IJCSC Volume 5 • Number 1 March-Sep 2014 pp. 181-187 ISSN-0973-7391

An Improved Approach to Multibiometrics Security

Gursimarpreet Kaur, Arun Kumar Yadav, Dr. Sheetal Chaudhary
Department of computer science and applications, kurukshetra university kurukshetra
gursimarpreet8029@gmail.com, arunkumar9429@gmail.com, sheetalkuk@rediffmail.com

Abstract: Unimodal systems use one biometric trait for authentication. Though unimodal systems enjoy the advantage of simplicity, yet there are some problems with these systems. To address these problems, multimodal systems are used, which combines the evidences of multiple traits. It will make the system more reliable and robust and thus increases the security of the biometric system. In this paper a novel approach of multimodal system is proposed, which uses fingerprints, hand geometry and palm print. Feature level fusion is used to combine the data obtained from these traits. The proposed system is also combined with cancellable biometrics. Using cancellable functions will further improve the performance of system. Also these three traits are extracted using single sensor i.e. 3 in 1 sensor so it reduces hardware cost and time. Thus the proposed framework has better performance than earlier approaches.

Keywords: Multimodal, cancellable, fusion, non-invertible.

I. INTRODUCTION

Biometrics is the science and technology of recognizing individuals based on physiological, behavioral or morphological characteristics. It includes fingerprint, face, gait, iris, hand geometry, signature etc. Biometrics systems can be divided into two types: Unimodal and multimodal systems. In Unimodal biometric systems, recognition is performed based on a single source of biometric information. Advantages of using Unimodal systems are that these are simple to use and of low cost. But unimodal suffers from many problems like noisy sensor data, susceptibility to circumvention, non-universality and lack of uniqueness, intra class variations and distortion from environment [1] [2].To abolish these problems a system called multimodal biometric system is gaining attention. Multimodal systems use input data from two or more traits in combined fashion in the authentication process. Multimodal system upgrades the performance but it is also not free from limitations. These includes increased storage requirement, more cost, processing time is increased which causes user inconvenience, increased resource requirement for computation etc. The information obtained from multiple sources has to combine in some way, the process is known as fusion. Fusion can be done at various levels of biometric system. To boost the security of stored template cancellable biometrics is used. In this approach a non invertible transformation is applied on the actual template and this transformed template is stored in the database. These functions can be cancelled and again applied if data is compromised.

The rest of the paper is organized as follows: related work is given in section II, fusion techniques are explained in section III, idea of cancellable biometrics is given in section IV, proposed framework is presented in section V,step by step algorithm for enrollment and authentication phase in section VI, conclusions in section VII and finally references are given.

II.RELATED WORK

Techniques have been proposed which combines the fingerprint and palmprint data. Firstly quality is enhanced using many preprocessing techniques. 2D Gabor filters is used to independently extract feature set of fingerprint and palmprint. EER (equal error rate) is highly improved using this technique [20]. Palmprint and hand geometry is also combined to achieve mutibiometric systems. Data from both traits are taken using single sensor i.e. digital camera. Each of these gray level images is aligned and then features are extracted from these. Acquisition process need not require special illumination so is very simple. Sample from 100 users is examined [21]. Three biometric traits i.e. fingerprint, hand geometry and palmprint have also been combined. Single sensor takes all three images so enrollment time is reduced. These features are fused on feature level and match score level. The database was tested on 98 persons and the system works fine [22]. Fusion techniques are addressed because verification using single biometric trait has many problems. To resolve these problems, two or more than two traits can be used. Effective fusion is required to integrate the data from multiple sources. Fusion can be done at four levels i.e. sensor level, feature level, matcher level and decision level. These techniques have their own advantages and problems [7]. Biometric data is permanent so if it is compromised then it would not be able to replace. So it is greatly required to

secure the template. This can be done by applying some transformations on data before storing it in database, these use non invertible functions. The process is known as cancellable biometrics [4].

III.FUSION TECHNIQUES

Information obtained from many sources has to be merged in some form so that this can be exploited in authentication process. This Process of integrating data from two or more traits is known as fusion. Fusion can be performed at four levels: sensor level, feature extraction level, matching score level and decision level. The classification is shown in figure 1.

