu

anu

Fig 6 Authentication's result

ISSN: 2278 – 7798

All Rights Reserved © 2016 IJSETR

In evaluation phase, classification is carried out between previously stored information with present one. Same steps are carried out for evaluation phase, same as shown in Fig. 5(a) and Fig. 5(b) and key pattern also must be entered. Finally authentication is displayed as shown in Fig. 6.In following table we tabularized the result.

User	Actual sign	Actual fingerprint	System detected
User 1	User 1	User 1	User 1
User 2	User 2	User 2	User 2
User 3	User 3	User 3	User 3
User 4	User 4	User 3	Match not found
User 5	User 4	User 5	Match not found
User 6	User 6	User 6	User 6
User 7	User 2	User 3	Match not found
User 8	User 8	User 8	User 8

Table 1: Result tabulation

CONCLUSION

This paper analyzes the implementation of the embedded system for the online signature, finger print and key pattern verification. And provide the biometric system for authentication with the extra layer of security. These paper implement such a biometric system which consist of ‘Physiological trait(fingerprint) as well Behavioral trait (signature) of biometrics. The complete embedded system works in two phases of authentication i.e enrollment phase and evaluation phase. In enrollment phase signature, fingerprint and user name are stored on database. In evaluation phase, system compares the user signature, fingerprint and key pattern with previously stored one. Thus it proposed a real time authentication framework for authentication.

ACKNOWLEDGEMENT

First and foremost I would like to express my deepest gratitude to my guide respected **Prof. H. Upadhyay**for his valuable support, guidance, motivation and encouragement throughout the period this work was carried out. I wish to express my gratitude to **Prof. SujathaRao**(HOD) for her valuable guidance, motivations and helpful attitude.

REFERENCES

[1] Anil Jain, Arun Ross and SalilPrabhakar, “Introduction to Biometric Recognition”, IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, No. 1, pp. 4-20,January 2004.

[2] D. Impedovo and G. Pirlo, “Automatic signature verification: The state of the art,” IEEE Trans. Syst., Man, Cybern.—Part C: Appl. Rev., vol. 38, no. 5, pp. 609–635, Sep. 2008.

[3] M. Fons, F. Fons, and E. Cantó-Navarro, “Fingerprint image processing acceleration through run-time reconfiguration hardware,” IEEE Trans. Circuits Syst. II: Exp. Briefs, vol. 57, no. 12, pp. 991–995, Dec. 2010.

[4] Gruber C, Gruber T, Krinninger S, Sick B, “Online Signature Verification With Support Vector Machines Based on LCSS Kernel Functions”, IEEE transaction on System, Man, and Cybematics, Part B: Cybemetics, Vol. 40, PP. 1088 – 1100, June 2010.

[5] Enrique ArgonesRúa,,José Luis Alba Castro, *M “*Online Signature Verification Based on Generative Models”,IEEE Transactions on Systems, Man, and Cybernetics—Part B: Cybernetics, Vol. 42, No. 4, pp 1231 - 1242 August 2012.

[6] Mariano lópez-garcía, Rafael ramos-lara, Oscar miguel-hurtado, and Enrique cantó-navarro, “Embedded system for biometric online signature verification”, IEEE Transactions on Industrial Informatics, Vol. 10, No. 1, PP 491 – 501 February 2014.

[7] Miguel A. Ferrer, J. Francisco Vargas, Aythami Morales, and AarónOrdóñez, ―Robustness of Offline Signature Verification Based on Gray Level Features‖. IEEE Transactions on Information Forensics and Security, Vol. 7, No. 3, June 2012.

[8] M. Fons, F. Fons, E. Cantó-Navarro, and M. López-García, "FPGA based personal authentication using fingerprints," *J. Signal Process.Syst.*, vol. 66, no. 2, pp. 153–189, Feb. 2012.

[9] O. Miguel-Hurtado, L. Mengibar-Pozo, and A. Pacut, "A new algorithm for signature verification system based on DTW and GMM," in *Proc. 42nd. Annu. IEEE Int. Carnahan Conf. Security Technol.*, Oct. 2008, pp. 206–213.

[10] B. Ly Van, S. Garcia-Salicetti, and B. Dorizzi, "On using the Viterby path along with HMM likelihood information for online signature verification," IEEE Trans. Syst., Man, Cybern. Part B: Cybern., vol. 37, no. 5, pp. 1237–1247, Oct. 2007.

