Implementing Multimodal Biometric Solutions in Embedded Systems

Jingyan Wang, Yongping Li, Ying Zhang and Yuefeng Huang
Shanghai Institute of Applied Physics, Chinese Academy of Science
P.R. China

1. Introduction

Embedded systems are widely used in the areas of PIM (Personal Information Management) and safety-critical mechanical manipulation. With the increasing demands of privacy protection and safety reliability, these systems confront with all kinds of security concerns. To start with, they are possibly operated in physically insecure environment. The small-size feature of the devices such as cellphones and PDAs lends them easy to be lost and stolen. Furthermore, increasing programmability and networking function of these devices make them feeble to secure against various hacker assaults. While recent advances in embedded system security have addressed issues like secure communication, secure information storage, and tamper resistance (protection from physical and software attacks), objectives such as user-device authentication have often been overlooked, placing a hidden danger on the overall security of the system (Yoo Jang-Hee; Ko Jong-Gook; Chung Yun-Su; Jung Sung-Uk; Kim Ki-Hyun; Moon Ki-Young; Chung Kyoil, 2008).

Traditional methods for personal identification depend on third-party objects such as keys, passwords, certifications, etc. However, these media could be lost or forgotten. Another possible way to solve these problems is through biometrics, for each person has his own special biometric features definitely. Biometric features that can be used for identification include fingerprints, palm prints, handwriting, vein pattern, facial characteristics, iris, and some others like voice pattern and gait. Biometrics-based authentication system is emerging as the most reliable solution (Zuniga AEF; Win KT; Susilo W, 2010). However, personal identity recognition based on any unimodal biometric may not be sufficiently robust or may not be feasible to a particular user group or under a particular situation. Unimodal biometric systems are usually affected by problems including noisy sensor data, inconformity and lack of individuality of the chosen biometric trait, absence of an invariant representation for the biometric trait and susceptibility to circumvention. Some of these problems can be relieved by using multimodal biometric systems, which consolidate evidence from multiple biometric sources (Fan Yang; Baofeng Ma, 2007). Multimodal biometric technology has been developed to an important approach to alleviate the problems intrinsic to unimodal biometric systems and getting more concerns in biometric area (Xiuqin Pan; Yongcun Cao; Xiaona Xu et al., 2008). The most recent commercial and research multi-biometric systems adopt software implementation on PC computer and require a dedicated computer for the image or digital signal-processing task–a large, expensive, and complicated-to-use solution, which is not practical for embedded devices like mobile phones. In order to make biometric recognition ubiquitous, the system's complexity, size, and price must be substantially reduced. This chapter investigates the problem of supporting efficient multimodal biometrics-based user authentications on embedded devices fusing two or more biometrics. In these devices, most traditional ways of interaction (e.g. keyboard and display) are limited by small size, power source and cost. The embedded system based on biometric authentication is applied as the platform of personal identification.

On the one hand, compared with traditional biometric identification systems, the embedded devices of biometric recognition have plenty of advantages. It is low-cost, simple-to-use, no dedicated image sensor; On the other hand, compared with the unimodal biometric systems in embedded device, the embedded multimodal biometrics need more capture devices and should run more than one algorithms. Additionally, it also needs a fusion method to improve the accuracy performance. In this chapter, we will introduce how to design an embedded multimodal biometric system, and describe several embedded multimodal biometric solutions, including the algorithms and the designs of the software and hardware.

The purpose of section 2 is to provide a general guidance for the readers to design a high performance embedded multimodal biometric system. In this section, we discuss two main problems which should be considered in the design of an embedded multi-biometric system: the selection of embedded platform and the biometric algorithms. In the first place, we investigate several embedded platforms suited for biometrics systems, including ARM based MPU processor, Multi-Core Processor combining ARM and DSP cores and so on. Afterwards, we introduce several biometrics algorithms designed for the implementation on embedded devices and the rules to select and optimize them. Following the guidance in section 2, we present three examples for the design of embedded multi-biometrics system in the following sections.

In section 3, we present a multi-biometric verification solution aiming at implementing on embedded systems within a wide range of applications. The system combines the voiceprint with fingerprint and makes the decision at score level. The fusion strategy is based on score normalization and support vector machine (SVM) classifier. This embedded platform adopts an ARM9-Core based S3C2440A microprocessor and the Microsoft Windows CE operation system. An external module PS1802 produced by Synochip Corporation is employed as fingerprint sub-system whilst the voiceprint sub-system uses the microphone of the developing board to capture vocal biometric samples.

In section 4, a new multi-biometrics system is designed for multi-core OMAP3 processor combing GPP and DSP cores, fusing iris and palmprint at sensor level (image level). The algorithm is based on phase-based image matching, which is effective for both iris and palm recognition tasks. Hence, we can expect that the approach can be useful for multimodal biometrics system with palmprint and iris recognition capabilities. The system accomplishes the fusion of palmprint and iris biometric at image level. A new image fusion algorithm, Baud limited image product (BLIP), designed especially for phase-based image matching is proposed. The algorithm is particularly useful for implementing compact iris recognition devices using the state-of-the-art DSP technology. OMAP3 process is utilized to realize this algorithm and then the new effective multi-biometrics system is proposed. Experiment results prove that the new scheme can not only improve the system accuracy performance, but also reduce the memory size used to store the templates and the time consumed for the matching.

In section 5, we introduce a DaVinci based multi-biometrics verification system mainly from the prospective of system design and fusion strategy. Verification systems require flexibility to solve different sorts of situations, so we adopt component-based architecture combined with simultaneous hardware and software considerations to address the problem. In addition, because methods to fuse multiple biometrics have also determined the improvement of the systems' performance, we raise the FAR-score strategy, which normalizes the scores into false acceptance rate. Once scores from all classifiers are normalized into FARs, common fusion rules could be utilized to calculate a singular scalar to make the final decision. The proposed system could fulfill the goals of flexibility and the enhancement of verification accuracy.
The paper would be concluded in section 6.

2. General guidance: How to select multi-biometrics algorithms and embedded platforms

In this section, we discuss the general principles for designing an embedded multiple biometrics authentication system. The discussion is two-fold: how to choose the embedded platform and design the multiple biometrics algorithms. We should notice that, though we mention the above two sections of embedded multiple biometrics system separately, they must be considered jointly when you are going to complete the system. Moreover, the essential rule of design is not to choose the most powerful embedded platforms or the most effective algorithms, but to satisfy the requirements of the user. We recommend that the readers keep this in mind, so that you can understand the followings are just options, not the necessarily optimal choice for the designer.

To sum up, the embedded multi-biometrics system, such as a hand-held personal authentication system owns the following two characters:

1. Unlike the traditional uni-biometrics system, it combines two or more biometric modalities for more secure authentication. The advantage of the fusion multimodal biometrics lies on the improvement of the accuracy of the system by fusing more information. Of cause, the improvement depends on the deft fusion strategy. However, it requires the embedded processor to run more than one biometrics algorithms, which might be fatal for resource-limited embedded system on both processor and memory. Thus, when the design chooses the modalities, the complexity of the algorithm should be considered with the fusion algorithms. At the same time, the way to capture the biometric data is also an important factor.
2. The system differs with other traditional CP based systems, for the embedded system is limited on resources for complex biometrics verification algorithms. Considerable though the advantages of the prospective embedded biometrics solutions enjoy, they can not diminish the realistic difficulties current systems suffer from, such as the limited resources of the embedded device, high computational expenses of the biometrics algorithm and so on.

2.1 Algorithms

The biometric fusion procedure usually involves two steps. The first is to choose appropriate biometrics, which could provide essential information for recognition. The second is to design an effective method for fusing the biometrics. First of all, we introduce some commonly used biometric modalities; then we will discuss the fusion methods. The biometrics can be an option for multi-biometrics including the following examples as displayed in (Fig 1).

