Biometrics Verification Techniques Combine With Hidden Biometrics for Multimodal Biometrics Payment System

Davinder Singh
Department of Computer Science & Engineering
GJUS&T, Hisar, India

Ravika Goel
Department of Computer Science & Engineering
GJUS&T, Hisar, India

Sheetal Panu
Department of Computer Science & Engineering
GJUS&T, Hisar, India

Abstract - When dealing with biometrics, we generally refer to security biometrics which is a set of techniques used to identify an individual using his biological or behavioral features. The multimodal biometrics payment is a new technology that allows people to pay with their own biometrics such as fingerprint, face, hand and so on. In this paper, the biometrics verification techniques combining with hidden biometrics and try to discuss and highlight the idea which consists in using medical data, such as biosignals. MRI images and X-Ray images for the purpose of individual identification or verification. That is what we call the "hidden biometrics" or "intrinsic biometrics" for multimodal biometrics payment system are introduced. Considering high universality, distinctiveness, easy collectability of fingerprint and faces, a multimodal biometrics verification system with fingerprint and faces as input is designed and the hybrid fingerprint features and infrared faces features for matching is to overcome the traditional method and grantee the integrity of the registered multimodal biometrics data.

Keywords- multimodal biometrics payment system biosignals, MRI images, ECG,EMG,hidden biometrics.

I. INTRODUCTION

A payment system is a system for the transfer of money which employs cash substitutes. Traditional payment systems are negotiable instruments such as drafts, credit cards and other charge cards. But these payment systems suffer the shortcomings that the token or passwords to ensure the security of the system are easily lost, forgotten, copied, shared or distributed. Biometrics payment is a technology that allow the people to pay at shop or market with one touch of their fingers, moving their faces or laying up their hands. Different with the normal payment methods, they would not need tokens or passwords except their own biometrics. When people use a biometrics payment system, their account information in the bank is automatically recognized to finish the payment procedure. Biometrics payment has the following advantages[5]: 1).Fast: no writing checks and no swiping cards. 2) Easy: no fumbling with cash. People can leave their wallet behind. 3) Secure: their biometrics are unique to them, so only the owner can access their financial accounts.

However due to complex input condition such as input with broken finger, smeared finger and fuzzy finger it is difficult for extracting all the correct minutiae. So the traditional minutiae based fingerprint identification system may cause identification failure. In addition based on a single biometric verification technique (fingerprint, face, hand recognition) there are demerit: some biological features missing (such as broken finger) , injuries (such as damaged finger), disease (such as cataract) or feature collection of poor quality (such as light change in face recognition), these feature will result in non-robust, poor reliability, weak identification[6].

Comparing with single biometric verification technologies, multimodal can be employed in order to increase the performance of the biometric system and achieve more robust system with noise immunity, universality, reliability, security[7].

Multimodal biometric is able to integrate various single biometric verification, and use of the merit of all kind of single biometric. Multimodal biometric is widespread in recent years and becomes a research focus.

Fingerprint, face, hand, veins, iris and other biological and behavioral feature are commonly used within a security context to identify or verify individuals. Specially, such process refers to “security biometric”. When dealing with identification process, biological signature of a given individual is compared to N other signature stored in a database. In such a case (1:N) comparison are performed. On the other hand, when considering (1:1) comparison, the process is called “verification”.

On the other hand, when talking about medical biometrics the purpose is completely different. The process is based basically on measurement performed on medical data where some clinical parameters are extracted in order to provide valuable diagnosis.

In this paper, we discuss the idea which consists in using the medical biometric for security of biometric payment system. In other words , instead identifying an individual using his face, hand, fingerprint, iris and other “visible” or “accessible” biological feature, why not using some ”inaccessible” feature ? Why not using the “brain-print”, “chess-print”, “bone-print”, etc. In such case we refer to “intrinsic biometrics” or “hidden-biometrics”.

The answer to this question may be simple because, it is easy to recognize an individual using the characteristics of what it is accessible or visible. It can be simple, fast, acceptable and not expensive. We can even perform, in some cases, contact less identification because we own the material to perform that. But the main problem is that these modalities or even if we are using multimodal biometric which is the combination of security biometric trait are sensitive to some potential forgeries e.g. fake fingerprint, fake voice, fake face, etc and also sensitive to injuries. However, when considering the hidden biometric no one can modify, deliberately, the geometry and the texture of his own brain or the shape of his bones!