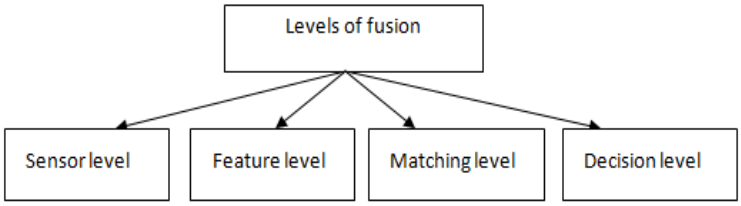

Fig. 1 Classification of fusion levels

a. Sensor level fusion: In this fusion level, biometric traits measured from different sensors like Video Camera, Iris Scanner, fingerprint sensor etc is combined to form a composite biometric trait [8].But at this level fusion is very intricate [2]. This type of fusion is not used commonly because information acquired through various sensors should be compatible to each other, which is sparse.
b. Feature level fusion: Features are calculated from all the inputs distinctly. These feature set are independent to each other. Now these are combined to form a new feature set. Advantage is that, this level is enriched with highest amount of information so it results in better fusion. But problem with this fusion level is that it is very demanding because features of traits are incompatible to each other. For e.g. features in case of finger is minutiae points whereas in face they are Eigen values [7] [3].
c. Matching level fusion :After comparing sample with stored template a score is generated for each trait that can be fused to obtain a combined score[8].Advantage is that this level has adequate in information content and also scores are easy to access and consolidate[1][3][12].
d. Decision level fusion: For each trait individual can be categorized into two groups, accept or reject. This information is combined to generate a final decision of acceptance or rejection [6].Advantage is that it is easiest fusion level because it is easy to combine decision of all traits [3].But problem is that it has very less information content [13].

IV.CANCELLABLE BIOMETRICS

Biometric information is eternally associated with a user and an individual cannot revoke its biometric identifier. Once this data is compromised, it is lost forever. If this data is employed for authentication with many applications, all can be spoofed leading to substantial loss. So it is highly required to the biometric template to be secured. This is done through the concept of cancellable biometrics. In this technique intentional and repeatable set of non invertible transformation is applied on original data and this transformed template is then stored in database [5][6][11].This transformation is applied on the template, consisting of feature set obtained from trait, is transformed using parameters derived from user specific password or key[4][6]. Non invertible means that once the data is transformed, it will not be possible to retrieve the original data by using same or different transformation i.e. data is non invertible now.

This means a template is never stored in original format. Even if intruder is able to obtain transformed data, it would be impossible for it to recover the original data back. A user can be given multiple biometric identifiers by issuing a new transformation key. These can be cancelled and replaced as required or when compromised. There are many transformation functions are available like polar, Cartesian and surface folding etc. We can apply hundreds of transformations and can store all these as distinct data. As discussed these transformation functions are non invertible but by applying multiple experiments revocability can be earned [5] [11].

Three main objectives of cancellable biometrics are [18]:

- Diversity: Different application will use different template.
- Reusability: In case template is compromised, it can be cancelled and revoked.
- Non-Invertibility: Transformation functions should be one way.

Advantages of using cancellable biometrics are that security gets increased manifold. So we are never exposing the original data anywhere. This will be great benefit against spoofing attacks. But the problem is that the computation time of matcher will be increased which leads the system to slow down to some extent. But the great advantage overweighs this problem.

V. PROPOSED FRAMEWORK

Multimodal system refers to the biometric system using two or more than two traits for authentication. There are many traits that can be combined together. In this paper a novel approach to multibiometrics is presented which combines the three biometric traits. These are fingerprint, hand geometry and palmprint. The system works in two modes, enrollment and authentication. These two modes are shown in figure 5 with the help of dotted line. The working of framework is explained as follows:

1. Enrollment Phase: The first time an individual gives its biometrics is known as enrollment. By this data of most of the population is collected, processed and templates are stored into the database.

A. 3 in 1 sensor: This sensor is known as 3 in 1 because giving one input sample i.e. by presenting hand data, it will retrieve three images from this information .This includes fingerprint image, hand geometry image and palmprint image. So advantage of using this sensor is that user need not give all these three samples singly, they just required placing their hand on sensor. Sensor will automatically generate three images out of this one data. This will also diminish enrollment time and thus makes the system very swift. Also this is user friendly. But problem with this sensor is that its computation will be complicated because three images extracted from single image so computation time may increase.