- **Iris** is a kind of biometrics with high security. However, it needs a special capture device, which limits its applications. We design a high-security authentication system in case II, using iris as one modality, providing for the readers as reference.
- **Fingerprint** is another high performance biometrics. Similar to iris, it also needs a special fingerprint sensor. However, among the most frequently used biometric solution, there are many commercial devices which could be integrated into self-designed systems directly, making it an excellent choice for identity authentication.
- **Face** can be captured easily with a general camera integrated in a cellphone or a PDA, but it is easily influenced by the clients' posture, the environment's illumination and so on. Nonetheless, this disadvantage can be compensated by fusing with other biometrics insensitive to the above factors.
- **Palmprint** has several advantages compared with other biometrics (Ito K.; Aoki T.; Nakajima H. et al., 2006): palmprint capture devices are cheaper than iris devices; and palmprints contain additional distinctive features which can be extracted from low-resolution images. However, the accuracies of these approaches are not so satisfied for the requirement of some high secure applications.
- **Voiceprint** is the most natural modality for PDA or cellphone based embedded system, for most mobile devices can capture voice signals using a microphone. This feature is used in case I.

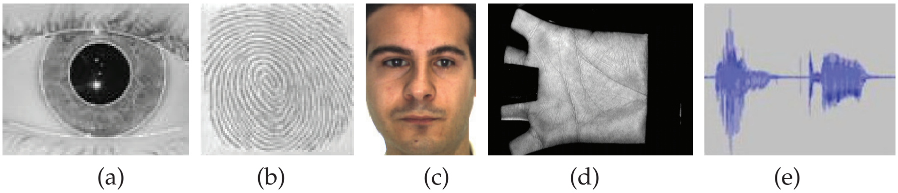


Fig. 1. Biometric modalities used in embedded multi-biometrics system: (a)Iris; (b)Fingerprint; (c)Face; (d)Palmprint; (e)Voiceprint.

Multi-biometric systems fuse information from multiple biometric sources in order to achieve better recognition performance and overcome other limitations of unibiometric systems (Nandakumar K; Chen Y; Dass SC et al., 2008). Fusion can be performed at four different levels of information, namely, sensor, feature, match score, and decision levels (Fig 2).

1. Fusion at the sensor level means the biometric data is fused directly before the features are extracted. This kind of fusion can preserve most parts of the information, for it combines the biometric modalities before they are processed further. The case II in this chapter utilizes this fusion strategy, integrating palmprint and iris image at the pixel level. This fusion needs flexible algorithms and is not general for all the other biometric modality.
2. In fusion at the feature-extraction level, the features extracted using two or more sensors are concatenated. The fusion is established by joining two or more features into a long vector. This category of modes is not practical because the features of the various

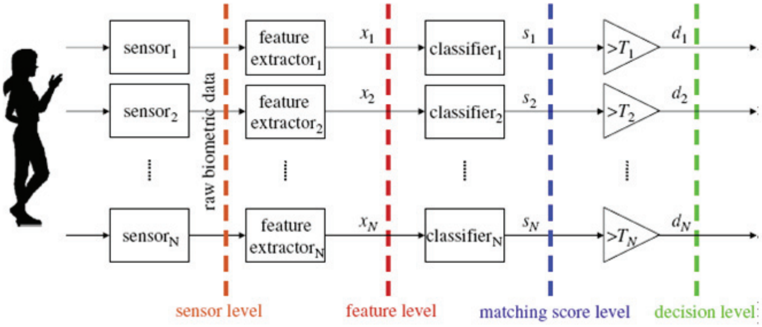


Fig. 2. Four levels at which multimodal biometrics can be fused.

modalities could be incompatible. For example, face images normally have larger sizes than those of finger images. Moreover, in this type of fusion modes, the recognition system does not work if one or more modalities of testing samples are not available.

3. In fusion at the matching-score level, the matching scores obtained from multiple matchers are combined. Furthermore, score fusion techniques can be again divided into the following three categories:
   - Transformation-based score fusion. The match scores are first normalized (transformed) to a common domain and then combined with each other. The case III is based on this fusion strategy.
   - Classifier-based score fusion. Scores from multiple matchers are treated as a feature vector; then, a classifier is constructed to discriminate genuine and impostor scores. We adopt this strategy in case II.
   - Density-based score fusion. The approach is based on the likelihood ratio test. It requires explicit estimation of genuine and impostor match score densities (Jingyan Wang; Yongping Li; Xinyu Ao et al., 2009).
4. In fusion at the decision level, the accept/reject decisions of multiple systems are jointly considered.

In practice, fusion at match score level and decision level are usually employed since they are much easier to accomplish, but in these modes, the useful information has never been exploited for fusion before the match and decision.
Here, we recommend the readers to choose the fusion strategy jointly with the biometric modalities. Two rules can be referenced as follows:

1. Because fusion at the lower level can preserve more useful information than higher level, we should first consider lower fusion (sensor or feature level). However, lower level algorithms are hard to design, for the original data is quite distinctive for different modalities. The best chance to use low-level fusion is when different modalities can be matched in the same way. An example is given in case II in section 4 of this chapter, as iris and palmprint can both be matched by POC function. Another advantage of low-level fusion is that it only matches once for verification, which reduces the time and space complexity of the algorithm.

2. When the modalities cannot be fused at low-level, the reader can consider the matching score level. Fusion at this level has been studied a lot by researchers and plenty of effective algorithms have been developed. An example is given in section 3.

2.2 Embedded platform

For the biometric solutions, there are many embedded platforms to be considered:

GPP A common ARM-Core processor, such as LPC2106 (Martin T., 2004) by NXP Semiconductors, or S3C2440A (SAMSUNG Electronic Company, 2004) by SAMSUNG Electronics Company, can be a good choice for multi-biometrics system. For example, an advanced smart card chip($5mm \times 5mm$) can employ 32-bit ARM7 or ARM9 CPU, 256KBytes of ROM program memory, 72KBytes of EEPROM data memory, and 8KBytes of RAM at most. Since the smart card chip has very limited memory, typical biometric verification algorithms cannot run on the card successfully. However, we can use a commercial device for a uni-biometric verification, just like what we do in section 3, so that the complex verification algorithm is finished outside the ARM processer with only the fusion being done by ARM. The advantage of using ARM is that it can usually run an Embedded WinCE or Linux operating system. This is very useful for real-world applications, because it can provide a good user interface.

DSP DSP might be the most suitable processer for biometric algorithms. Some powerful DSP solutions provided by Texas Instruments have already been used in biometric systems, which could refer to Wencang Zhao; Zhen Yang; Haiqing Cao (2010); Xin Zhao; Mei Xie (2009); Shah D.; Han K.J.; Narayanan S.S. (2009); Yanushkevich (S.N.; Shmerko) for more information. We must notice that the only use of DSP is not enough for the real-world applications, for it usually cannot provide a friendly user interface. This is mainly because it cannot run an OS like ARM which is designed to work with an embedded system. This shortage can be overcome by the so-called multi-core processer.

Multi-core processer Recently, some powerful embedded multimedia platforms have be proposed by TI. Two typical examples are the DaVinci and OMAP. These platforms are often combined with an ARM based GPP processor and a DSP processor. At the same time, some software and hardware components have also been provided to the developers to establish the communication between them. For multi-biometrics systems, the complex verification algorithms can be implemented on the DSP core, and the user interface can be implemented in the OS on ARM core. We will give two examples in this chapter, in section 4 and section 3 separately.

FPGA FPGA or CPLD is another choice for multi-biometrics solution. However, due to the complexity of the design, we usually won't consider it as a practical option.

At last, we should note that the choice of embedded platform should consider the two following factors:

1. Are the algorithms complex? If yes, we recommend you to implement in Multi-core system like DaVinci; else, a sample MCU or ARM processor will be enough.
2. Is this system stand-alone or integrated to existing embedded system? If it is a stand-alone system, you will have more freedom to choose a platform; if it is integrated, apparently, it should match the existing processor, and what you need to do is just to develop a new software system.

