Journal of Korea Multimedia Society Vol. 13, No. 6, JUNE 2010(pp. 875-883)

# Secure Biometric Hashing by Random Fusion of Global and Local Features

Yang Ou[†], Kyung-Hyune Rhee[††]

## ABSTRACT

In this paper, we present a secure biometric hashing scheme for face recognition by random fusion of global and local features. The Fourier-Mellin transform and Radon transform are adopted respectively to form specialized representation of global and local features, due to their invariance to geometric operations. The final biometric hash is securely generated by random weighting sum of both feature sets. A fourfold key is involved in our algorithm to ensure the security and privacy of biometric templates. The proposed biometric hash can be revocable and replaced by using a new key. Moreover, the attacker cannot obtain any information about the original biometric template without knowing the secret key. The experimental results confirm that our scheme has a satisfactory accuracy performance in terms of EER.

**Key words:** Biometric Hashing, Multi-biometrics, Feature Fusion

## 1. INTRODUCTION

Cancelable biometrics are proposed to protect template privacy, in which the biometric data are firstly one-way transformed into cancelable templates by using random tokens [1-3]. When the biometric template is compromised, a different token is selected to generate another template. The difficulty of this kind of approaches is the feature extraction with high accuracy performance after the non-invertible transformations, since the feature sets may be destroyed after the transformation. Teoh, et al. proposed a Biohashing algorithm to project the biometric feature set into random orthogonal matrices and generate binary biometric hash codes. This algorithm is applied to several different biometric traits [5-8]. However, the good performance of the scheme is evaluated under the assumption that the secret key is not known by an unauthorized user, which is heavily impractical [4-5].

The biometric hashing has similar properties on security viewpoints as traditional cryptographic hash functions such as one-wayness and collision-freeness. However, comparing to the traditional cryptographic hash functions, a biometric hash has a lighter property of collision-freeness due to intrinsic redundancy of image. More detailed description on the security requirements for biometric hash is given in the next section. A biometric hash is a compact representation used to recognize and verify the validity of biometric inputs. The randomness should be introduced in the hash value by using a secret key, in order to ensure that an unauthorized user cannot forge a valid hash of the template without the key. Unlikely the traditional hash, a biometric hash captures the essential perceptual attributes of the input

※ Corresponding Author : Kyung-Hyune Rhee, Address: (608-737) Daeyeon 3-dong, Nam-gu, Busan, Korea, Tel: +82-51-626-4887, FAX : +82-51-626-4887, E-mail : khrhee@pknu.ac.kr
Receipt date : Jan. 11, 2010, Revision date : Mar. 15, 2010
Approval date : Apr. 13, 2010
[†] Department of Information Security, Pukyong National University
(E-mail: ouyang@pknu.ac.kr)
[††] Department of IT Convergence and Application Engineering, Pukyong National University
※ This work was supported by the Pukyong National University Research Fund in 2009(PK-2009-50).

template. An ideal biometric hash function should be robust enough against intra-user variance, whereas the sensitivity to inter-user variance should be also ensured.

On the other hand, face recognition is one of the most significant research topics in biometric authentication systems. While the face perception can be easily changed due to different expressions, lights and various poses. Several approaches are proposed to combine global and local features to achieve higher verification performance [6-8], where the security and privacy issues are not involved in these schemes.

### 1.1. Contribution and Organization

In this paper, in order to achieve a good accuracy performance, as well as ensuring the security of biometric templates, we propose a secure biometric hashing scheme by random fusion of global and local features. The proposed scheme utilizes Fourier-Mellin transform and Radon transform to extract global and local features, respectively. Both global and local features are captured by using secret keys and actually constructed as hash values. The key injection in each feature generation procedure ensures that the attacker cannot obtain any original biometric information even features are lost before fusion. The final hash, i.e. the fusion hash, is generated by key-based random weighting sum rule which introduces more confusions in our biometric hashing scheme. We simulate the scheme and the results confirm that the proposed secure biometric hashing obtains a high accuracy performance.

The rest of the paper is organized as follows. Section II provides the requirements of biometric hash, the backgrounds of Fourier-Mellin Transform and Radon transform. In Section III, the proposed secure biometric hashing scheme is introduced in detail. Experimental results are presented and analyzed in Section VI. Finally, we conclude the paper in Section V.