In summary, we propose to use hybrid fingerprint features and IR faces for matching. These features were sophisticated for matching and they were proved of being able to overcome the demerits of the traditional method with high accuracy performance and we propose to use hidden biometric features for matching and to overcome the demerits of the multimodal biometric.

The paper is organized as follows: multimodal biometric verification system is briefly introduced in section 2. In section 3 we will evoke some of the hidden biometric techniques based on biosignals such as ECG and EMG .Afterwards we will discuss how one can use some medical modalities such as MRI images and X-Ray images to perform a robust biometrics.

II. MULTIMODAL BIOMETRICS VERIFICATION SYSTEM

Multimodal biometric verification system contains two stages: the enrollment stage and the matching stage.

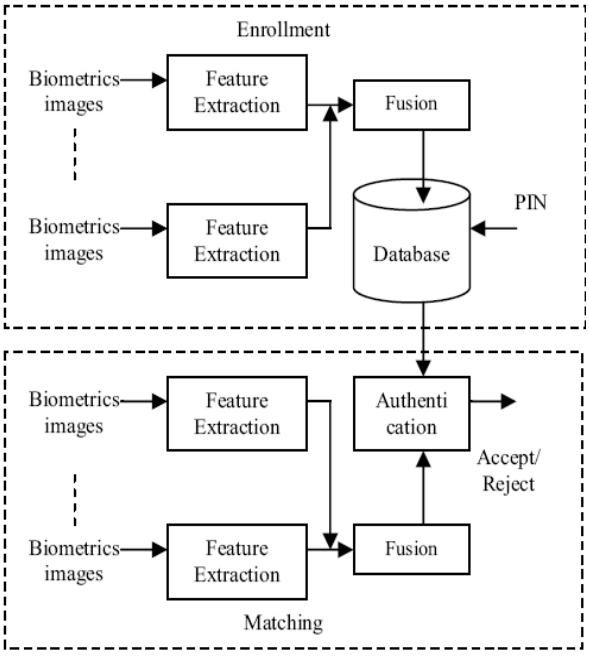


Figure 1- Overview of our multimodal biometrics verification system

The enrollment stage: the multimodal biometric images of the different individual to be verified are first processed by feature extraction module; the extracted features are stored in templates in the database for later use.

The matching stage: the multimodal biometric image of the individual to be verified first processed by feature matching module with his/her identity ID, which match them against his/her own template in the database.

The enrollment stage is realized in the registration step; however the matching stage works when the multimodal biometric payment is adopted.

A. Fingerprint feature extraction

Usually, there are two well-known fingerprint verification methods: (a) minutiae-based methods (b) image-based methods. The minutiae-based methods use several characteristics of minutiae such as type, position, orientation, etc for matching. Minutiae are the small spots or gaps near bifurcation of the ridges. There are many and randomly distributed at various places on the fingerprint minutiae based technique first find minutiae points and map their relative placement on the finger. However these methods may suffer from several shortcomings. Image based methods use features other than characteristics of minutiae from the fingerprint ridge pattern such as local orientation and frequency, ridge, shape and texture information. The feature of these methods may be extracted more reliably than those of minutiae. To combine both merits of two methods, in this paper, we propose a hybrid approach using both global and invariant moment for fingerprint verification. These methods have higher performance comparing with other famous image-based method, so we choose to use these technologies to ensure the integrity of the acquired data.

The algorithm of a hybrid approach using both global minutiae and invariant moments for fingerprint verification is summarized as below:

Step1. Preprocessing with enhancement.

The first step is to preprocess the fingerprint image, which includes fingerprint image segmentation, enhancement, binarization and thinning.

Step2. Minutiae and reference point determination.

In the second step, we determine minutiae and reference point respectively. The minutiae can be extracted from the thinning image by using the crossing number. The core point is defined as the point of maximum curvature of the concave ridges, and is determined by using the complex filtering method [8].

Step3. Fingerprint alignment

We use the reference point to align the input fingerprint image with the template image. The rotation metric is used to align both images in the same orientation, and the translation vector is used to align the relative distance of minutiae in both images.