3. Case details I: ARM based multi-biometrics fusing fingerprint and voiceprint

In this case, we propose a new multi-biometric verification solution aiming at implementing on an embedded system within a wide range of applications. The system combines the voiceprint with fingerprint and makes the decision at score level. Fusion strategy is based on score normalization and support vector machine (SVM) classifier. We test the performance of SVM using three kernel functions for system adaptation. Experimental results demonstrate that proposed multi-biometric verification approach achieve. 1.0067% in equal error rate (EER), which means it can be deployed in the majority of embedded devices such as PDA and smart cellphone for user identity verification. We first introduce the single biometric verifiers, including the fingerprint and voiceprint. Then the proposed score level fusion method is given. Afterwards, we describe the design and implementation of multi-biometric system. Finally, we show the performance testing results.

3.1 Fingerprint and voiceprint verifiers

3.1.1 Fingerprint verifier

For fingerprint verification implementation, the full-functioned fingerprint identification system-on-chip (SOC) PS1802 produced by Synochip Corporation (Synochip Corporation, 2006) is employed. PS1802 fingerprint module uses a commercial minutia extraction algorithm, including image preprocessing, binarization, thinning and minutia finding. The output image of each process is given, as we can see from Fig. 3. With these minutia features, the alignment-based elastic matching algorithm is used.

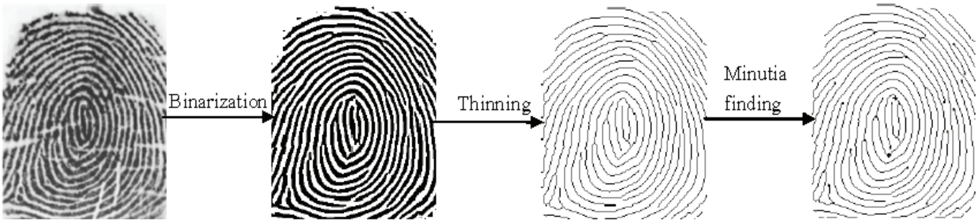


Fig. 3. Output images of PS1802 modaląŕs minutia extraction algorithm.

3.1.2 Voiceprint verifier

The voiceprint recognition system is content-dependent; it accepts voice samples for up to 10 seconds and enrolls the user in less than 4 seconds. The speech recordings used for feature extraction are utterances of a 4-digit PIN in English. The recording speech is divided into several small segments with a fixed length. Then a 34-dimensional feature vector is calculated using 20ms Hamming windows with 10ms shift. Each feature vector consists of (concatenated):

- the Mel Frequency Cepstral Coefficients (size 16);
- the energy coefficient (size 1),
- the first order derivatives of the MFCC (size 16)
- the delta energy (size 1).

The number of feature vectors between users and presentations may differ. With these feature vectors, we train the code book for each speaker with VQ (Vector Quantization) (Cai Geng-ping; Huang Shun-zhen; Xu Zhi-hong, et al.).

3.2 Multiple biometrics fusion method

As to fuse fingerprint and voiceprint verification systems, a score vector $X = (x_1, x_2)$ representing the score output of multiple verification systems is constructed, where x_1 and x_2 correspond to the scores obtained from the fingerprint and voiceprint verification system respectively. Then the identity verification turns to be the problem of separating the 2-dimension score vector $X = (x_1, x_2)$ into two classes, genuine or impostor. In other words, identity verification typically equals to binary classification problem, i.e. accept (genuine) or reject (imposter). We adopt SVM as the fusion strategy of the fingerprint and voiceprint identity verification system.

3.2.1 Score normalization

In our approach, the raw scores from fingerprint and voiceprint match system are normalized before they can be inputted into SVM, following (Jain, A; Nandakumar). These score can be normalized by max-min method as follows:

$$x = \frac{x - min}{max - min} \tag{1}$$

where *min* and *max* are the minimum and the maximum values of these scores x.

3.2.2 Support vector machine fusion

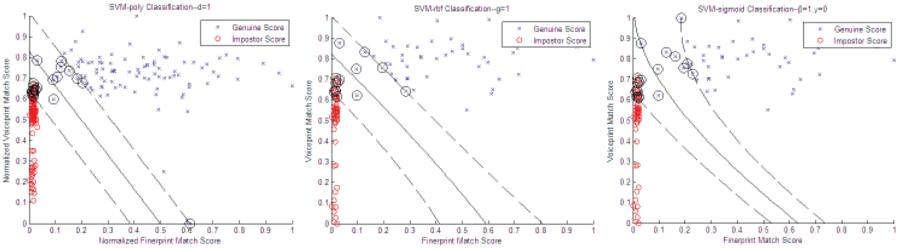
Support vector machine (SVM) is based on the principle of structural risk minimization (Suykens JAK; Vandewalle J., 1999). In Yuan Wang; Yunhong Wang; Tieniu Tan. (2004), SVM is compared with other fusion methods of fingerprint and voiceprint, and its performance is the best. In this paper, we pay attention to the performance of SVM with different kernel functions. The detailed principle of SVM has not been shown in this paper, but it can be seen in reference Suykens JAK; Vandewalle J. (1999). Three kernel functions of SVM used in our study are:

Polynomials $K(x, z) = (x^\top z + 1)^d, d > 0$

Radial Basis Functions $K(x, z) = exp(-g||x - z||^2)$

Hyperbolic Tangent $K(x, z) = tanh(\beta x^\top z + \gamma)$

In order to choose the best kernel function for our system, we test the performances of SVMs based on three kernel functions mentioned above, and the results can be seen at the Fig. 4.
Fig. 4 shows different SVMs with different kernel functions classifying genuine and impostor of fingerprint and voiceprint after normalization. We can see that three SVMs can all separate the two classes correctly. Their performances are similar; however, the number of support vectors and the difficulty to adjust parameters of kernel function are different. In our experiment, the SVM-poly is easier to be trained than SVM-RBF and SVM-sigmoid; the latter two need more patience during training period. Moreover, the classification error of the SVM-poly is the lower (0.3%) than the other two (0.4% and 0.5%), which makes polynomials kernel function our final choice.



(a) (b) (c)

Fig. 4. SVM Classification results with different kernel functions: (a) SVM-Poly; (b) SVM-RBF; (c) SVM-Tanh.

3.3 Design and implementation of multi-biometric system

3.3.1 System frame and design scheme

The multi-biometric verification system is composed of three sub-systems: fingerprint sub-system, voiceprint sub-system and score level fusion sub-system. The embedded platform adopts an ARM9-Core based S3C2440A microprocessor and the Microsoft Windows CE operation system. An external module PS1802 produced by Synochip Corporation is employed as fingerprint sub-system whilst the voiceprint sub-system uses the microphone of the developing board to capture voice biometric samples. System software is developed by using Microsoft Embedded Visual C++. The system frame is shown in Fig. 5.

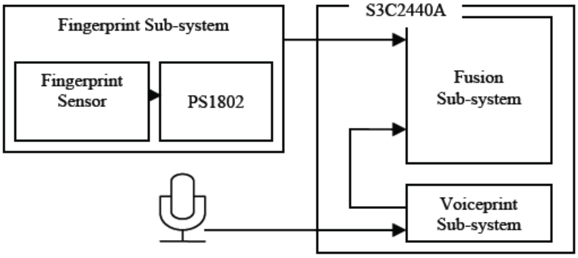


Fig. 5. The frame of multi-biometric verification system.

3.3.2 Hardware architecture

We utilize the S3C2440A, a 32-bit RISC microprocessor made by Samsung Company (SAMSUNG Electronic Company, 2004). To meet the demand of the audio capturing of voiceprint, the IIS-bus interface model with a UDA1341 audio CODEC is adopted. The Universal Asynchronous Receiver and Transmitter (UART) model is used as interface to fingerprint model PS1802. The techniques concerning the voiceprint recognition and multi-biometric fusion algorithm have been used in the system. Fig. 6 shows the hardware structure of the multi-biometric embedded system.

