Secured Authentication of Space Specified Token with Biometric Traits – Face and Fingerprint

B.Prasana Lakshmi[#] & A.Kannammal[*2]
[#]SCSVMV University, Kanchipuram 631501, TN, India
[*]Coimbatore Institute of Technology, Coimbatore 641014, TN, INDIA

Abstract
This paper deals with the efficient authentication model using multimodal face and fingerprint on space specified token. Since space specified token occupies only small amount of data this proposal has been given to minimize the data storage in the card. Here the face images are encrypted and encoded into fingerprint images . The verification accuracy is also high and provides a cheap solution from spoofing and many other attacks.
Key words:
Multimodal Biometrics, Face, Fingerprint, Smart token, Authentication.

1. Introduction

Personal identification technology is nowadays becoming more important in security systems. Today authenticating through traditional mode such as password, key, magnetic card etc., are vanishing and disliked by people since they could be stolen or easily forgotten. In order to fill this vanishing space biometric technology is emerging in wide number of systems. Also biometric systems have been an important area of research in these recent years. Two important utilizations of biometric systems are Authentication or Verification and Identification, which is based on the biometric trait enrolled. This enrolled biometric trait may be physiological or behavioral characteristic of a human being satisfying the requirements of universality, uniqueness, permanence and collectability. These biometric systems are non- deterministic , since a single entity when spoofed may be analyzed and the fact that usage of multimodal traits can avoid such spoofing problems we go on for multimodal biometric traits.

For the real time authentication since people prefer to have cards, the multimodal biometrics discussed above are invoked into the smart card which is a space specified token. The multimodal biometric traits taken under consideration are the Face and Fingerprint. In any biometric entity there are some features involved in it. These features constitute the pattern.

The following section discusses in detail the algorithms for face feature extraction, Fingerprint core point detection, a random number generator which encrypts the face template and encoding technique adapted to embed encrypted face template into the core point of fingerprint. These many steps are involved to enhance and ensure security and also a case exists that even if one trait fails the encoded template can act as backup of the claimed identity.

2. Proposed scheme

In order to attain secure multimodality the fingerprint image's template hides the face template. The proposed scheme is diagrammatically illustrated below.

A. Face Feature Extraction

Face feature extraction is done based on the following scheme and the Face Feature vector we get is of size *n-k* .

1. Compute the Singular Value Decomposition of the given face image, and take the *n-k* most significant components. Let the result be the vector $F_s = (V_{k+1,} \ldots, V_n)$

2. Similar to the fingerprint features , assume that there is another random *n-k* by *n-k* randomization matrix M_s associated with each user. Compute $F_s M_s = (U_{k+1,} \ldots, U_n)$

3. Quantize the above feature vector. In particular, we choose a scalar quantizer with step size λ_j for the component $U_{j,}$ and each λ_i is selected according to the variation of U_j over the entire population. Let the final discrete feature for the i^{th} user be $F_i^{(2)} = (Z_{k+1,} \ldots, Z_n)$

During authentication, given another face image, we can extract its feature in the same way and get another feature vector $F' = (W_{k+1,} \ldots, W_n)$. This vector is considered as similar to $F_i^{(2)}$.

B. Fingerprint Feature Extraction

The fingerprint feature extraction is minutiae based which are feature points extracted from the captured fingerprint images. The Steps followed are:

Manuscript received July 5, 2009
Manuscript revised July 20, 2009

1. Compute the centroid C=(X_c , Y_c) of the minutiae F_r as the center of mass of the minutiae available in lump.

2. For every pair of minutiae, if the distance between them is more than the threshold T, draw a straight line passing these two points , and mark its intersection with the circle of center C and radius R.

3. Partition the intersection points obtained in the previous step. In particular , we divide the circle into list of ordered arcs of Δ degrees each. Let the arcs be $A_{1,\ldots\ldots} A_K$ where K= 360 / Δ. Let the vector V= ($V_{1,\ldots\ldots} V_K$) represent the list of number of intersection points on these arcs.

4. Assume that there is a random matrix M_r of order *K* by *K* .associated with each user then compute V $M_r = Z_{K+1,\ldots\ldots} Z_n$.