Step 4. Feature extraction

We present the global matching algorithm based on the aligned fingerprints. Firstly, the global minutiae feature vectors are extracted. We also compute the seven invariant moments (n=1, 2…7) of the rectangle region of interest (ROI), which centered on each minutia and the centre or the rectangle's direction is the same with the orientation of the minutia. Then the fingerprint feature vector consists of minutiae feature and for seven invariant moments for each minutia

B. Face feature extraction

Over the last decades, researchers from multiple disciplines have endeavored to build a machine capable of automatic face recognition with visual images. As a face acquired in visual images has significantly different appearance due to the large variation both in intrinsic (pose, expression,hairstyle,etc). and extrinsic condition (illumination,imaging system, etc.), it is difficult to find the unique characteristics for each face, and it is accordingly not easy to develop a reliable system for face recognition by using visual images.

While visual images represent the reflectance information of the face surface, IR face images contain more fundamental information about faces themselves, such as anatomical information; the thermal characteristics of faces with variations in facial expression and make-up remain nearly invariant, and tasks of face detection, location and segmentation are relatively easier and more reliable than those in visual images. In this paper we adopt to use a method which uses the blood perfusion data for face recognition from skin heat transfer (SHT) model, based on one thermogram. Blood perfusion model of human faces based on thermodynamics and thermal physiology. Blood perfusion data perfusion data are less sensitive to ambient temperature. Blood perfusion data are characterized by regional blood flow in human tissue and therefore do not depend entirely on surrounding temperature. Blood per data are related to distribution of blood vessels under the face skin. A distribution of blood vessels is unique for each person. SHT model converts facial thermogram into blood perfusion data. Facial thermogram vary with ambient temperature blood per data are more consistent in representing facial features. Heat pattern created by branching of blood vessels and emitted from the skin. These patterns called thermogram.

The algorithm of using the blood perfusion data for face recognition from the skin heat transfer (SHT) model is summarized with following steps:

Step1. Image preprocessing.
The first step is to preprocess the face image. First, we acquire the IR image through the infrared camera. When considering noise reduction and keeping effective information, our experiment have demonstrated that rank order filters and morphological filters are the most suitable filters to those impulse noises.

Step2. Face detection
We notice that the outer boundaries of faces, i.e., external boundaries (or we call black boundaries) exist in IR images is thermally separated from its surrounding environment. And such information is independent of imaging condition, so the face can be localized by detecting the face contour. This results in a binary segmentation map with value '0' indicating background and '1' indicating face.

Step3.SHT model
In order to extract the stable and consistent physiological facial features. Blood perfusion model which convert the temperature information of the face image into body's biological information.

Step4.Feature extraction.
After applying the SHT model, the facial image is converted into blood perfusion image, and then Eigen face feature are extracted from the blood perfusion image by using the Karhunen-Loeve Transform (KLT).

C. Fusion and Authentication

Fusion is to combine these two kinds of biometric and from the best output for the multimodal biometric payment system: fusion at extraction level, fusion at score level, fusion at decision level. The latter two methods will lost more information than the first one. So here we adopt the approach of fusion at the feature extraction level. The algorithm can be summarized as below:
Step1. The data obtained from each biometric sensor is used to compute a feature vector.

Step2. As the feature extracted from one biometric trait are independent of those extracted from the other, it is reasonable to concatenate the two vectors into a single new vector.

Step3. The new feature vector now has a higher dimensionality and represents a person's identity in a different (and hopefully more discriminating) hyperspace.

Step4. Feature reduction technique (such as principle component analysis) may be employed to extract useful feature from the larger set of features.

In the authentication stage, the matching algorithm to match the extracted feature of the template and input biometric is through a matching score. This matching score definition assumes that if two feature vectors belong to the same biometric, they will be similarity that yield a larger matching score, whereas if they are different, their score will be still small. The matching can be done in different authentication models.

