Robust Memory-Efficient Data Level Information Fusion of Multimodal Biometric Images

Afzel Noore [*], Richa Singh and Mayank Vatsa

Lane Department of Computer Science and Electrical Engineering
West Virginia University, Morgantown, WV 26506.

Abstract

This paper presents a novel multi-level wavelet based fusion algorithm that combines information from fingerprint, face, iris, and signature images of an individual into a single composite image. The proposed approach reduces the memory size, increases the recognition accuracy using multimodal biometric features, and withstands common attacks such as smoothing, cropping, JPEG 2000, and filtering due to tampering. The fusion algorithm is validated using the verification algorithms we developed, existing algorithms, and commercial algorithm. In addition to our multimodal database, experiments are also performed on other well known databases such as FERET face database and CASIA iris database. The effectiveness of the fusion algorithm is experimentally validated by computing the matching scores and the equal error rates before fusion, after reconstruction of biometric images, and when the composite fused image is subjected to both frequency and geometric attacks. The results show that the fusion process reduced the memory required for storing the multimodal images by 75%. The integrity of biometric features and the recognition performance of the resulting composite fused image is not affected. The complexity of the fusion and the reconstruction algorithms is $O(n \log n)$ and is suitable for many real-time applications. We also propose a multimodal biometric algorithm that further reduces the equal error rate compared to individual biometric images.

Key words: Biometric information fusion, multimodal biometrics, wavelet transform, identity verification.

[*] Corresponding author. Tel.: +1-304-293-4821 ext. 2547. Fax: +1-304-293-8602. *E-mail addresses:* afzel.noore@mail.wvu.edu (A. Noore), richas@csee.wvu.edu (R. Singh), mayankv@csee.wvu.edu (M. Vatsa).

Preprint submitted to Elsevier Science *19 September 2005*

1 Introduction

A major motivation for using biometrics is the ability to authenticate the true identity of an individual [11]. It has been shown that some people have difficulty with fingerprint for enrollment or verification due to the inherent characteristics of their finger. Sometimes the problem is associated with noisy data from biometric sensors and environmental conditions. All these lead to an increase in false acceptance and false rejection rates. To overcome these problems, multimodal biometrics relies on more than one form of biometric data. An overview of the multimodal biometric algorithms is presented in [6,8,10]. A new fast approach of multi-biometrics based on retrieval and verification is presented in [6] and [8]. These algorithms first retrieve top matches using one biometric trait and then verify the individual among the top matches using another biometric trait. Although multimodal biometrics addresses many problems associated with single biometrics, a major issue arises with storing multiple biometrics of a large number of users. Using selected feature sets from individual biometric images can alleviate this problem; however the verification is constrained to a dedicated system and lacks interoperability.

In [22], four levels of biometric data fusion are described. They are raw data level fusion or image fusion, feature level fusion, match score level fusion and decision level fusion. In this paper, we present a novel approach for raw data level fusion which fuses the information from multiple biometric traits to generate a single composite image. The fusion algorithm is based on multi-level discrete wavelet transform. The advantages of the proposed approach are reduction in memory size, increase in recognition accuracy due to the use of multimodal biometrics, and resilience to common attacks such as smoothing, cropping, JPEG 2000 and filtering. The effectiveness of the algorithm is validated by comparing the verification performance of biometric images extracted from the composite fused image.

2 Proposed Algorithm for Fusion and Reconstruction of Biometric Images

The fingerprint, face, signature, and iris images represent the biometric of an individual. A multimodal system that uses these four biometric traits requires a large amount of memory for storage. A compact composite image is generated using the proposed fusion algorithm which retains the biometric features for matching purposes. Wavelets are used to decompose an image into different frequency components, and to analyze each component with a resolution matched to its scale. Discrete Cosine Transform (DCT) uses block based approach which makes it challenging to completely decorrelate the blocks at the boundaries of the image. In biometric images, any discontinuity due to artifacts can introduce false features or distort the already existing genuine features. For example biometric images such as fingerprint contain ridges and bifurcations, and are especially sensitive to blocking artifacts [17]. Any discontinuity due to artifacts introduces false minutiae points and lowers the recognition accuracy. Discrete Wavelet Transform (DWT) on the other hand, preserves different frequency information in a more stable form compared to DCT and allows good localization both in time and spatial frequency domain. Wavelet transformation splits the image into high frequency and low frequency components. The Wavelet Transform of 1D signal $f(t)$ can be written as,