5. The final feature is the vector F= $Z_{1,\ldots\ldots} Z_k$

C. Encoding face template into fingerprint template

Figure 1 shows the steps that are taken for this encoding and description of each step follows.

1. Fingerprint and Face images of the person are retrieved through corresponding sensors.

2. For authentication purpose the important features of the face are extracted which is done by a highly scalable facial feature extraction method .

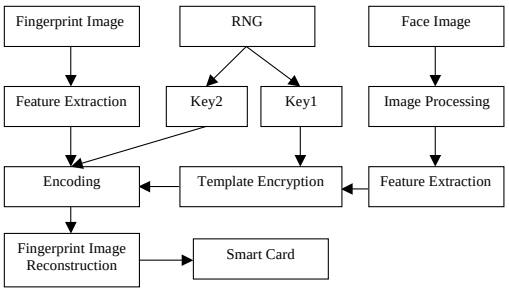

Fig. 1 Encoding Process

3. The extracted face feature is framed into template and stored in database.

4. For security reasons the face template is encrypted. Security here concerns with avoidance in hacking, copying or replacing encoded templates from the fingerprint template without a valid decryption key.

5. This encryption process is done with the help of RNG which generates random numbers.

6. The random number generated is used to encrypt the face template in the form of

$$W(n) = \sum_{i=1}^{n} b(n) \oplus c(n)$$

where W(n) → encrypted face template in binary form
n → size of the template
b(n) → normalized face template
c(n) → random number generated by RNG
⊕→XOR operation

7. Encrypted face template W(n) is encoded into the feature of fingerprint using Discrete wavelet transform technique.
8. Embedding and secret key generation is done as discussed in the following section.

D. Embedding encrypted face template

The following conditions are analyzed for fixing the values of flag.
For values
α → encoding / embedding strength
$K_{i,j}$ → selected pixel value
$M_{i,j}$ → Mean value.
$W_{i,j}$ →Transformed encrypted binary template
$F_{i,j}$ → Flag raised.

Condition 1:
If (($K_{i,j} > M_{i,j}$) && ($W_{i,j} = 1$)) then
$K'_{i,j} = K_{i,j} (1 - \alpha W_{i,j})$
$F_{i,j} = 0$

Condition 2:
If (($K_{i,j} > M_{i,j}$) && ($W_{i,j} = 0$)) then
$K'_{i,j} = K_{i,j} (1 - \alpha)$
$F_{i,j} = 1$

Condition 3:
If (($K_{i,j} < M_{i,j}$) && ($W_{i,j} = 1$)) then
$K'_{i,j} = K_{i,j} (1 + \alpha W_{i,j})$
$F_{i,j} = 2$

Condition 4:
If (($K_{i,j} < M_{i,j}$) && ($W_{i,j} = 0$)) then
$K'_{i,j} = K_{i,j} (1 + \alpha)$
$F_{i,j} = 3$

E. Decoding and Authentication

Figure 2 shows the steps that are taken for this decoding and description of each step follows