[11] J. Fierrez-Aguilar, J. Ortega-García, D. D. Ramos, and J. Gonzalez-Rodríguez, "HMM-based on-line signature verification: Feature extraction and signature modeling," Pattern Recognit. Lett., vol. 28, no. 16, pp. 2325–2334, Dec. 2007.

[12] Eric Monmasson , MarcianCirstea, "Guest Editorial Special Section on Industrial Control Applications of FPGAs" IEEE Transactions on Industrial Informatics, Vol. 9, No. 3, pp 1250-1252, August 2013.

[13] S. Jin, D. Kim, T. T. Nguyen, D. Kim,M. Kim, and J. W. Jeon, "Design and implementation of a pipelined datapath for high-speed face detection using FPGA," IEEE Trans. Ind. Inf., vol. 8, no. 1, pp. 158–167, Feb. 2012.

[14] E. Monmasson, L. Idkhajine, M. N. Cirstea, I. Bahri, A. Tisan, and M. W. Naouar, "FPGAs in industrial control applications," IEEE Trans.Ind. Inf., vol. 7, no. 2, pp. 224–243, May 2011.

[15] Y. Komiya, T. Ohishi, and T. Matsumoto, "A pen input on line signature verifier integrating position, pressure and inclination trajectories," IEICE Trans. Inf. Syst., vol. E84 D, no. 7, pp. 833–838, Jul. 2010.

[16] S. Impedovo and G. Pirlo, "Verification of handwritten signatures: An overview," in *Proc. 14th Int. Conf. Image Anal. Process.*, Sep. 2007,pp. 191–196.

[17] T. Ahonen, A. Hadid, and M. Pietikainen, ―Face description with local binary patterns: Application to face recognition, IEEE Trans. Pattern Anal. Machine Intell., vol. 28, no. 12, pp. 2037–2041, Dec. 2006.

[18] H. Ketabdar, J. Richiardi, and A. Drygajlo, "Global feature selection for on-line signature verification," in Proc. 12th IGS Conf., Salerno, Italy, Jun. 2005, pp. 59–63

[19] J. Richiardi, H. Ketabdar, and A. Drygajlo, "Local and global feature selection for on-line signature verification," in Proc. IAPR 8th ICDAR, Seoul, Korea, Aug. 2005, vol. 2, pp. 625–629.

[20] J. Fiérrez Aguilar, L. Nanni, J. López-Pe´nalba, J. Ortega García, and D. Maltoni, "An on-line signature verification system based on fusion of local and global information," in Proc. IEEE Int. Conf. Audio Video-BasedPerson Authentication, Halmstad, Sweden, Jun. 2005, pp. 523–532.

[21] J. Y. Kim, D. Y. Ko, and S. Y. Na, "Implementation and enhancement of GMM face recognition systems using flatness measure," in Proc.IEEE Int. Workshop Robot Human Interact. Commun., Sep. 2004, pp. 247–251.

[22] J. J. Igarza, L. Gómez, I. Hernáez, and I. Goirizelaia, Searching for an Optimal Reference System for On-Line Signature Verification Based on (x, y) Alignment, D. Zhang and A. K. Jain, Eds. Berlin, Germany:Springer-Verlag, 2004, pp. 519–525, ICBA 2004, LNCS 3072.

[23] G. Dimauro, S. Impedovo, M. G. Lucchese, R. Modugno, and G. Pirlo, "Recent advancements in automatic signature verification," in Proc. 9th Int. Workshop Frontier Handwriting Recognit., Oct. 2004, pp. 179–184, IEEE Comput. Society Press.

[24] B. Fang, C. H. Leung, Y. Y. Tang,K.W. Tse, P.C.K.Kwok, andY.K. Wong, "Off-line signature verification by tracking of feature and stroke positions," IEEE Trans. On Pattern Recognit., vol. 36, no. 1, pp. 91–101, Jan. 2003.

[25] B. Bhanu, X. Tan, “Fingerprint indexing based on novel features of minutiae triplets”, IEEE Trans. Pattern Recog. Anal. Mach. Intell. 25(5) (2003) 616–622.

[26] M. Diligenti, P. Frasconi, and M. Gori. Hidden tree markov models for document image classification. IEEE Transactions on Pattern Analysis and Machine Intelligence, 25(4):519–523, 2003.