$$\gamma(S,\tau) = \int f(t)\,\psi^{*}_{S,\tau}(t)\,dt \tag{1}$$

$$\psi_{S,\tau}(t) = \frac{1}{\sqrt{S}}\,\psi\left(\frac{t-\tau}{S}\right) \tag{2}$$

where $\psi_{S,\tau}(t)$ is the mother wavelet and S and τ represent the scaling and the translation factors respectively. The mother wavelet for DWT is expressed as,

$$\psi_{j,k}(t) = \frac{1}{\sqrt{S_0^j}}\,\psi\left(\frac{t-k\tau_0}{S_0^j}\right) \tag{3}$$

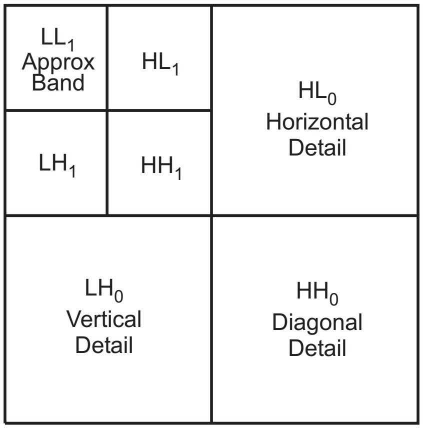

Fig. 1. Wavelet Decomposition

where j and k are integer values. Using the Inverse Discrete Wavelet Transform (IDWT), the original signal can be reconstructed as shown in Equation 4.

$$f(t) = \iint \gamma(S, \tau)\, \psi_{S,\tau}(t)\, d\tau\, dS \tag{4}$$

The DWT and IDWT for a two dimensional image is obtained by computing the one dimensional DWT and IDWT for each dimension separately, resulting in the pyramidal representation of an image. Fig. 1 shows the DWT representation of low-frequency components of an image in the approximation band, LL_1, and the high frequency components in the detail subbands.

2.1 Fusion of Information from Biometric Images

The proposed biometric data fusion algorithm uses the fingerprint, face, iris, and signature images of an individual as shown in Fig. 2 to generate a single composite multimodal biometric image. Fig. 3 shows the process of fusing biometric images to form a single image and is described as follows:

Step 1: The fingerprint image is decomposed to three levels using Daubechies 9/7 wavelet transform and the face, iris, and signature images are decomposed

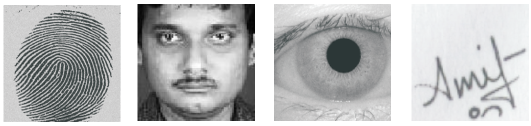

Fig. 2. Multimodal Biometric Images used by the Fusion Algorithm

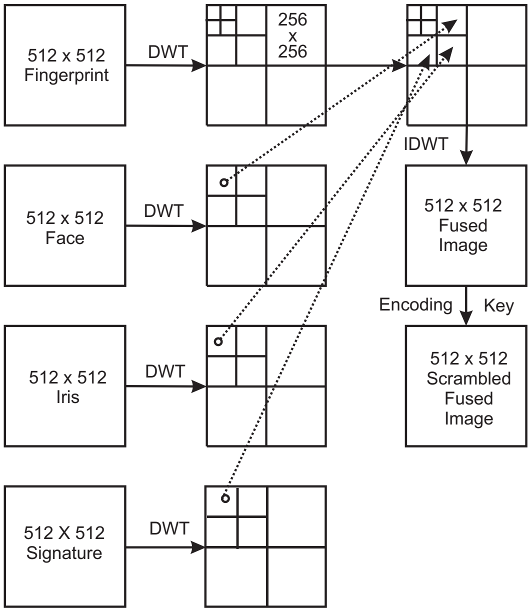

Fig. 3. Fusion of Information from Multimodal Biometric Images

to two levels. The additional level in the fingerprint image allows face, iris and signature images to be embedded so that the reconstruction can be performed with minimal error. Fig. 4 shows the wavelet decomposition of fingerprint, face, iris and signature images.