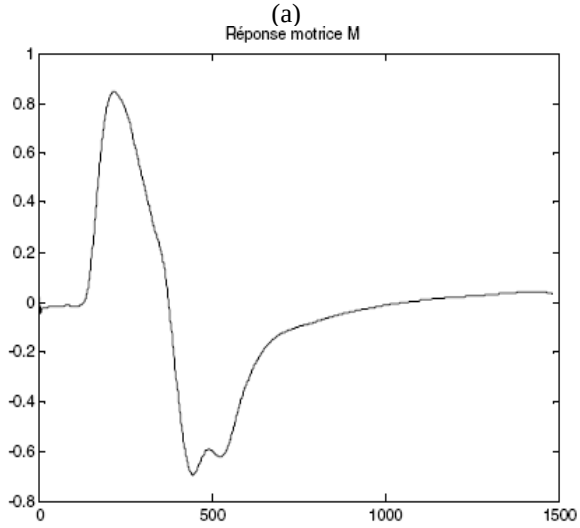
III. HIDDEN BIOMETRIC

A. Biosignals for hidden biometric

Biometric approach inspired from the medical field consists in using the electromyogram (EMG) as a signature. As it is shown on figure-2 , the muscle of the forearm is excited by an impulsional electrical stimulation where the intensity belong with in the range [20-30] mA. The response is recorded using two electrodes. This technique is very efficient since the performance obtained from ten individuals vary between 93% and 100%. Figure--- represents a typical response of a muscle. This simple signal can be easily modeled using a parametrical model which means that few parameters are required to identify an individual.

Another characteristics of this technique is that the signature may change over time since human morphology is subject to slow variations. This aspect can be regarded as an advantage since this characteristics can be useful within the context of cancelable or volatile biometric which make it interesting when dealing with application that require frequent update of the reference signature. Obviously, this is not the case when considering fingerprint biometric.

(a)

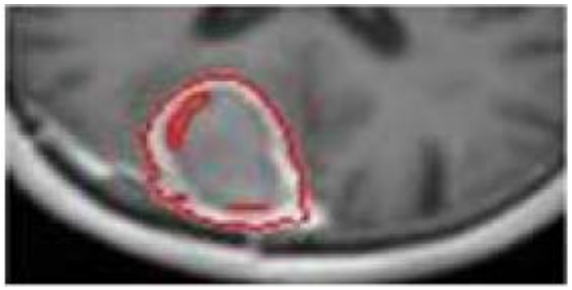


(b)

Fig 2-EMG biometrics. (a) Acquisition system : the muscle is stimulated using an electrical impulse (20-30 mA). (b) Recorded response used as signature.

B. Medical images for hidden biometric

In this section, we show that some technique used for medical biometric can be also used within the context of hidden biometrics for security purposes. For instance, figure--- shows a brain MRI image highlighting an important tumor. This image can be downloaded from the Medical Database for the Evaluation of image and Signal Processing Algorithms (MeDEISA), available at www.medeisa.net. This tumor is extracted from a volumetric image and visualized in 3D[1].



(a)

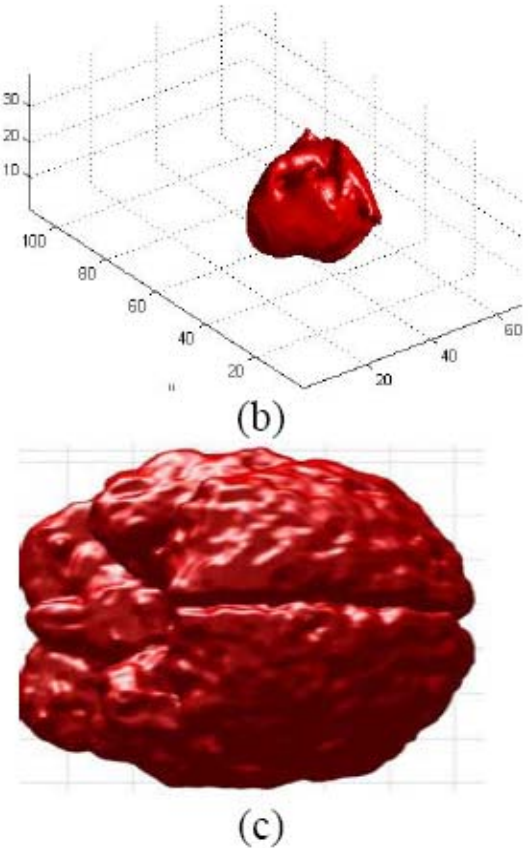


Fig 3-3D brain biometrics. (a) Tumor extraction from and MRI image. (b) 3D representation of a tumor. (c) Hidden biometrics based on 3D brain feature extraction.