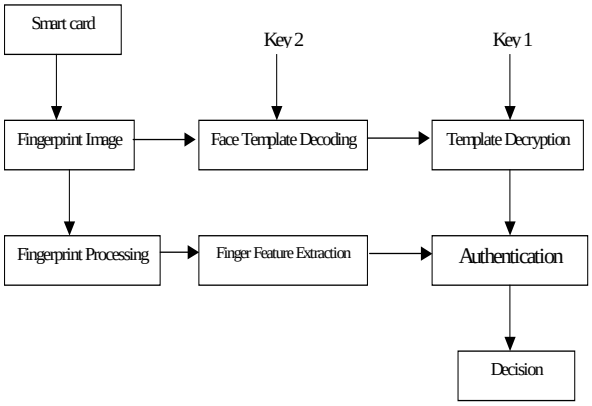

Fig. 2 Decoding Process

1. The face and fingerprint images are captured at the time of verification.

2. Simultaneously the fingerprint from the token is scanned.

3. The fingerprint image is transformed using second level discrete wavelet decomposition(IWDT).

4. The previous step results in decomposing and extracting data from LH2,HL2 & HH2 subbands.

5. The embedded location is identified using the same key used in the hiding procedure discussed in section II-D.

6. After extracting the face template from fingerprint image decryption is done using the secret key as

$$b(n) = \sum_{i=1}^{n} W'(n) \oplus c(n)$$

7. Now the extracted face and fingerprint template are

$$FP_M = \left(\sum_{i=1}^{N} b'(n) \oplus b(n) \right) \Big/ n$$

$$F_M = \left(\sum_{i=1}^{N} f'(n) \oplus f(n) \right) \Big/ n$$

8. The matching score is developed as

$$S = \alpha F_M + (1 - \alpha) FP_M$$

Where $\alpha \in [0,1]$.

3. Conclusion

Experiments are to be conducted in real time for fingerprint and face data collection. Since the accuracy of data raises with the number of dataset , the dataset is expected to be of huge number. This dataset of fingerprint and face images are to be collected from students of SCSVMV university. For much clarity in face images they are to be taken under different details with dark background. The performance of the template is to be calculated through:

$$PSNR(I,I') = 10\log_{10} \left[\frac{(\max I_{\forall(m,n)}(m,n))^2}{(1/N_I) \sum_{\forall(m,n)} (I'(m,n)-I(m,n))^2} \right]$$

Where I and I' are the original and encoded fingerprint. Amongst the attacks the proposed system is expected to produce 97% accuracy approximately as predicted from literature proofs. Also analysis is to be made on Incremental Weighted Average Sampling method for Face feature extraction.

4. Results and discussion

There are some attacks that may occur on image which are held as keys . Some of these attacks were tested to find the reliability of the system and are summarized as illustrated in the table 1.

Table 1 Reliablity on attacks of Proposed system

Attacks	PSNR(dB)	Accuracy(%)
Gaussian filter	28.59	91.001
Median Filtering	34.02	96.27
JPEG compression	23.74	94.86
Weiner Filter	35.78	95.98

This works presents a novel multimodal face and fingerprint biometrics authentication scheme on space-limited tokens as SMART cards and RFID which are the technologies to be included in the future main work. This sub work now proves its resistance to various attacks which proves its genuineness. This proposed work may be proceeded in the future with some other combination of biometrics traits like Iris, Retina, Gait, Signature, Keystroke. etc.,

References

[1] M.K.Khan and J.Zhang. Multimodal face and fingerprint biometrics authentication on space – limited tokens.Neurocomputing Vol :71(2008) Pg:3026 – 3031..
[2] E.C.Chang and Q.Li. Hiding secret points amidst chaff. Eurocrypt, Vol : 4004 of LNCS Pg –59-72.
[3] A.Teoh, D.Ngo and A.Goh. Personalised cryptographic key generation based on face hashing. Computers and security, Vol:23(2004), 606-614.
[4] A.K.Jain, S.Prabhakar,L.Hong, A multichannel approach to fingerprint classification ,IEEE trans. Pattern Anal. Mach. Intell.vol: 21(1999)pg:348 – 359.
[5] F.Song, H.Liu,David Zhang,J.Yang , A Highly scalable incremental facial feature extraction method, Neurocomputing vol:71(2008) pg:1883-1888.
[6] http://www.cryptosys.net - RNG.

Author Details

B.Prasanalakshmi is a faculty member in the Department of Computer Science and Engineering at Sri Chandrasekharendra Saraswathi Viswa Mahavidhyalaya , Kanchipuram. She receives her Master Degree and Master's degree in Philosophy from Bharathidasan University in 2001. She is undergoing her Ph.D in Computer Science from Bharathiyar University, Coimbatore ,India . Her research interests include Cryptography, Multimodal Biometrics and Image processing.

Kannammal Sampath is a faculty member in the Department of Computer Technology and Applications in Coimbatore Institute of Technology, Coimbatore, India. She received her Master's Degree from the Indira Gandhi National Open University, India in 2001. She received her PhD in Computing Sciences from VIT University, Vellore, India in 2007. Her research interests include electronic business, agent technology and web services. She has published papers in the following: *International Journal of Electronic Business*, *Journal of Computer Science*, *Pacific Asian Journal of Mathematical Sciences*, *Academic Open Internet Journal* and *IEEE Computer Society*.