## 2. PRELIMINARY

### 2.1. Requirements of biometric hash

An biometric hash should capture the essential attributes of the image so that insignificant changes to the human eyes will not substantially alter the hash value. The following notations are used to describe the requirements of biometric hashing:

$X$: the input image;

$X_s$: a similar version of X distorted under content preserving operations (CPOs);

$X_d$: a different version of X tampered under content changing operations (CCOs);

$k$: a key involved in biometric hash generation;

$\psi(\bullet)$: an biometric hash function;

$P(\bullet)$: a certain probability;

$\theta_1$, $\theta_2$: two given parameters where $\theta_1$, $\theta_2(0,1)$;

$\tau$: a given threshold.

Generally, a good biometric hash should satisfy the following requirements:

(1) Randomization (Unpredictability):

$$P(\psi(X,k)=h)\approx\frac{1}{2^q},\forall\, h\in 0,1^q$$

where q is the length of the binary hash sequence, This property indicates that with a secret key k varying in an available range, the biometric hash value should be approximately uniformly distributed among all possible q-bit outputs.

(2) Robustness against CPOs:

$$P(\parallel\psi(X,k)-\psi(X_s)\parallel<\tau)\geq 1-\theta_1$$

for a given $\theta_1$ and predefined $\tau$. $X_s$ is a perceptually similar or identical image of $X$. the hash value of $X_s$ should be close to the hash of $X$ by using same $k$.

(3) Discrimination to CCOs:

$$P(\parallel\psi(X,k)-\psi(X_d,k)\parallel>\tau)\geq 1-\theta_2$$

for a given $\theta_2$ and predefined $\tau$. $X_d$ is a perceptually different image from $X$. This property

implicates that a good biometric hash function should be discriminative to perceptual different images.

(4) Onewayness:

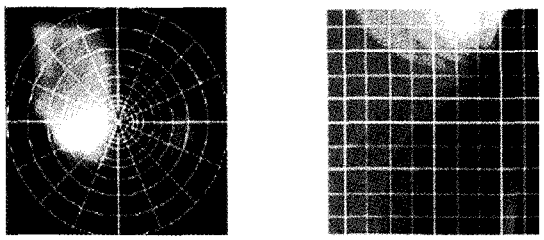
Given the hash value $h$ and hash function $\psi(X,k)$, it is difficult or impossible to get information related to original $X$.

(5) Compactness:

On the premise of satisfying the above properties, the hash sequence should be as short as possible to save on storage space.

### 2.2. Invariance of Fourier-Mellin Transform

The Fourier-Mellin Transform is widely used for image recognition, watermarking, object matching and image registration, because its resulting spectrum is invariant in rotation, translation and scale [9].



(a) Cartesian Coordinate (b) Log-polar Coordinate

Fig. 1. Coordinate transformation.

To implement the Fourier-Mellin Transform, an image is firstly transformed into frequency domain by Discrete Fourier Transform. And then the frequency coefficients are projected onto the log-polar plane by the coordinate transform as shown in Figure 1. The Fourier transform is translation invariant, whereas the log-polar transformation can be used to describe both rotation and scaling as a shift. Therefore, when log-polar transform is used on a Fourier image, which is called Fourier- Mellin Transform, we can get rotation, scale and translation invariance. More details can be referred in [10].

### 2.3. Radon Transform

The Radon transform [11] of a two-dimensional (2-D) function f(x,y) is defined as

$$P(t,\theta)=\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f(x,y)\delta(t-x\cos\theta-y\sin\theta)dxdy \qquad (1)$$

where t is the perpendicular distance of a straight line from the origin O (see Figure 2), $\theta$ is the angle between the distance vector and x-axis, i.e. $\theta\in[0,\pi)$.

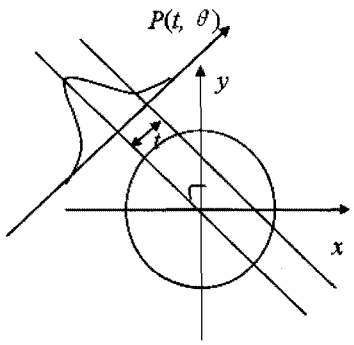



Fig. 2. Radon transform of a 2-D function f(x,y).