3.3.3 System software implementation

A multi-biometric verification system works in two models: enrollment model and verification model. In the off-line enrollment model, an enrolled fingerprint image and

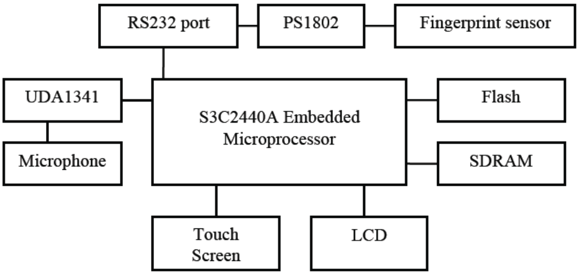


Fig. 6. The hardware structure of ARM-based multi-biometric verification system.

voice signal is preprocessed, and the features are extracted and stored into the on-board memory or the external SD card. In the on-line verification model, the similarity between the enrolled features and the features of real-time captured fingerprint image and voice signal are examined, giving two match scores. After fusing the two scores using SVM, decision can be determined by comparing the fusion score with the threshold. Fig. 7 shows the working models and data flow of a multi-biometric verification system.

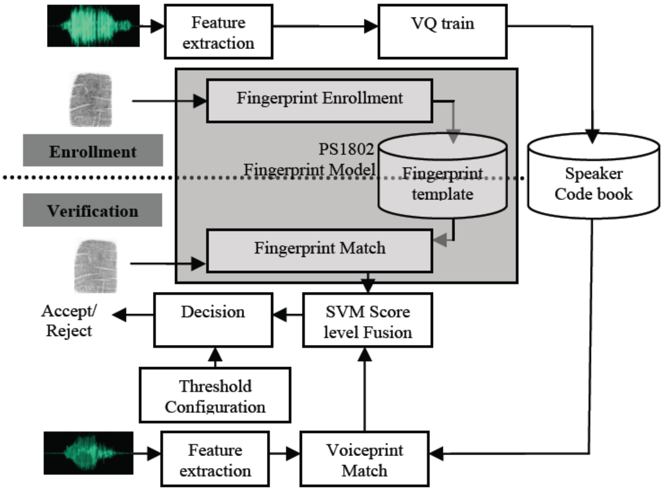


Fig. 7. The working models and data flow of a multi-biometric verification system.

4. Case details II: OMAP3 based multi-biometrics fusing iris and palm at image level

To improve the performance of the multimodal biometrics system, we proposed an effective image fusion method—band limited image product (BLIP) (Jingwang Liu; Yan Hou; Jingyan Wang; Yongping Li; Ping Liang, 2007), especially for phase based image matching. Using this method, we fuse iris and palmprint images to construct a multimodal framework, which can not only improve the security, but also can reduce the time and space complexity. Based on

OMAP3530's 'Dual Processor' character, we implement the algorithm and optimize it in terms of algorithm and programming, improving the execution efficiency further.

4.1 Multi-biometrics verification algorithm fusing iris and palmprint at image level

Figure 8 shows the overview of the proposed algorithm, which fuses the iris and palmprint image to one single image and uses it for verification. In this section, we describe the detailed process of the proposed algorithm, which consists of effective region extraction (to be explained in Section 4.1.1), image fusion (to be explained in Section 4.1.2), and matching score calculation (to be explained in Section 4.1.3).

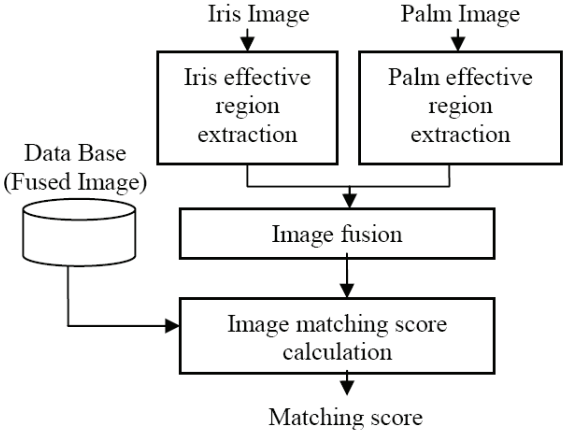

Iris Image
Palm Image
Iris effective region extraction
Palm effective region extraction
Data Base (Fused Image)
Image fusion
Image matching score calculation
Matching score

Fig. 8. Flow diagram of the proposed algorithm.

4.1.1 Iris and palm effective region extraction

To extract region from the iris, two circular boundaries of iris are searched by the integro-differential operators. Then, the disk-like iris area is unwrapped to a rectangular region by using doubly dimensionless projection, as shown in Figure 9.

In order to detect the effective palmprint areas in the palm image, we examine the n_1-axis projection and the n_2-axis projection of pixel values. Only the common effective image areas with the same size are extracted for the succeeding image matching step, as is shown in Fig. 10.

4.1.2 Baud limited image product fusion

In previous work (Miyazawa, Kazuyuki; Ito; Ito K.; Aoki T.; Nakajima H. et al., 2006; Miyazawa K; Ito K; Aoki T et al., 2006; Miyazawa, K.; Ito), the idea of the Phase-Only Correlation (POC) function for matching of iris and palm is proposed. Inspired by the POC function, we can fuse the image of iris and palm into one single image which containing all the phase information of iris and palm used for POC match. Since the product of two complex number's phase is the sum of the two phases, we can use the product of the iris and palm image, and the product image will contain the sum of the phase of the two. To solve the mismatch of the iris and palm' size and to improve the matching performance, Baud

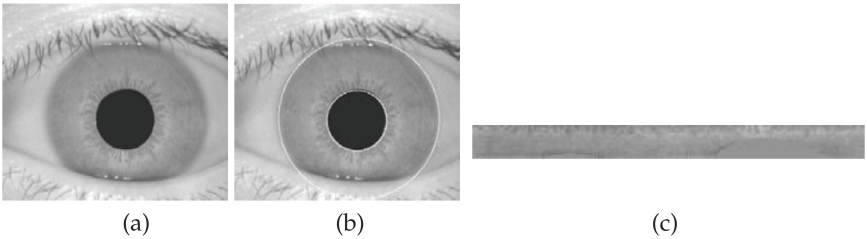


Fig. 9. Iris effective region extraction: (a) Iris image; (b) Two circular boundaries of iris; (c) rectangular region.

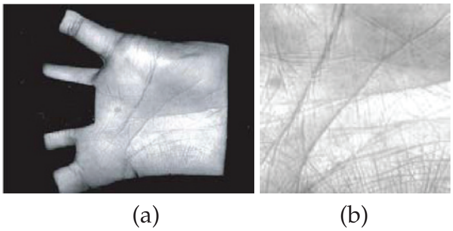


Fig. 10. Palm effective region extraction: (a) The palm image; (b) extracted common regions.

Limited 2D-IDFT (BL 2D-IDFT) considering the inherent frequency components of images is raised. Our observation shows that the 2D DFT of a normalized iris image and the extracted common palm regions sometimes includes meaningless phase components in high-frequency domains as illustrated in Fig. 11. The idea to improve the matching performance is to eliminate meaningless high frequency components in the calculation of 2D IDFT depending on the inherent frequency components of palmprint images.

For mathematical simplicity, consider $(2M_1+1) \times (2M_2+1)$ iris images $f_{iris}(n_1, n_2)$ and $(2N_1+1) \times (2N_2+1)$ iris image $f_{palm}(n_1, n_2)$,where we assume that the index ranges are $n_1 = -M_l, \cdots, M_l$, $n_2 = -M_2, \cdots, M_2$ for iris image and $n_1 = -N_l, \cdots, N_l$, $n_2 = -N_2, \cdots, N_2$ for palm image. Moreover, we assume that the ranges of the inherent frequency band are given by $k_1 = -K_1, \cdots, K_1$ and $k_2 = -K_2, \cdots, K_2$, where $K_1 = Min(M_1, N_1)$ and $K_2 = Min(M_2, N_2)$. Thus, the effective size of frequency spectrum is given by $L_1 = 2K_1 + 1$ and $L_2 = 2K_2 + 1$. The Baud Limited 2D-IDFT (BL 2D-IDFT) function is given by

$$f'(n_1, n_2) = \frac{1}{L_1 L_2} \sum_{k_1=-K_1}^{K_1} \sum_{k_2=-K_2}^{K_2} F(k_1, k_2) W_{K_1}^{-n_1 k_1} W_{K_2}^{-n_2 k_2} \tag{2}$$

Where the $F(k_1, k_2)$ is the 2D-DFT of $f(n_1, n_2)$,and $f(n_1, n_2)$ can be $f_{iris}(n_1, n_2)$ or $f_{palm}(n_1, n_2)$,as illustrated in Figure 5. Then the BLIP algorithm can be described in Algorithm 1.