B. Feature set extraction: In this step unique information known as features are extracted from the three images.

a. Fingerprints: A fingerprint is made up of ridges and furrows. Uniqueness is determined by ridges, furrows, the minutiae points. Fingerprint is one of oldest and most popular recognition technique. Every individual possesses unique finger patterns, even twins has different patterns of rings and furrows [9]. Features extracted from fingers are known as minutia points. Major minutia points are ridge ending, bifurcation, and short ridge or dot as shown in figure 2.

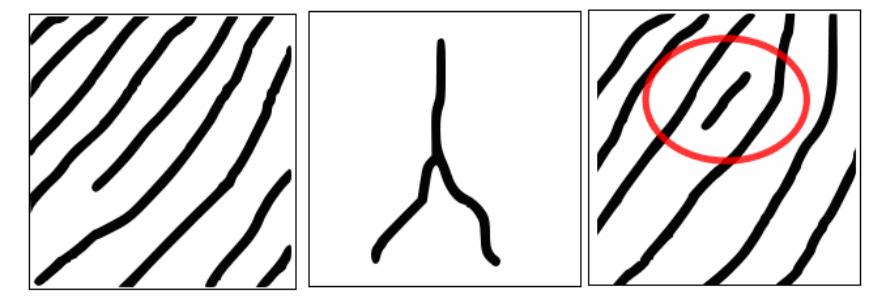

Fig. 2 Minutia points [14]

Ridges are composed of three basic patterns i.e. arch, loop and whorl. Loop can be further divided into left and right loop. These patterns are shown in figure 3.

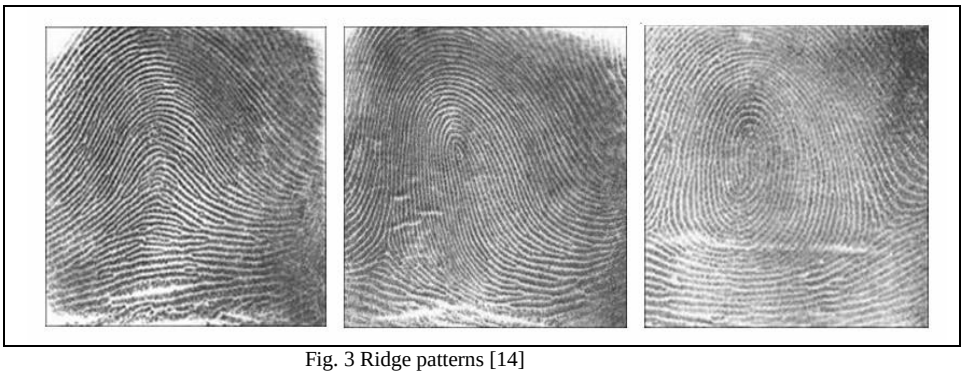

Fig. 3 Ridge patterns [14]

b. Hand geometry: This recognition include measuring length, width, thickness and surface area, overall bone structure etc. of the hand. The fact is that a person's hand is unique and it does not alter after certain age [10].The features extracted includes length of fingers, width of fingers at three locations and the width of palm. This sum up to total 21 features as shown in figure 4.a [15].

c. Palmprint: Palmprint is slightly different implementation of fingerprints [11].Palm of human consists of pattern of ridges and furrows much like fingerprint but this also includes additional features. There are five main feature types extracted i.e. geometric features, principle lines, wrinkles, delta point and minutia features [16].This is shown in figure 4.b.