Step 2: The HL_1, HH_1 and LH_1 bands of fingerprint image are replaced by the approximation bands of the transformed face, iris, and signature images.

Step 3: IDWT is performed on the combined image to generate a single composite image with fingerprint as the base image and face, iris, and signature images embedded into it. After fusion, the memory required for storing the multimodal images is reduced by 75%.

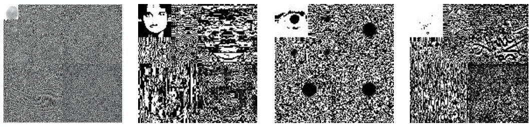

Fig. 4. Wavelet Decomposition of Fingerprint Face, Iris and Signature Images

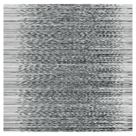

Fig. 5. Scrambled Multimodal Biometric Fused Image

Step 4: The fused multimodal biometric image is scrambled using a secret encoding key generated using Fibonacci Transforms [30]. The scrambled image shown in Fig. 5 does not resemble any of the original images but it retains the biometric characteristics needed for verification. This image can be safely transmitted on any network for authentication, if desired.

In the proposed fusion algorithm, we replace the HL_1 component of the fingerprint image by the LL_1 component of the face image. The HH_1 component of fingerprint image is replaced by the LL_1 component of the iris image, and the LH_1 component of the fingerprint image is replaced by the LL_1 component of the signature image. In this algorithm, the fingerprint image is chosen as the base image. However, any image can be chosen as the base image without affecting the overall performance.

2.2 Reconstruction of Original Biometric Images

Fig. 6 shows the block diagram for reconstructing the original fingerprint, face, iris, and signature images from the scrambled fused multimodal biometric image. The algorithm for retrieval is described below.

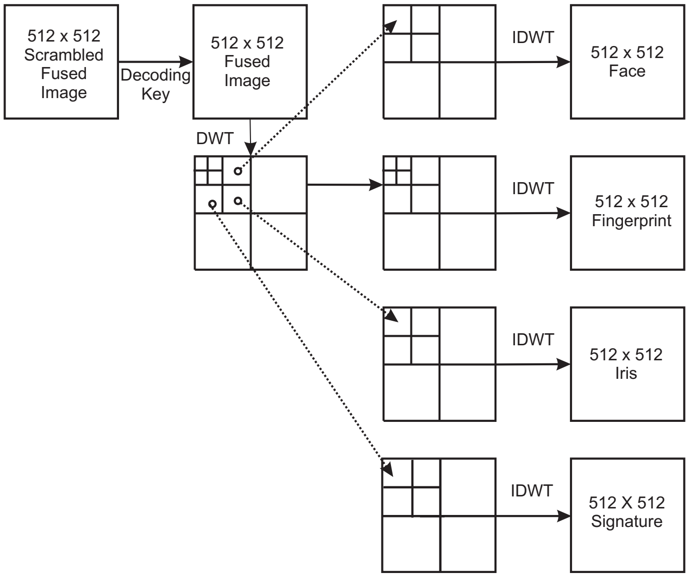

Fig. 6. Retrieval of Individual Biometric Images

Step 1: When reconstructing the original images to perform authentication, the scrambled fused image is descrambled using the decoding key [30].

Step 2: The image obtained after descrambling is decomposed into three levels using the same wavelet bases (Daubechies 9/7). The HL_1, HH_1 and LH_1 bands correspond to the approximation bands of face, iris and signature image respectively.

Step 3: All the four images are reconstructed by applying the inverse wavelet transform on these approximation bands with the other high level bands as zero (linear approximation). Fig. 7 shows the reconstructed fingerprint, face, iris and signature images.