The same technique can be used to represent the whole brain as shown in figure -. From the surfacic object, one can extract some valuable parameters that characterize the human brain. As a second approach, one can extract only one slice, from the vertex as shown in figure-4[2]. This slice is afterwards characterized within biometric context by modeling its texture. In our recent work, this slice is processed using the same approach developed for iris identification purpose and which is based on ID Log Gabor wavelet. Afterwards, the identification phase uses a simple hamming distance.

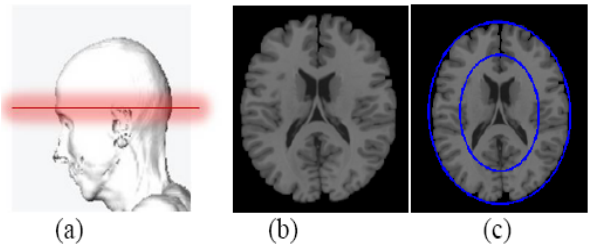


Fig4- 2D brain hidden biometrics. (a) Slice selection at a given distance from the vertex. (b) Corresponding MRI image. (c) Feature extraction using an approach similar to the one used in iris identification [3][4].

Each brain slice is then encoded as shown in figure—which represent the bitwise brain template, called brain code. This brain code characterizes each individual. Our experiments achieved on 210 MRI images provided an accuracy of around 98.25% which is very promising result.

It seems clear currently, “in 2011”, this solution seems inconceivable and cannot consider this type of biometric to access or secure resources, because the main constraint is the acquition system. As we know, in order to visualize the shape of a brain, we need to use MRI images. Within the same context, one should use X-Ray scanners to extract and visualize body skeleton, including skull and other bones, etc. But, we can expect that, in the near future, some system, developed initially for medical biometric application can be used also for security biometric to access to some protected resources. For instance, to increase the security in some airports, low radiation X-Ray machines are used to control the borders. We believe that this concept can be performed and adapted for some specific applications

dedicated to biometric by developing scanners to perform efficiently and safely, the "Hidden biometric" applied to some specific parts of the human body.

IV. CONCLUSION

In this paper, biometrics verification technique for a multimodal biometrics payment system is introduced. A multimodal biometric verification system with hybrid fingerprint features and IR faces features is firstly proposed to grantee the integrity of the registered multimodal biometric data and in this paper we are introducing the concept of hidden biometric technique they can be employed in some application which requires frequent up-date. Hidden biometric technique can be considered as a very robust approach to identify an individual since they can prevent any potential forgery. In fact, this approach cannot be subject to voluntary modification (e.g. no one can change the characteristics of his own brain). However the main problem in 2011 is the fact that acquisition system required producing MRI images or X-Ray images are not currently adopted for this type biometric. Consequently, we believe that a special effort can be provided by industries in order to make the acquition easy, fast, safe and less expensive.

REFERENCES

[1] K. Aloui, "Biométrie du cerveau humain", PhD thesis (in progress), supervised by A. Nait-ali, Université Paris-Est Créteil, France, 2011.
[2] K. Aloui, A. Nait-ali, and S. Nacer "A novel approach based Brain Biometrics: some preliminary Results for Individual identification," IEEE Workshop on Computational Intelligence in Biometrics and Identity Management, April. 2011.
[3] J. Daugman, "How iris recognition works". Proceedings of 2002 International Conference on Image Processing, Vol. 1, 2002.
[4] J. G. Daugman, "High Confidence Visual Recognition of Persons by a Test of Statistical Independence", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol.15, No. 11, pp. 1148–1161, 1993.
[5] http://www.paybytouch.com/portal/site/main.
[6] A. A. Ross, K. Nandakumar, and A. K. Jain, Handbook of Multibiometrics, Springer-Verlag New York, Inc., Secaucus, NJ,USA, 2006.
[7] A.K. Jain, K. Nandakumar, A. Ross, "Score Normalization in Multimodal Biometric Systems", Pattern Recognition, 2005.
[8] J. C. Yang, D.S. Park, "A Fingerprint Verification Algorithm using Tessellated Invariant Moment Features", Neurocomputing, vol. 71(10-12), pp. 1939-1946, 2008.
[9] J. Daugman, "How iris recognition works". Proceedings of 2002 International Conference on Image Processing, Vol. 1, 2002.