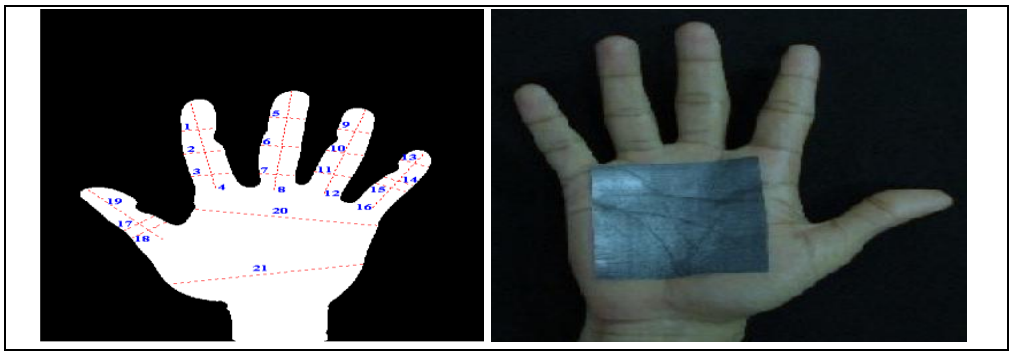

Fig. 4 a. Hand geometry feature set b. Palmprint

C. Fusion at feature level: The three images are now fused at feature level. There are various processes that have to be applied to fuse feature sets, which is given as follows [17]:

a. Compatibility check: Features to be fused should be compatible to each other. For this many processes are done for e.g. rotation and translation.

b. Normalization: The features are made according to some standards for better performance. There are many normalization methods for e.g. min-max technique.

c. Feature reduction: The process of eliminating irrelevant features is known as feature reduction. By this space requirement will also be reduced. The methods are divided into linear and non linear methods. Linear method includes Principle Component Analysis (PCA), Metric multidimensional scaling (MDS) etc. Non linear include non linear PCA [19].

d. Concatenation: Combining the three feature set together is named as concatenation. Let F, H and P denotes feature set of fingerprints, hand geometry and palmprint. C denotes the concatenated feature set.
C = F. H. P