The Radon transform has useful properties about translation, rotation and scaling as outlined in Equation (2)-(4).

Translation:

$$R(t,\theta)f(x-x_0,y-y_0)=P(t-t_0,\theta) \qquad (2)$$

Rotation by $\psi$ :

$$R(t,\theta)f(x\cos\theta+y\sin\theta,-x\cos\theta+y\sin\theta)=P(t,\theta+\psi) \qquad (3)$$

Scaling :

$$R(t,\theta)f(\frac{x}{\lambda},\frac{y}{\lambda})=\lambda P(\frac{t}{\lambda},\theta) \qquad (4)$$

Here, $P(t,\theta)$ is the Radon transform of $f(x,y)$, $t_0=x_0\cos\theta+y_0\sin\theta$, $\lambda$ is the scaling factor and $\psi$ is the rotation angle.

## 3. PROPOSED BIOMETRIC HASHING SCHEME

In this section, we present the proposed biometric hashing scheme for secure face recognition. As we introduced before, the difficulty of face recognition

is caused by the sensitivity to intra-user variance, since the face perception can be easily changed to different facial expressions and poses even from the same individual. Therefore, enlargement of the robustness against intra-user variance is guile important on the condition without sacrifice of the discrimination to different faces.

The Fourier-Mellin transform is robust to rescaling, rotation and translation operations. We exploit it to generate global face features, which leads to the scheme resistant against intra-user variance. On the other side, the local features are captured from image blocks by using Radon transform and 1-D DCT. The details of biometric information are presented in local features. During the feature generation, secret keys are involved in order to randomize biometric information and make the template replaceable.

Figure 3 illustrates the coding pipeline of our scheme. The global and local hashes are firstly generated independently, and then randomly fused to form the final biometric hash. During the hash generation, a fourfold key is used to secure and randomize the biometric template. The scheme includes three steps: (1) Global hash generation; (2) Local hash generation; (3) Hash fusion.

### 3.1 Global Hash Generation

The Fourier-Mellin transform is widely used in feature extraction, watermarking and robust image hashing, due to its robustness against 2-D geometric transforms. Here we employ a popular image hashing scheme from [10] to generate the global biometric hash.

The face image $I(x,y)$ is firstly Fourier transformed into frequency domain. And then the frequency coefficients are mapped into log-polar coordinate $I(\rho_i,\theta_j)$ with size $(n_\rho,n_\theta)$, as shown in Figure 4, where $n_\rho$ and $n_\theta$ are the desired size of the transformed image. Along $\theta$-axis, we calculate the random weighted sum and obtain the $i$ th global hash value:

$$h_{G_i} = \sum_{j=0}^{n_\theta} \alpha_{A_{ij}} |I_{(\rho_\theta \theta_j)}|$$

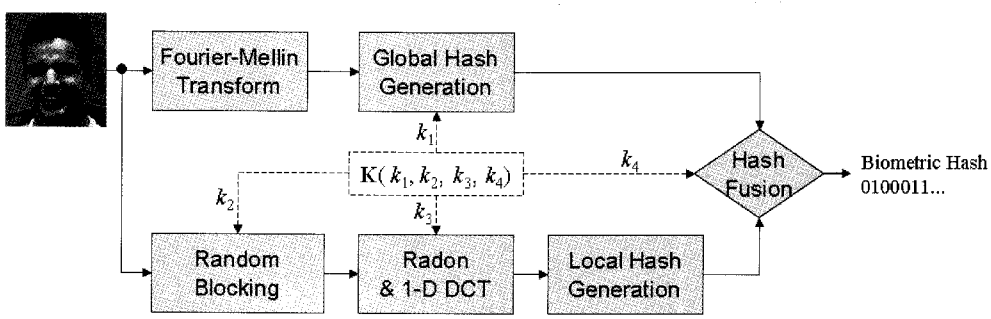



Fig. 3. Overview of the proposed biometric hashing scheme.