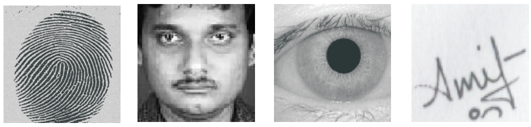

Fig. 7. Reconstructed Fingerprint, Face, Iris and Signature Images

In the fusion process, the fingerprint image is decomposed to three levels instead of two because the fingerprint image reconstructed from 3-level decomposition has better image quality. It has been shown that using a zero tree structure the third level contains information about the first and the second levels [14]. Experimentally, we verified that 3-level decomposition of a fingerprint image yields a better matching performance than 2-level decomposition. For 3-level decomposition, the Equal Error Rate (EER) for fingerprint is found to be 0.62% whereas for 2-level decomposition, it is 0.71%. The 3-level decomposition also makes the composite fused image resilient to attacks because the low and high frequency bands are more susceptible to attacks compared to the middle frequency bands.

2.3 Effect of Varying the Biometric Image Resolution on the Equal Error Rate

The proposed algorithm decomposes biometric images at different levels, which affects the resolution of the images. Due to the transformation and linear approximation, images are down-sampled and as a result we obtain low resolution images after fusion and reconstruction process. The effect of reducing the resolution of biometric images on the verification performance is next examined. Before fusion, the resolution of all images is 512 x 512. The effective resolution of the reconstructed face, iris and signature images is 128 x 128, while the effective resolution of the fingerprint image is 256 x 256. To study how the EER of each biometric trait changes with varying resolutions, the images are down-sampled from 512 x 512 to 32 x 32 in steps of two using wavelet transformation. The EER is calculated for each resolution using the verification algorithms described in Section 3. Fig. 8 shows the EER of each biometric trait at different resolutions. For each biometric trait, the EER remains fairly constant and the performance is not degraded when the images are down sampled from 512 x 512 to 128 x 128. Any further reduction in the resolution of the images increases the EER considerably. The performance deteriorates when these low resolution images are subjected to attacks. When the effective resolution is reduced to 64 x 64 and 32 x 32, the EER increases to 38% and 54% respectively, thereby rendering the composite image of little value for practical use.

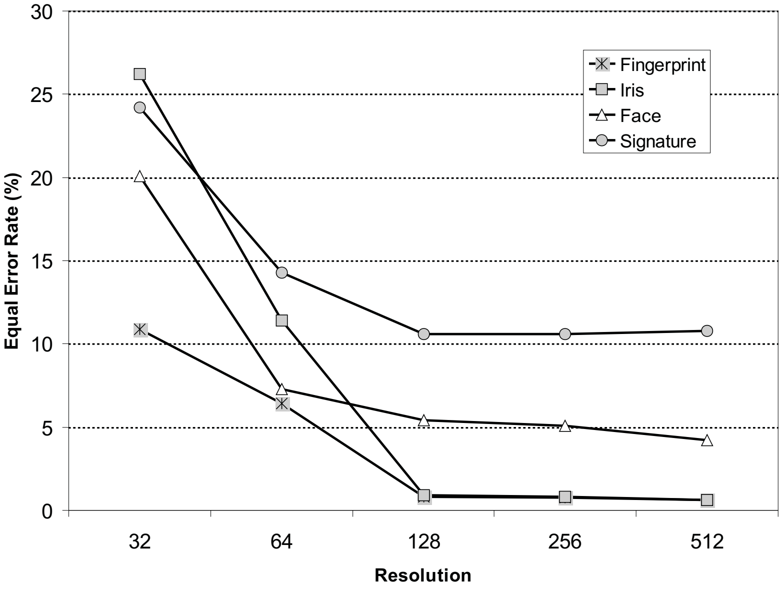

Fig. 8. Impact on Equal Error Rates with Varying Image Resolutions

2.4 *Computational Complexity of the Algorithm*

The computational complexity of the proposed algorithm depends on the discrete and inverse discrete wavelet transformation, replacement of approximation bands, and scrambling/descrambling process. For an image of size n x n, the computational complexity of applying DWT and IDWT is $O(n \log n)$, the replacement of approximation band has a complexity of $O(n/4)$, and the scrambling/descrambling has a complexity of $O(n)$. Thus the overall complexity of the fusion and the reconstruction algorithms is $O(n \log n)$. The fusion algorithm took 0.41 seconds to generate the composite biometric image on a computer with processing speed of 2.8 GHz. The reconstruction of individual biometric images from the composite image took approximately 0.45 seconds. This level of performance is attractive for many real-time applications.