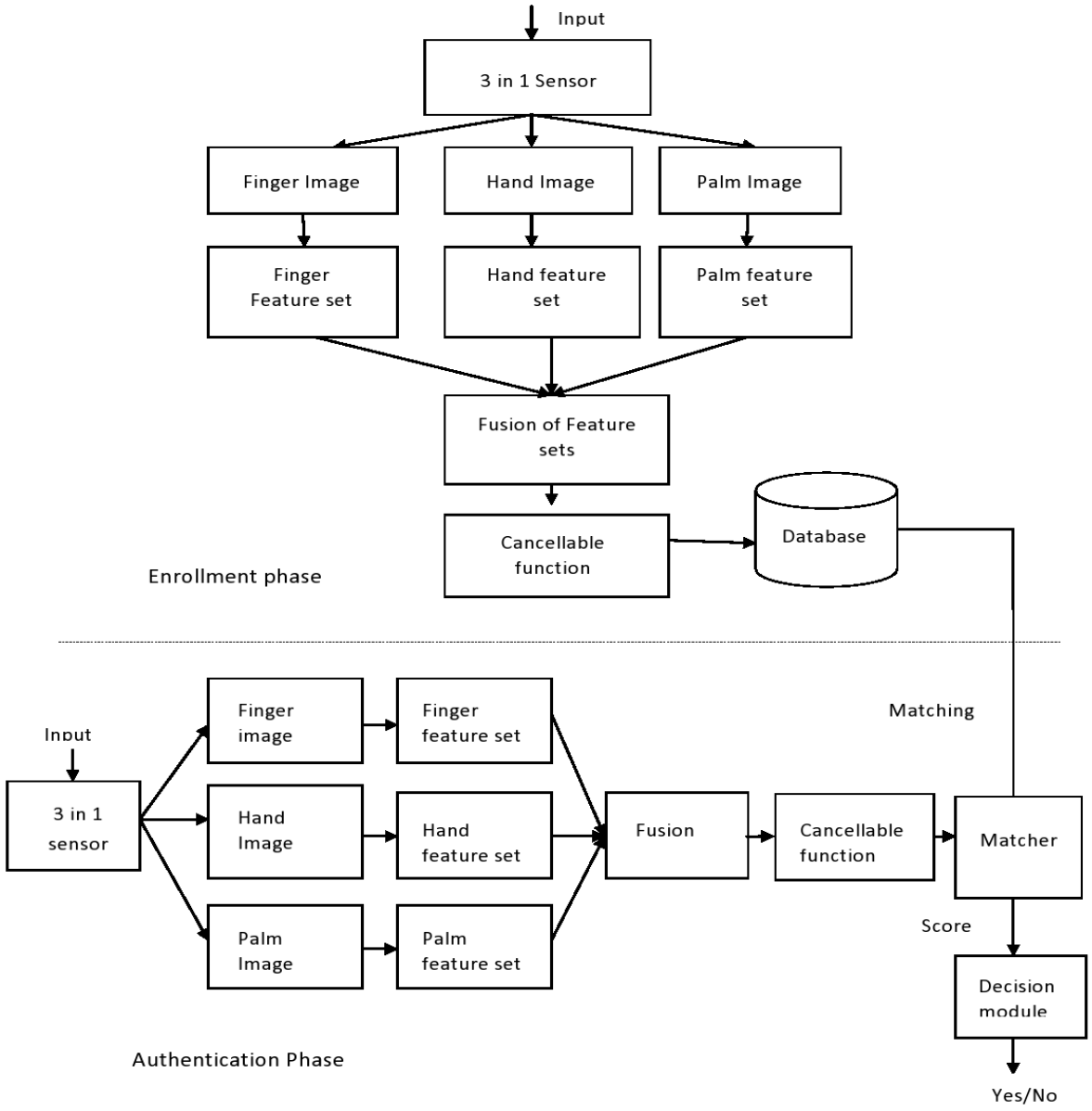

Fig. 5 Proposed framework

D. Applying Cancellable technique: A non-invertible transformation is applied before storing the template into the database. There are various techniques e.g. biometric salting, biohash, polar and Cartesian transformations etc. Let C' denotes the output after applying cancellable transformations.

C'= Cancellable transformation(C)

After this the fused and transformed template is stored into database.

2. Authentication process: At the time of authentication 3 in 1 sensor will work in same manner. Feature set is extracted individually from the three images. Then these independent feature sets are fused together. Then same transformation function, as applied in enrollment phase is applied on the fused data. Now this transformed information will be matched by matcher with the stored templates in the database and a similarity or difference score will be generated. A threshold value is set for acceptance and rejection. Based on this score, decision module will accept or reject user.

Advantages of using this technique are I) Security are increased tremendously because of using both fusion and cancellable biometrics. II) Single sensor is capturing the three images which will reduce enrollment time greatly. But the proposed framework is not free from all the limitation for e.g. complexity of sensor will be high as it is capturing three images together. Also verification time can increase due to applying fusion and cancellable transformations.

VI ALGORITHM OF PROPOSED SCHEME

A Algorithm for enrollment phase

1) Present biometric data to 3 in 1 sensor for first time (enrollment)
2) Sensor extracts finger, hand and palm images
3) Feature extraction from three images
4) Fusion at feature level
   a) Compatibility check
   b) Normalization
   c) Feature reduction
   d) Concatenation
5) Apply non invertible transformation
6) Store template in database

B Algorithm for authentication phase

1) Present biometric data to 3 in 1 sensor
2) Sensor extracts finger, hand and palm images
3) Feature extraction from three images
4) Fusion at feature level
   a) Compatibility check
   b) Normalization
   c) Feature reduction
   d) Concatenation
5) Apply same non invertible function as of enrollment phase
6) Matcher matches this template with stored one
7) Generate similarity or distance score
8) Decision module accepts/ reject user based on this score

VII. CONCLUSIONS

Multimodal biometrics begins to be used due to some issues of unimodal system like noise, intra class variations, lack of uniqueness and universality etc. The multimodal system can reduce the FTC (Failure To Capture) /FTE (Failure To Enroll) rates and also it reduces the possibility of spoofing. The objective in the proposed framework is to use three biometric traits, which includes fingerprint, hand geometry and palmprint. A 3 in 1 sensor is used so user has to enroll only once and three images will be produced. So it is highly user friendly. Feature level fusion is performed. Finally cancellable biometric is applied on the fused data. This will greatly increase security and reliability of system. This novel approach will enhance the system performance to a great extent. But it also suffers from some problems like long processing time due to fusion and cancellable techniques. Also thumb image can't be captured. In future work can be done to remove these problems.