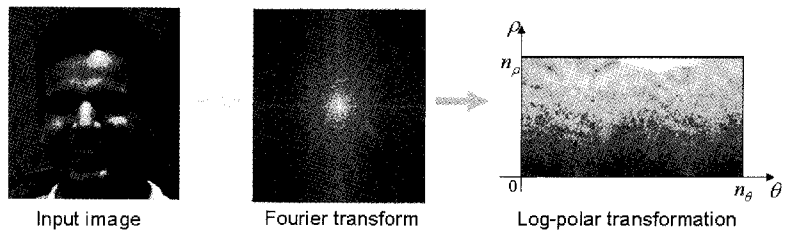



Fig. 4. Global hash generation.

where $\{\alpha_{\rho_{ij}}\}$ are pseudorandom weighting numbers which are generated by the secret key $k_1$ to ensure that the attacker can not use fourier coefficients to reconstruct the input image. The final global hash is denoted as $h_G(k_1)=(h_{G_1},h_{G_2},...,h_{G_{n_\rho}})$, where $n_\rho$ is the number of components in the hash vector.

### 3.2 Local Hash Generation

The local hash aims to capture the detailed local informations from biometric images, while the security should be also kept during hash generation. Generally, the local information is generated from regular blocks in the image, which can be easily guessed by the attacker. Here we randomly partition the image into overlapping rectangular blocks and extract features from each block by using Radon transform and 1-D DCT. The main procedures are illustrated in Figure 5.

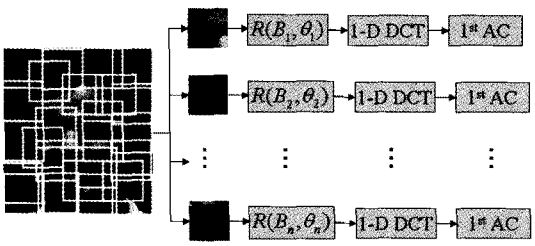



Fig. 5. Local hash generation.

Before feature extraction, two keys $(k_2,k_3)$ are firstly defined, where $k_2$ is used to randomly partition the original image into $n$ random blocks $B_i$ with size $p\times p$ and $k_3$ is used to generate $n$ random degrees $\theta_i$, i.e. $n$ random directions, for Radon transform. The above randomizations are denoted as:

$$B(k_2)=(B_1,B_2,...,B_i,...,B_n)$$
$$\Theta(k_3)=(\theta_1,\theta_2,...,\theta_i,...,\theta_n)$$

Note that the blocks are overlapped each other in order to make more confusions. For the random block $B_i$, the details of feature extraction are given as followings:

(1) Perform Radon projection on the random direction $\theta_i$. Thus, for each block, one Radon vector is obtained with its corresponding direction;

(2) Delete all zero values at the two boundaries of the Radon vector. This will remove the redundancy data generated by rotation or shift;

(3) Apply 1-D DCT on the projection to derive the frequency features for the Radon space;

(4) Select the second DCT coefficient, i.e. the first AC coefficient as the feature coefficient of the corresponding projection, since it contains the most stable energy when the input image is affected by different incidental factors.

In fact, one block is compacted into only one feature coefficient. Therefore, for $n$ blocks, we get totally $n$ AC coefficients which compose the local hash vector $h_L(k_2,k_3)=(h_{L_1},h_{L_2},...,h_{L_n})$.

### 3.3 Hash Fusion

The final stage of the proposed scheme is the hash fusion. In multi-biometrics, there are two typical combination ways to fuse biometric features. One is simply concatenating two features, and the other one is the sum rule by fixed weight values. However, under both two method, the attacker can directly classify each features and recover the original biometric data.

In order to introduce more randomness, we propose a random weighting sum rule to combine the global and local hashes. A precondition of our random fusion is that the number of the components of both global and local hash vectors should be the same, i.e. $n_\rho=n$. Following, a random weights sequence are generated by secret key $k_4$, denoted as $w(k_4)=(w_1,w_2,...,w_n)$. And then, the two hash vectors are combined as:

$$h(k_4)=(h_1,h_2,...,h_n)=w\ \cdot h_G+(1-w)\ \cdot h_L$$

where $1=(1,1,...,1)_n$ and $w$ is a uniformly distributed random floating number sequence in the range (0,1). In detail, the elements in the fused hash h can be calculated as:

$h_i = w_i \times h_{G_i} + (1-w_i) \times h_{L_i}$, for $i = 1,2,...,n$

In our scheme, all hash vectors are post-processed by $q$-bit quantization and finally represented as a binary form for authentication, transmission or storage. Therefore, the length of the proposed biometric hash is $n \times q$ bits.