The flow diagram of Baud Limited Image Product Fusion is shown in Figure 11.

4.1.3 Image matching using POC

We calculate the POC function $r_{fg}(n_1, n_2)$ between the two fusion images $f'_{fusion}(n_1, n2)$ and $g'_{fusion}(n_1, n2)$, and evaluate the matching score. Let $F(k_1, k_2)$ and $G(k_1, k_2)$ denote the 2D-DFTs of the two images $f'_{fusion}(n_1, n2)$ and $g'_{fusion}(n_1, n2)$. The cross-phase spectrum

Algorithm 1 Baud Limited Image Product Algorithm.

```
Require: The iris image $f_{iris}(n_l, n_2)$ and the palm image $f_{palm}(n_1, n_2)$;
Require: The fused image $f'_{fusion}(n_l, n_2)$;
  Calculate 2D-DFTs of $f_{iris}(n_l, n_2)$ and $f_{palm}(n_1, n_2)$ to obtain $F_{iris}(k_l, k_2)$ and $F_{palm}(k_l, k_2)$;
  Calculate BL 2D-IDFTs of $F_{iris}(k_l, k_2)$ and $F_{palm}(k_l, k_2)$ to obtain $f'_{iris}(n_l, n_2)$ and $f'_{palm}(n_1, n_2)$;
  Calculate the pixel product of $f'_{iris}(n_l, n_2)$ and $f'_{palm}(n_1, n_2)$ to get the final fused image $f'_{fusion}(n_l, n_2)$, as follows,
      $$f'_{fusion}(n_l, n_2) = f'_{iris}(n_l, n_2) \times f'_{palm}(n_1, n_2) \qquad (3)$$
```

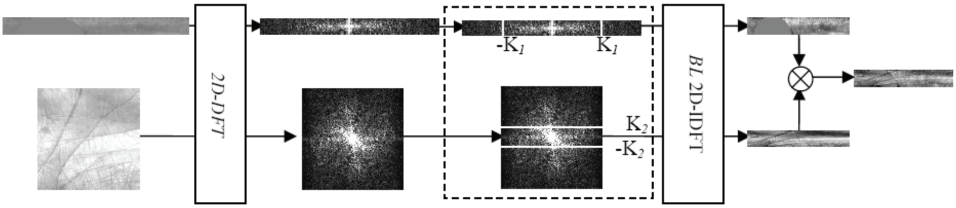


Fig. 11. Flow diagram of Baud Limited Image Product Fusion

$R_{FG}(k_l, k_2)$ is given by

$$R_{FG}(k_l, k_2) = \frac{F(k_1, k_2) \times \overline{G(k_1, k_2)}}{|F(k_1, k_2) \times \overline{G(k_1, k_2)}|} \tag{4}$$

where $\overline{G(k_1, k_2)}$ is the complex conjugate of $G(k_1, k_2)$. The POC function $r_{fg}(n_1, n_2)$ is the 2D Inverse DFT (2D-IDFT) of $R_{FG}(k_l, k_2)$ and is given by

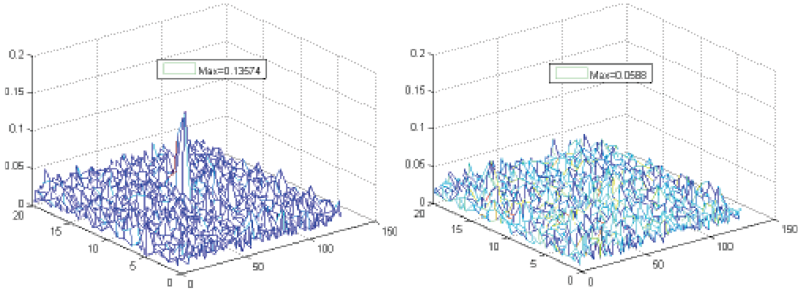
$$r_{fg}(n_1, n_2) = \frac{1}{L_1 L_2} \sum_{k_1=-K_1}^{K_1} \sum_{k_2=-K_2}^{K_2} R_{FG}(k_l, k_2) \quad W_{K_1}^{-n_1 k_1} W_{K_2}^{-n_2 k_2} \tag{5}$$

Figure 12 shows examples of genuine and impostor matching respectively. When two images are similar, their POC function $r_{fg}(n_l, n_2)$ gives a distinct sharp peak, or the peak value drops significantly, so the matching score is the highest peak value.

4.2 Design of OMAP3 based multi-biometrics system

The personal authentication system's framework is given in Fig. 13. According to the requirements of personal authentication, the system can be divided to two parts: the user enrollment module and the verification module.

- **Enrollment Module.**This module should capture the templates of users and store them into the database. First, the iris and palmprint images are captured; then the effective region of both iris and palmprint are extracted; finally they are fused using the BLIP



(a)

(b)

Fig. 12. Example of image matching using the POC function: (a) Genuine matching; (b) Impostor matching.

algorithm and stored in the database as templates. This procedure is illuminated in the pink dashed block in Fig. 13.

- **Verification Module.** In this module, the client first input his iris and palmprint image, and similarly, the effective region are extracted and fused to a single image, which contains the phase information of both iris and palm. Finally, this image with a small size is matched with the template using the POC function and the matching score is compared with the threshold to make a decision.

4.2.1 OMAP3530 applications processor

To design a multi-biometrics personal authentication system, a great variety of embedded system platforms and strategies are available for choice, but the following advantages have made TI's DSP based open multimedia application platform (OMAP) an excellent one. Firstly, it can accomplish complex DSP algorithm in real-time with very low power consumption and very small package size. Secondly, it integrates widely used and supported processors which represent the leading technical level. At last, The OMAP platform is based on a highly extensible architecture that can be expanded with application-specific processing capabilities and additional I/O so that even the most complicated multimedia applications will execute smoothly and seamlessly. In this case, a mobile multi-biometrics authentication terminal based on OMAP MPSoC device would be presented.

The device integrates multiple processors. The main parts consist of MPU and DSP (Texas Instruments, 2009):

MPU The MPU is a 600-MHz ARM Cortex-A8 processor core with a high-effectively, lower power consumption, and the DSP core is a 430-MHz TMS320DMC64x+ which is designed for digital signal processing. The MPU controls all resources of the device though running generic operating system such as Linux or Windows CE.

DSP The DSP acts as a coprocessor of the MPU. In addition, the device includes other processors or subsystems, such as 2D/3D hardware accelerator to deal with vector graphics processing.

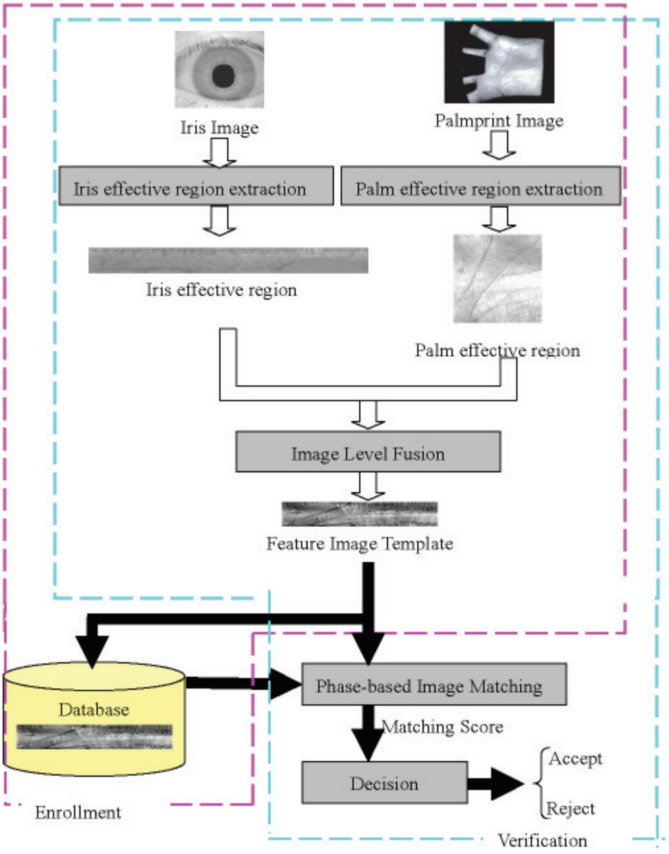


Fig. 13. Framework of the multi-biometrics software system.