REFERENCES

[1] Karthik Nandakumar,,"Integration of multiple cues in biometric systems",2005.
[2] Anil K. Jain and A. Ross. Multibiometric Systems. Communications of the ACM Special Issue on Multimodal Interfaces, 47(1):34–40, January 2004.
[3] Karine Pellerin," Increasing Accuracy in Multimodal Biometric Systems",Global Information Assurance Certification Paper,2004.
[4] Abhishek Nagar, Karthik Nandakumar and Anil K. Jain," Biometric Template Transformation: A Security Analysis".
[5] Nalini K. Ratha, Sharat Chikkerur, Jonathan H. Connell, and Ruud M. Bolle," Generating Cancelable Fingerprint Templates", IEEE transactions on Pattern Analysis and Machine Intelligence, VOL. 29, NO. 4, APRIL 2007.
[6] King-Hong Cheung, Adams Kong, David Zhang, Mohamed Kamel, Jane You1 and Toby, Ho-Wang Lam," An Analysis on Accuracy of Cancelable Biometrics based on BioHashing".
[7] Arun Ross, Anil Jain," Information fusion in biometrics", Pattern Recognition Letters 24 (2003) 2115–2125.
[8] Ashish Mishra," Multimodal Biometrics it is: Need for Future Systems", International Journal of Computer Applications (0975 – 8887), Volume 3 – No.4, June 2010.
[9] Jain, A. K.; Ross, A. & Pankanti, S., "Biometrics: A Tool for Information Security," IEEE Transactions on Infor-mation Forensics and Security, vol. 1, no. 2, pp 125 – 144, 2006.
[10] R.Sanchez-Reillo, C. Sanchez-Avilla, and A. Gonzalez-Macros, "Biometrics Identification Through Hand Geo-metry Measurements", IEEE Transactions on Pattern Anakysis and Machine Intelligence, Volume 22,Issue 18, Oct. 2000, pp. 1168-1171.
[11] Anil K. Jain, Arun Ross, and Salil Prabhakar, "An Introduction to Biometric Recognition", IEEE transactions on Circuits and Systems for Video Technology, VOL. 14, NO. 1, JANUARY 2004.
[12] N.K. Ratha, J.H. Connell, and R. Bolle, "Enhancing Security and Privacy in Biometrics-Based Authentication System," IBM Systems J., vol. 40, no. 3, pp. 614-634, 2001.Jain, A.K., Prabhakar, S., Chen, S., 1999b. Combining multiple matchers for a high security fingerprint verification system, Pattern Recognition Lett. 20, 1371–1379.
[13] Zuev, Y., Ivanon, S., 1996. The voting as a way to increase the decision reliability. In: Foundations of Information/Decision Fusion with Applications to Engineering Problems,Washington, DC, USA. pp. 206–210.
[14] Chander Kant Verma," Efficiency and Security Optimization for Fingerprint Biometric System" 2009.
[15] Peter Archol, Dusan Levicky," Using of Hand Geometry in Biometric Security", Radio engineering, vol. 16, no. 4, December 2007.
[16] Dapeng Zhang, Wei Shu,"Two novel characteristics in palmprint verification: datum point invariance and line feature matching", Pattern Recognition 32 (1999).
[17] A. Rattani, D. R. Kisku, M. Bicego, and M. Tistarelli," Feature Level Fusion of Face and Fingerprint Biometrics ".
[18] Andrew B.J. Teoha, Yip Wai Kuan, Sangyoun Lee, "Cancellable biometrics and annotations on BioHash", Pattern Recognition archive. Volume 41, Issue 6, June 2008, pp. 2034-2044, ISSN: 0031-3203.
[19] Imola K. Fodor," A survey of dimension reduction techniques", June 2002.
[20] Yong Jian Chin, Thian Song Ong, Michael K.O. Goh and Bee Yan Hiew, "Integrating Palmprint and Fingerprint for Identity Verification", Third International Conference on Network and System Security, 2009.
[21] Ajay Kumar, David C. M. Wong, Helen C. Shen1, Anil K. Jain," Personal Verification using Palmprint and Hand Geometry Biometric".
[22] Fan yang, Didi Yao, "Information Fusion of Biometrics Based-on Fingerprint, Hand-geometry and Palm-print", IEEE workshop on automatic identification advanced technologies, 2007.