## 4. Experimental Evaluations

### 4.1 Experimental Environment

We test our scheme on the Essex face94 database provided by the vision group of Essex university [12]. The database is taken from the video sequences' frames which consist of various expressions, illumination conditions, angles, age and sex. Some of them are wearing glasses and beards. Figure 6 shows some examples of face images from Essex database. There are 152 individuals and each of them has 20 face images, leading to total 3040 images. The size of each face images are 180*200. The normalized Hamming distance is used to measure the similarity of two binary hash codes, whereas the Euclidean distance is used to measure two quantized but non-binary hash vectors.

The performance of the our hashing scheme is evaluated by using three performance criteria: False Accept Rate (FAR), False Reject Rate (FRR) and Equal Error Rate (EER). EER is the rate at which both FAR and FRR are equal. The value of EER can be easily obtained from Receiver Operating Characteristic (ROC) curves. In general, the lower the EER, the more accurate of the authentication systems. We construct genuine pairs and imposter pairs from the database. The genuine pairs are composed of any two face images from the same individual, leading to 28880 pairs $(152 \times (20 \times 19)/2)$ and the corresponding FRR is recorded. For the imposter pairs, firstly two images of each individual are randomly selected. And then each of both images is compared with all other individuals' two images, leading to 22952 imposter pairs $(2 \times (151 \times 152)/2)$ and the corresponding FAR is recorded. Note that all experimental results are tested under the assumption that the attacker (or the imposter) knows correct keys of their corresponding biometric images, which is the worst hypothesis in [5].

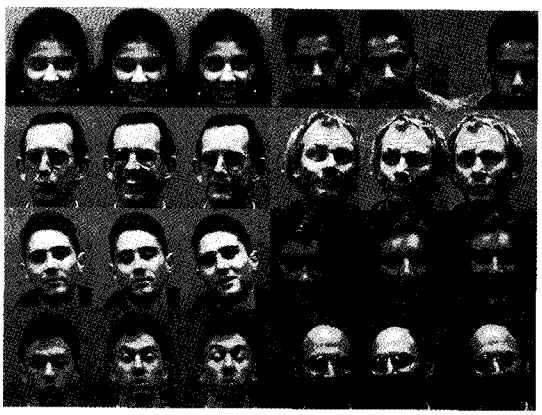


Fig. 6. Examples of face images from the database.

### 4.2 Experimental Results

The performance improvement is firstly evaluated by comparing the error rates of global hash, local hash and fusion hash, respectively. In global hash generation, we set $n_\theta = 90, n_\rho = 48$. In local hash generation, we set the block size $p = 32$, the number of blocks $n = n_\rho = 48$ and $q = 8$ bits quantization. Hence the length of final hash is 384 bits. The normalized Hamming distance is used as the measure of metric. The FAR and FRR are recorded by setting gradually increasing thresholds. Their ROC curves are drawn in Figure 7. While the curve which is nearest to coordinate axis implies the highest accuracy. We find that the fusion hash achieves the better results than other two hashes. In Figure 7, we obtain the EER values of the global, local and fusion hashes which are 0.1135, 0.1278, and 0.0871, respectively, where the fusion hash leads to 23.26% accuracy improvement over the global hash and 31.85% over the local hash.

The global and local hashes reflect the coarse and detail information of biometric templates,

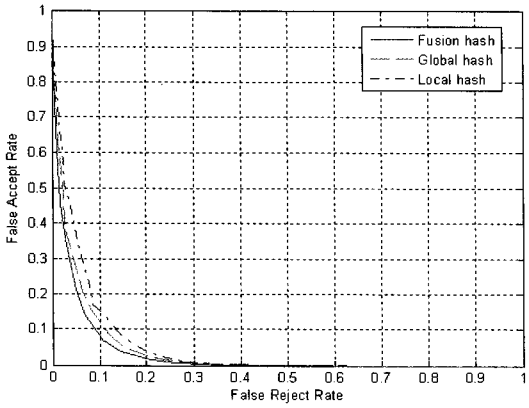



Fig. 7. The ROC curves of the global, local and fusion hashes.