4.2.2 System software implementation and optimization

The software design starts from embedded operating system running on ARM Cotex-A8 core. MontaVista Linux and Google Andriod have been successfully ported to the terminal respectively.

Another sort of important software for the terminal is DSP/BIOS Bridge (DSP Bridge). Itąŕs a software package designed by TI Instruments for OMAP platform. It enables asymmetric multiprocessing on target platforms which contain a general purpose processor (GPP) and one or more attached DSPs. Itąŕs a combination of software for both the GPP Operating System (OS) and DSP OS that links the two operating systems together. The linkage enables applications on the GPP and the DSP to easily communicate messages and data in a device-independent, efficient fashion (Jinhe Zhou; Tonghai Wu; Rongfu Wu, 2009). The software of OMAP platform includes the application layer and signal processing layer. The application layer runs in the Linux on OMAP's GPP core, while signal processing layer runs in OMAP's DSP core, and their interaction is through the Codec Engine.

Although the time complexity of the algorithms is not high, the preliminary implementation on the Linux in MPU core is not satisfying in real-time performance. ARM Cortex-A8 Core shows poor real-time performance in reading the image, extracting the effective region, 2D-FFT and 2D-IFFT transformation, image production and image matching. To finish this procedure, it takes ARM Cortex-A8 as long as 1 minute. To satisfy the real-time requirement of real-world applications, we need to optimize the algorithm. The strategy is to employ the DSP core in OMAP3530 processor to do the operation like FFT, so that the system can improve its performance. At the same time, we will also optimize the programs running in DSP core to save the operating time.

4.2.3 Algorithm transplantation on dual-core processor

According to the characteristics of the algorithms, we transplant parts of the program to the DSP core. The main program will call these functions and finish the enrollment and verification. The strategy of transplantation is shown in Table 1.

Program	GPP	DSP
Flow Control	all	-
User Input and Output	all	-
Iris Effective Region Extraction	Locating Iris Center	Inner and outer boundary detection; Iris Normalization
Palm Effective Region Extraction	Constructing axes; Extracting the center subimage	Palmprint binaryzation; Boundary detection
Image Fusion	-	all
Image Matching	-	all

Table 1. Strategy of Algorithm'S Transplantation

On the one hand, in the whole Flow Control procedure, there are many *if-else* and *switch* statements, and GPP is better than DSP on running these statements; on the other hand, the iris and palmprint images are both stored in the Linux file system on GPP, which cannot be accessed by DSP directly, so we decide to implement the main flow control and the input output procedure in GPP. The algorithms in the system, including the iris and palmprint effective region extraction, fusion, and matching, utilize many 2D-FFT and 2d-IFFT operations; at the same time, they are suitable for parallel computing, which can be executed by DSP's pipelines efficiently, so we choose to transplant them to DSP core. All the algorithms are implemented according to xDAIS standard, and are called by application program in Linux on GPP based on the Codec Engine (CE) module. The corresponding enrollment and verification flow-process diagram is given in Fig 14.

4.2.4 Program optimization on DSP

Because the TMS320C64x+ DSP core in OMAP3530 is a fixed-point processor and most of our algorithms are floating-point algorithms, we carry out fixed-point programming to the programs to improve the efficiency. According to our experiments, we scale the data using Q11, which can both keep the precision of the program and improve the algorithm's efficiency. Other technologies are also taken to improve the efficiency:

- Optimization of compiling options;

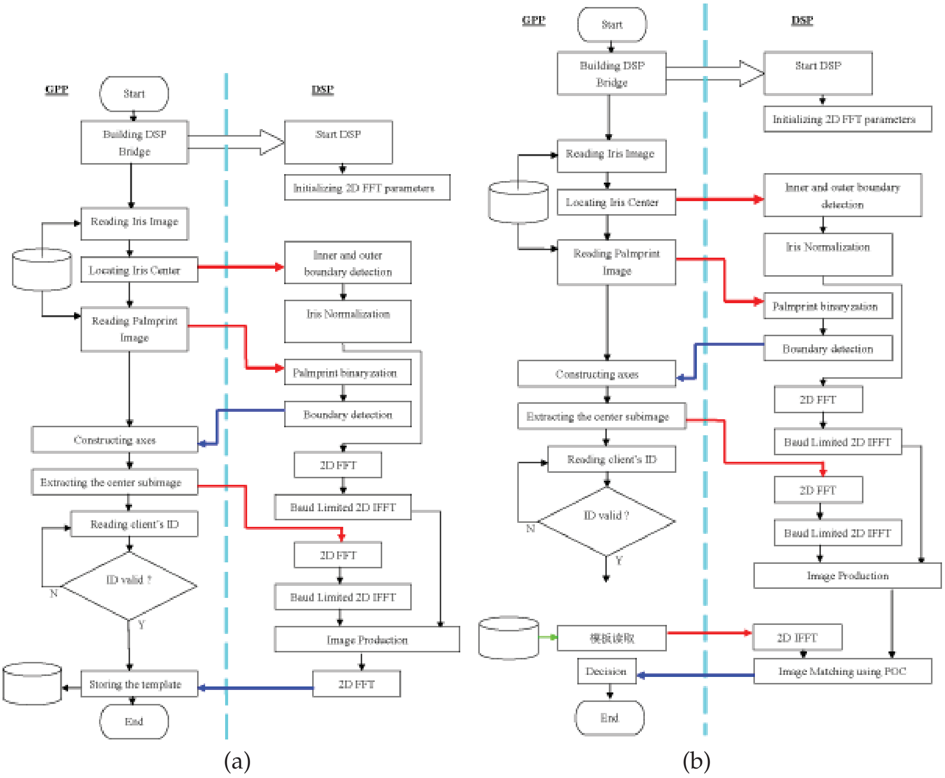


Fig. 14. Enrollment and Verification Flow-Process Diagram on Dual-Core Processor OMAP3530.

- Loop Unrolling;
- Block Data Movement Using DMA Module.

5. Case Details III: DaVinci based multi-biometrics verification

In this case, a multi-biometric verification system based on TI's DaVinci DSP platform is presented. It aims to achieve the following goals: (1) deployed friendly with environment; (2) flexible to networking circumstances; and (3) configurable with changing on scheme of biometrics matching. Accordingly, we extend the component-based architecture to the embedded computing environment and this will be introduced in the first part. Based on the systematic design, a face recognition subsystem and fingerprint recognition subsystem are constructed to test the solution and explore the capability of multiple biometrics subsequently. In the end, conclusions would be drawn on the DaVinci based verification system.

5.1 System design on embedded system

The unpredictability of complex scene requires flexibility of the verification system. To address this issue, sensors capturing biometrics features should be plugged at any time, which should be coined as "Plug and Play" standard updating its state dynamically. The system architecture as shown in Fig. 15 is given in the following. However, there are several other problems existing in the biometrics verification system. First, verification system usually is based on simple assumptions. Biometrics is idealized to be captured in the best condition, where faces are deemed to be acquired with the frontal view. Secondly, the traditional dumb terminal model fails to adapt in more volatile circumstances, such as at the POS site or in the subway check-in station. Thirdly, occlusions and camouflages decrease the verification performance greatly in reality, which become the main obstacle for companies to adopt biometrics verification solutions in their business. Furthermore, limited biometrics excludes particular groups of people from the verification process, such as disabled person without fingerprint or palm print.