[27] A. K. Jain, F. D. Griess, and S. D. Connell, “On-line signature verification,” Pattern Recognit., vol. 35, no. 12, pp. 2963–2972, 2002.

[28] Y. Komiya, T. Ohishi, and T. Matsumoto, “A pen input on line signature verifier integrating position, pressure and inclination trajectories,” *IEICE Trans. Inf. Syst.*, vol. E84 D, no. 7, pp. 833–838, Jul. 2001.

[29] N. K. Ratha, A. W. Senior, and R. M. Bolle, “Automated biometrics,” in Proc. 2nd Int. Conf. Adv. Pattern Recog., Rio de Janeiro, Brazil, Mar. 2001, pp. 445–474

[30] J. Li, A. Najmi, and R. Gray. “Image classification by a two dimensional hidden markov model”. IEEE Transactions on Signal Processing, 48(2):517–533, 2000.

[31] D. Impedovo and G. Pirlo, “On-line signature verification by stroke-dependent representation domains,” in Proc. 12th ICFHR, Kolkata, India, Nov. 2010, pp. 623–627, 16–18.

[32] R. Bajaj and S. Chaudhury, “Signature verification using multiple neural classifiers,” Pattern Recognit., vol. 30, no. 1, pp. 1–7, Jan. 1997

[33] R. Kashi, J. Hu, W. L. Nelson, and W. Turin, “On-line handwritten signature verification using hidden Markov model features,” in Proc. 4th Int.Conf. Doc. Anal. Recog., Ulm, Germany, Aug. 1997, pp. 253–257.

[34] L. L. Lee, T. Berger, and E. Aviczer, “Reliable on-line human signature verification systems,” IEEE Trans. Pattern Anal. Mach. Intell., vol. 18, no. 6, pp. 643–647, Jun. 1996.

[35] S. Nabeshima, S. Yamamoto, K. Agusa, and T. Taguchi, “MEMOPEN: A new input device,” in Proc. Int. Conf. Companion Human FactorsComput. Syst. (CHI’95), 1995, pp. 256–257.

[36] G. Pirlo, “Algorithms for Signature Verification,” in Proc. NATO-ASI Series Fund. Handwriting Recognit., S. Impedovo, Ed., Berlin, Germany,1994, pp. 433–454, Springer-Verlag.

[37] O. Miguel-Hurtado, L. Mengibar-Pozo, and A. Pacut, “A new algorithm for signature verification system based on DTW and GMM,” in Proc. 42nd. Annu. IEEE Int. Carnahan Conf. Security Technol., Oct. 2008, pp. 206–213.

[38] R. Ramos-Lara, M. López-García, E. Cantó-Navarro, and L. Puente- Rodriguez, “Real-Time speaker verification system implemented on reconfigurable hardware,” J. Signal Process. Syst., vol. 71, no. 2, pp.89–103, May 2013.

[39]] M. López-García, J. Daugman, and E. Cantó-Navarro, “Hardware-software co-design of an iris recognition algorithm,” IET Inf. Security, vol. 5, no. 1, pp. 60–68, Apr. 2011.

[40] J. Liu-Jiménez, R. Sánchez-Reillo, L. Mengibar-Pozo, and O. Miguel Hurtado, “Optimisation of biometric ID tokens by using hardware/software co-design,” IET Biometrics, vol. 1, no. 3, pp. 168–177, Sep. 2012.

[41] Y. Sato and K. Kogure, “Online signature verification based on shape, motion, and writing pressure,” in IEEE Proc. 6th Int. Conf. PatternRecognit., 1982, pp. 823–826.

[42] H. Sakoe and S. Chiba, “Dynamic programming algorithm optimization for spoken word recognition,” IEEE Trans. Acoust. Speech, SignalProcess., vol. 26, no. 1, pp. 43–49, Feb. 1978.

[43] M. Erbilek and M. Fairhurst, “Framework for managing ageing effects in signature biometrics,” IET Biometr., vol. 1, no. 2, pp. 136–147, Jun. 2012

[44] J. Ortega-García, J. Fierrez-Aguilar, D. Simon, J. Gonzalez, M. Faundez-Zanuy, V. Espinosa, A. Satue, I. Hernaez, J. J. Igarza, C. Vivaracho, D. Escudero, and Q. Moro, “MCyT baseline corpus: A bimodal biometric database,” IEE Proc.—Vision, Image, SignalProcess., vol. 150, no. 6, pp. 395–401, Dec. 2003.