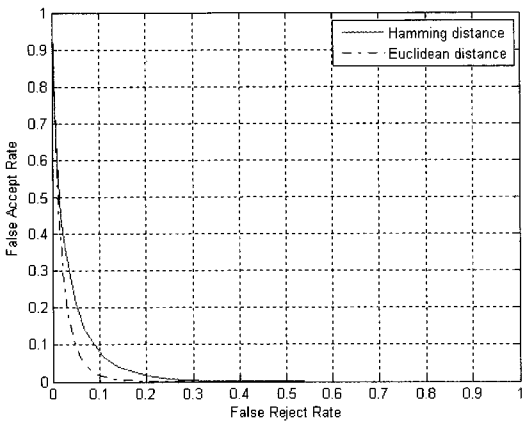



Fig. 8. The ROC curves of fusion hashes by using Hamming distance and Euclidean distance.

respectively. Only usage of the global hash reduces the sensitivity to inter-user variance, whereas additional usage of the local hash increases the sensitivity to intra-user variance. Based on the above experimental results, it can be confirmed that a good tradeoff between the sensitivities to inter- and intra-user variances is obtained by using our fusion hash.

The binary representation of hash vectors is convenient for hash storage or transmission and many existing algorithms employ Hamming distance to compare hashes. However, direct matching of two binary hash may not be suitable since the binarization may generate bit errors and affects the results of Hamming distance. For instance, the binary code of 32 and 31 are 100000 and 011111, while only 1-bit difference will cause 6-bit difference after measuring by Hamming distance. Therefore, we test the performances in the following two cases: comparing binary hash codes by using Hamming distance and comparing hash vectors by using Euclidean distance. The two ROC curves are drawn in Figure 8. Obviously, comparison of the hash vectors by using Euclidean distance obtains a much better accurate performance. Its EER is 0.0609 which leads to about 30% accuracy enhancement.

Different setting of parameters may affect the accuracy performance. In our scheme, the block size p of random partitioning in local hash generation and the hash length n are directly related to the hash value. Here we test their effects on the accuracy performance. The different values and testing results are shown in Table 1. We observe that when $p$=48, $n$=32, the EER is the lowest. That because when smaller block size and larger block number are used, the hash would be sensitive to intra-variance, i.e. two input images of different facial expressions from the same individual may be regarded as different persons. On the other hand, when larger block size and smaller block number are used, the hash would be insensitive to inter-variance, i.e. two input images from two different individuals may be accepted as same person. Based on our simulation, we suggest that the size of each block should be 4% ~ 7% of the whole image size. And $n$ satisfies that $h \times w < n \times p \times p \leq 3 \times h \times w$, where $h \times w$ is the size of the input image. Figure 9 depicts the FAR and FRR of the fusion hash when using $p$=48, $n$=32.

Based on the above results, it is obtained that

Table 1. The EER values by using different parameters

| Parameters | $p$=32 $n$=48 | $p$=48 $n$=32 | $p$=64 $n$=16 |
|---|---|---|---|
| EER | 0.0609 | 0.05901 | 0.06576 |

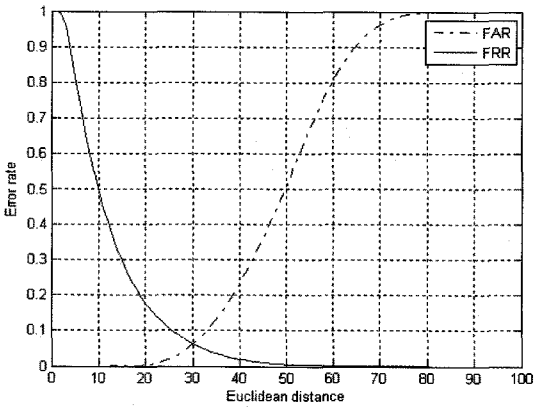



Fig. 9. The FAR and FRR of fusion hash when using p=48, n=32.

by properly setting parameters, the EER can be low as 0.05901, where all results are obtained in the worst hypothesis, i.e. the attacker knows the secret information embedded in biometric feature generation. However, in the same hypothesis, we observe that the accuracy performances from other schemes [3,13,14] cannot be as satisfactory as ours. It is worthy to note that the zero EER in [13], which is the perfect performance, is gained under the assumption that the attacker does not know any secret keys during hash generation, while this assumption is not common and just a special case.