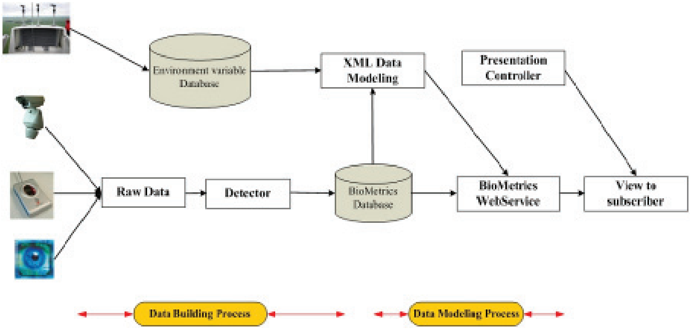


Fig. 15. Architecture of biometrics system.

To eliminate problems above, the system should add precaution mechanisms to facilitate the usage. In our system, knowledge of the angle and distance to the reference point is added to the sensors. We try to find location mismatch itself and collect the input again from a sensor which can minimize such disparity between different locations. Resultantly, the system is equipped with the capability to find the change of its attached sensors and its related configuration. Currently, the change of sensors and its configuration depend on manual work, so does the trigger of reloading the new configuration.

As shown in Fig. 16, the red line between data layer and service layer is triggered when the system tries to send feedback to data layer for new data from different conditions. The hardware to support this kind of behavior is smart sensors based on DSP technology. The sensor is connected to the system using network cables. HTTP server is installed on the DSP server to listen to the port for possible commands action specified by the system. Command and control input is fed from specific port after the DSP chip receives the signal and will be dispatched to the GPIO interface of the DSP to control movement of the sensor. In the experiment, DaVinci Multimedia platform is only used for video processing. Hopefully, it could be extended to other sensors which could be sensitive to the position when capturing biometrics data in the future.

5.1.1 Hardware platform

In the DaVinci system, the TMS320Dm6446 DSP chip is used here. Within the DSP chip, there are ARM926EJ-S kernel, TMS32064x+DSP, video/image compressors (VICP), and Video

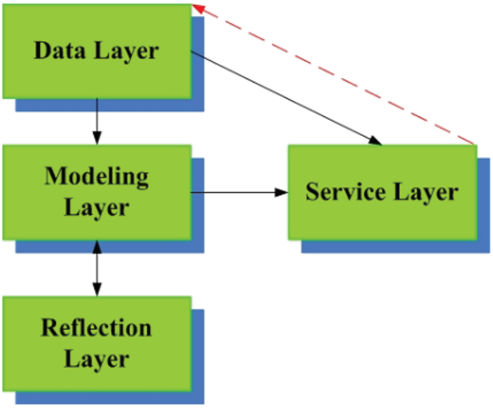


Fig. 16. Architecture of biometrics system.

Processing Sub System (VPSS). The DaVinci system is placed in the smart camera. The verification system is running on an IBM eServer with four Itanitum CPUs, which is running Linux Server.

5.1.2 Software subsystem

The software module running on the DSP system includes a real-time Linux, which will communicate with the DSP hardware through DSP link as illustrated in Fig. 17. The software running on the DSP-enabled sensors abides the standard of TI as shown in Fig. 18. That is to say software module should be conformed to xDAIS standard. The numbers in the figure correspond to the following actions.

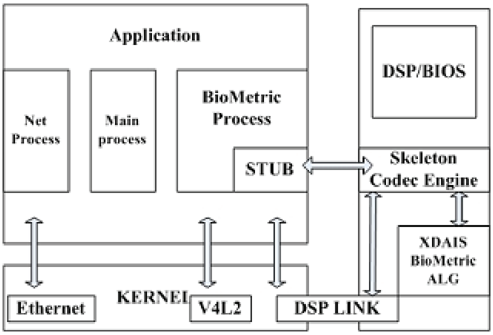


Fig. 17. Architecture of biometrics system.

- The GPP (General Processor Platform) side application makes an algorithm call;
- Codec Engine forwards this calling conventions to the GPP side algorithm stub;
- The stub places the argument in a compact inter-CPU message and replaces all GPP-side (virtual address) pointer values with DSP-side (physical address) values, which is called "marshalling" the argument;

- CE delivers the message to the DSP-side algorithm skeleton;
- The skeleton unmarshals the argument and calls the actual xDAIS algorithm's process function;
- On the way back, the skeleton marshals any return arguments, places them in a message and the stub unmarshals them for the application.

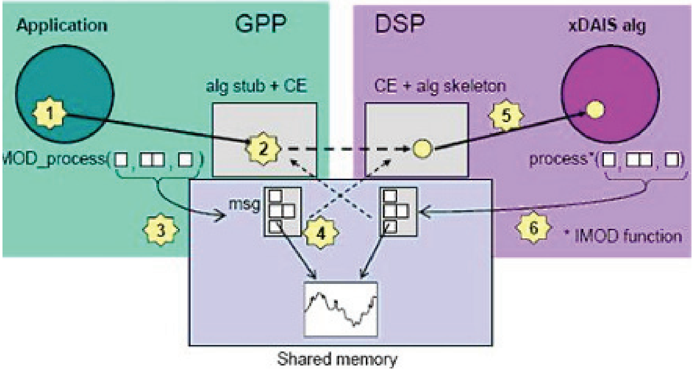


Fig. 18. Architecture of biometrics system.

These steps are excerpted from reference (Texas Instrument, 2007).

5.2 Fusion on multiple biometrics

There are three kind of multi-modal biometrics verification system: the first is the multi-algorithm system which employs different algorithms to verify a single biometric trait; the second is the multi-biometric system that involves two or more distinct modules of biometric traits; the third is the hybrid system wherein the multi-algorithm and multi-biometric systems are integrated together. The paradigm employed here takes the second way to fusion on multiple biometrics to reach a single conclusion. The fusion method employed here is to convert the matching score into the false acceptance rate. Score normalization for multi-classifier fusion refers to transform the various scores obtained by different classifiers into a common domain. Distinct matcher produces score diversely in numerical range and meaning, so the evaluation standards vary accordingly. It is necessary to normalize the scores into homogeneous domain before combination. When normalizing scores of different classifiers, two factors should be considered.

In practice, classifier outputs a matching score s to reflect the similarity between the testing sample Z and the claimed class. In general, s can be modeled as shown in Eq. 6.

$$s = f[P(genuine|Z)] + \eta(Z) \tag{6}$$

f is a monotonic function and η is the bias of the classifier and often supposed to be zero.

Jain et. al recommends normalizing scores with a certain functions such as z-score and their functions as below.

$$n = \frac{s - mean(S)}{std(S)} \tag{7}$$

$$n = \frac{1}{2}[tanh(0.01\frac{s - mean(S)}{std(S)}) + 1] \tag{8}$$

n is the normalized score, *mean* and *std* denote the arithmetic mean and standard deviation operators respectively. S is the set composing of scores from the classifier. Although these functions use the statistical characters of scores such as means and variances, they do not follow the distributions of the scores from different classifiers.

We introduce a novel normalization method here, which converts scores into false acceptance rate. In the typical Receiver Operating Characteristic (ROC) curve of a classifier, two sorts of probabilities are relevant to the scores: the false acceptance rate and false rejection rate. They are functions of threshold (denoted as h) and can be written as following.

$$\begin{aligned} f_{far}(h) &= P(genuine|imposter, s < h) \\ &= \frac{false\ positive}{positive\ instances} \end{aligned} \tag{9}$$

$$\begin{aligned} f_{frr}(h) &= P(imposter|genuine, s > h) \\ &= \frac{false\ negative}{negative\ instances} \end{aligned} \tag{10}$$

To learn the FAR-score curve, a series of thresholds h should be calculated beforehand. For a training set of K classes, each class has m samples, so there are $mK(K-1)$ imposter samples in sum. For the j classifier, at the ith threshold of h^j_i, the false acceptance rate is $f(h^j_i)$. Using a set of thresholds ($h^j_{i-1} < h^j_i < h^j_{i+1}$), the FAR-score curve can be calculated. When a testing sample Z comes with a claim, the score S^j from the jth matcher can be normalized by the curve. If FAR monotonically increase with h^j, s^j is normalized by the following equations.

$$n^j = far^j_i(h^j_i) + \frac{dfar^j_i}{dh^j}|_{h^j=h^j_i}(s^j_i - h^j_i);\ \ h^j_{i-1} \le h^j_i \le h^j_{i+1} \tag{11}$$

Otherwise, Eq. 12 is used to normalize S.

$$n^j = far^j_i(h^j_{i+1}) + \frac{dfar^j_i}{dh^j}|_{h^j=h^j_i}(s^j_i - h^j_{i+1});\ \ h^j_{i-1} \ge s^j_i \ge h^j_{i+1} \tag{12}$$

When scores from all classifiers are normalized into FARs, the common fusion rules such as sum, min, med and max can be adopted to compute a single scalar to make a final decision. In the experiment, the face module and fingerprint module will compute their score independently first, then it will be combined in the way in different algorithm to get the single value.