## 5. Conclusion

In this paper, we have proposed a secure biometric hashing scheme by combining the global and local features which are used for coarse and detail representations of biometric data. Both feature sets are robustly extracted and protected by secret keys. The fusion of features is performed by random weighting sum rule to produce the final hash code. By fusing both global and local hashes, the proposed fusion hash provides a good tradeoff between the inter- and intra-user variances. Moreover, the conjunction with the fourfold key provides the cancelability of biometric templates and also protects their privacy. We also demonstrated that a high verification accuracy can be obtained by properly selecting the measure metric and parameters via ROC curves and EER.

## REFERENCES

[1] R. M. Bolle, J. H. Connell, and N. K. Ratha, "Biometric perils and patches," *Pattern Recognition*, Vol.35, No.12, pp. 2727-2738, 2002.

[2] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating cancelable fingerprint templates," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol.9, No.4, pp. 561-572, 2007.

[3] M. A. Dabbah, S. S. Dlay, and W. L. Woo, "Secure face biometric verification in the randomized radon space," International Conference on Multimedia & Expo (ICME 2008), pp. 909-912, 2008.

[4] A. Kong, K. H. Cheung, D. Zhang, M. Kamel, and J. You, "An analysis of biohashing and its variants," *Pattern Recognition*, Vol.2006, No.39, pp. 1359-1368, 2005.

[5] A. Lumini and L. Nanni, "An improved BioHashing for human authentication," *Pattern Recognition*, Vol.2007, No.40, pp. 1057-1065, 2007.

[6] Y. Fang, T. Tan, and Y. Wang, "Fusion of global and local Features for face verification," International Conference on Pattern Recognition, pp. 382-385, 2002.

[7] J. Huang, P. C. Yuen, J. H. Lai, and C. Li, "Face recognition using local and global features," *EURASIP Journal on Applied Signal Processing*, Vol.2004, No.4, pp. 530-541, 2004.

[8] Y. Su, S. Shan, X. Chen, and W. Gao, "Hierarchical ensemble of global and local classifiers for face recognition," International Conference on Computer Vision, pp. 1-8, 2007.

[9] J. J. K. O'Ruanaidh and T. Pun, "Rotation, scale and translation invariant digital image watermarking," IEEE International Conference

of Image Processing, pp. 536-539, 1997.

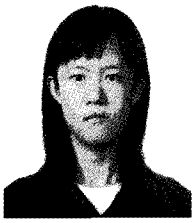
[10] A. Swaminathan, Y. Mao, and M. Wu, "Robust and secure image hashing," *IEEE Transactions on Information Forensics and Security*, Vol.1, No.2, pp. 215-230, 2006.

[11] M. A. Fiddy, "The Radon transform and some of its applications," *Journal of Modern Optics*, Vol.32, No.1, pp. 3-4, 1985.

[12] Essex Face Database, http://cswww.essex.ac.uk/mv/allfaces/index.html.

[13] A. B. J. Teoh and D. C. L. Ngo, "Cancelable biometrics featuring with tokenised random number," *Pattern Recognition Letters*, Vol. 2005, No.26, pp. 1454-1460, 2004.

[14] C. Karabat and H. Erdogan, "A cancelable biometric hashing for secure biometric verification system," *International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, pp. 1082-1085, 2009.



**Yang Ou**

Received the B.E. degree in computer science from University of Science and Technology Liaoning, China, in 2004 and M.E. degree from Gyeongsang National University, Korea, in 2006. She received a Ph.D in the Department of information security, Pukyong National University, Korea, in 2010. Her research interests include image processing, image encryption and authentication

**Kyung-Hyune Rhee**

received his M.S. and Ph.D. degrees from Korea Advanced Institute of Science and Technology(KAIST), Daejon Korea in 1985 and 1992, respectively. He worked as a senior researcher in Electronic and Telecommunications Research Institute(ETRI), Daejon Korea from 1985 to 1993. He also worked as a visiting scholar in the University of Adelaide in Australia, the University of Tokyo and Kyushu University in Japan, and University of California at Irvine in USA, respectively. He has also worked for Colombo Plan Staff College of Technician Education (CPSC) in Manila, Philippines as a director of Information and Communication Technology during 2002 through 2003. He is currently a professor in the Department of IT Convergence Applications in Pukyong National University, Republic of Korea. His research interests are related to cryptography and its applications, wireless communication security and multimedia encryption and authentication.