5.3 Conclusions on DaVinci based verification system

The DaVinci based system performs well and reaches the active responsiveness standard with the aid from outside. It could launch the newly developed modules at run time with the only need being that you specify the change in related configuration document. Currently, face and fingerprint modules are tested. The FAR-score curve of each classifier is computed without assumptions of observing any distributions, and scores from all classifiers can be normalized by it own FAR-curve. Therefore, the method can be adapted to scores from any classifiers. However, the responsiveness needs extra improvement.

6. Conclusion

In this chapter, we discuss the design of multi-biometrics authentication system for embedded devices like high-end cellphones or PDAs. The aim here is to provide the readers on ideals about how to design a multi-biometrics satisfying the requirement of embedded devices. The general guidance is first given on how to select proper algorithms and embedded platforms. Then we introduce three useful examples in the following sections to show how to fuse them together.

With the fast development of mobile communication, embedded devices advance with each passing day. Because it is power efficient, fast authentication and compact in size, embedded device-based multi-biometrics verification system would be in widespread use in the near future.

7. References

Yoo, Jang-Hee; Ko, Jong-Gook; Chung, Yun-Su; Jung, Sung-Uk; Kim, Ki-Hyun; Moon, Ki-Young; Chung, Kyoil. Design of embedded multimodal biometric systems. Proceedings - International Conference on Signal Image Technologies and Internet Based Systems, SITIS 2007, p 1058-1062, 2007.

Zuniga, AEF; Win, KT; Susilo, W. Biometrics for Electronic Health Records. JOURNAL OF MEDICAL SYSTEMS Volume: 34 Issue: 5 Pages: 975-983 Published: 2010

Fan Yang; Baofeng Ma A new mixed-mode biometrics information fusion based-on fingerprint, hand-geometry and palm-print. 2007 4th International Conference on Image and Graphics Pages: 689-93 Published: 2007 .

Xiuqin Pan; Yongcun Cao; Xiaona Xu, et al. Ear and face based multimodal recognition based on KFDA. 2008 International Conference on Audio, Language and Image Processing Pages: 965-9 Published: 2008.

Yuefeng Huang; Xinyu Ao; Yongping Li; Chengbo Wang (2008), Multiple biometrics system based on DavinCi platform, 2008 International Symposium on Information Science and Engineering (ISISE) Pages: (vol.2) 88-92 Published: 2008.

Jingyan Wang; Yongping Li; Ping Liang, et al.(2009), An effective multi-biometrics solution for embedded device Proceedings of the 2009 IEEE International Conference on Systems, Man and Cybernetics. SMC 2009 Pages: 917-22 Published: 2009.

Jingyan Wang; Yongping Li; Xinyu Ao, et al. Multi-modal biometric authentication fusing iris and palmprint based on GMM. 2009 IEEE/SP 15th Workshop on Statistical Signal Processing (SSP) Pages: 349-52 Published: 2009.

Nandakumar, K; Chen, Y; Dass, SC, et al. Likelihood ratio-based biometric score fusion. IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE Volume: 30 Issue: 2 Pages: 342-347 Published: 2008.

Martin, T. Introduction to the LPC 2100 architecture. Embedded System Engineering Volume: vol.12, no.1 Pages: 30-2 Published: Jan.-Feb. 2004.

Wencang Zhao; Zhen Yang; Haiqing Cao. The System of Face Detection Based on DSP. 2010 8th World Congress on Intelligent Control and Automation (WCICA 2010) Pages: 2834-7 Published: 2010.

Xin Zhao; Mei Xie. A practical design of iris recognition system based on DSP 2009 International Conference on Intelligent Human-Machine Systems and Cybernetics. IHMSC 2009 Pages: 66-70 Published: 2009.

Shah, D.; Han, K.J.; Narayanan, S.S. A low-complexity dynamic face-voice feature fusion approach to multimodal person recognition. Proceedings of the 2009 11th IEEE International Symposium on Multimedia (ISM 2009) Pages: 24-31 Published: 2009.

Yanushkevich, S.N.; Shmerko, A.V. Fundamentals of biometric system design: new course for electrical, computer, and software engineering students. Proceedings of the 2009 Symposium on Bio-inspired Learning and Intelligent Systems for Security (BLISS 2009) Pages: 3-8 Published: 2009.

Jwu-Sheng Hu; Ming-Tang Lee; Chia-Hsing Yang An embedded audio-visual tracking and speech purification system on a dual-core processor platform. Microprocessors and Microsystems Pages: 274-84 Published: 11 2010 Nov. 2010.

Synochip Corporation: PS1802 DSP Brief Introduction. Technical report, Synochip Corporation (2006)

Cai Geng-ping; Huang Shun-zhen; Xu Zhi-hong, et al. Voiceprint recognition system. Journal of Shenzhen University Science & Engineering Volume: vol.19, no.2 Pages: 78-80 Published: June 2002.

Jain, A; Nandakumar, K; Ross, A. Score normalization in multimodal biometric systems. PATTERN RECOGNITION Volume: 38 Issue: 12 Pages: 2270-2285 Published: 2005.

Suykens, JAK; Vandewalle, J. Least squares support vector machine classifiers. NEURAL PROCESSING LETTERS Volume: 9 Issue: 3 Pages: 293-300 Published: JUN 1999.

Yuan Wang; Yunhong Wang; Tieniu Tan. Combining fingerprint and voiceprint biometrics for identity verification: an experimental comparison. Biometric Authentication. First International Conference, ICBA 2004. Proceedings (Lecture Notes in Comput. Sci. Vol.3072) Pages: 663-70|xvii+800.

SAMSUNG Electronic Company: S3C2440A 32-BIT RISC MICROPROCESSOR USER’S MANUAL.

Miyazawa, Kazuyuki; Ito, Koichi; Aoki, Takafumi; Kobayashi, Koji; Nakajima, "An effective approach for Iris recognition using phase-based image matching", IEEE Transactions on Pattern Analysis and Machine Intelligence, , v 30, n 10, p 1741-1756, 2008.

Ito, K.; Aoki, T.; Nakajima, H., et al. A phase-based palmprint recognition algorithm and its experimental evaluation. 2006 International Symposium on Intelligent Signal Processing and Communications (IEEE Cat. No.06EX1444) Pages: 215-18|CD-ROM Published: 2006

Miyazawa, K; Ito, K; Aoki, T, et al., An iris recognition system using phase-based image matching, 2006 IEEE International Conference on Image Processing, ICIP 2006, Proceedings Pages: 325-328 Published: 2006.

Miyazawa, K.; Ito, K.; Aoki, T., et al., An efficient iris recognition algorithm using phase-based image matching. 2005 International Conference on Image Processing Pages: II-49-52|CD-ROM Published: 2006

Texas Instruments,OMAP3530/25 Applications Processor, http://focus.ti.com.cn/cn/docs/prod/folders/print/omap3530.html.

Jinhe Zhou; Tonghai Wu; Rongfu Wu, A mobile multimedia network terminal based on MPSoC 2009 First International Conference on Future Information Networks. ICFIN 2009 Pages: 121-5 Published: 2009.

Texas Instrument. Codec Engine Algorithm Creator User's Guide, Published: 2007.

Jingwang Liu, Yan Hou, Jingyan Wang, Yongping Li, Ping Liang, Fusing Iris and Palmprint at Image Level for Multi-Biometrics Verification, 2010 The 3rd International Conference on Machine Vision, Accepted.