3 Algorithms for Verifying the Integrity of Reconstructed Biometric Images

This section describes the fingerprint, face, iris, and signature algorithms used to verify the integrity of the reconstructed biometric images. The equal error rate for each individual algorithm is calculated to validate the fusion algorithm. We use an existing algorithm for fingerprint and propose new algorithms for face, iris, and signature verification. To show that the performance of fusion process is independent of the verification algorithms, we also included other standard algorithms [15,18,23].

3.1 Fingerprint Verification

The fingerprint verification is based on minutiae matching algorithm. To extract the minutiae from the fingerprint image, a ridge tracing minutiae extraction algorithm [12] is used. The extracted minutiae are then matched using a dynamic bounding box based matching algorithm [7]. The algorithm gives the matching score based on Equation 5.

$$MS(\mathit{finger}) = \left(\frac{MaxS}{MaxM}\right) \tag{5}$$

where *MaxS* is the maximum score among all the possibilities of the reference minutiae [7] and *MaxM* is the maximum number of minutiae in the fingerprint image. We use this matching score to compute the accuracy and determine the integrity of the extracted fingerprint image from the composite biometric image.

3.2 Face Verification

Existing face recognition algorithms require large amounts of memory and training data. We propose a new face recognition algorithm that is suitable for a low memory environment and uses fewer training data. The algorithm is based on the facial features extracted from the Gabor wavelet [5]. We use Gabor wavelet to extract the facial features from the face image treating it as a texture image and encoding it into the binary pattern [24]. In this process, face is detected from the image using the face detection algorithm described in [25]. The detected face is then converted into the polar coordinate system and convolved with the Gabor filters in frequency domain. The output is a complex valued matrix Z, which is the convolved form of face image. Phase quantization is applied on this convolved image using Equation 6.

$$face = \begin{cases} 1 & Re(Z) * Im(Z) \geq 0 \\ \\ 0 & Re(Z) * Im(Z) < 0 \end{cases} \tag{6}$$

where $face$ is the feature template obtained in the form of a binary template. An example of the face template is shown in Fig. 9. The image stored in the database is also convolved in a similar manner to generate the binary template which is then used for comparison.

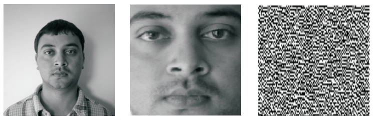

Fig. 9. Face Template using 2D Gabor Wavelets

The proposed recognition algorithm does not require a large dataset for training. Since the algorithm encodes only the phase information in the face template, it is invariant to changes in lighting. The Adaptive Hamming Distance matching algorithm [16] computes the matching score as

$$MS(\mathit{face}) = \left(1 - \frac{1}{N}\sum_{i=1}^{N} A_i \otimes B_i\right) \tag{7}$$

where A_i and B_i are the two templates to be compared, N is the number of bits represented by each template and $\otimes$ is the XOR operation. This XOR operation is performed by shifting bits from -8 to +8 in all directions enabling the algorithm to handle angular rotations of around 10^0.

3.3 Iris Verification

The proposed iris verification algorithm uses 1D log Gabor for feature extraction [28]. Iris images are first preprocessed to retain the region of interest and to remove the eyelids and eyelashes in the image [4,29]. The preprocessed iris image is convolved with 1D log Gabor wavelet to generate an iris template. In [1], log Gabor filters are used for natural textures which often exhibit a linearly decreasing log power spectrum. In the frequency domain, log-Gabor filter bank is defined as,

$$G_{ij}(\omega_r, \omega_\varphi) = G(\omega_r - \omega_{r_i^\alpha}, \omega_{\varphi_i^\alpha}) \tag{8}$$

where (r, φ) are polar coordinates, $\omega_{r_i^\alpha}$ is the logarithm of the center frequency at scale i, and $\omega_{\varphi_i^\alpha}$ is the j^{th} orientation [1]. $G(\omega_r, \omega_\varphi)$ is defined as,

$$G_{\omega_r,\omega_\varphi} = exp(\frac{\omega_r^2}{2\sigma_{ri}^2} - \frac{\omega_\varphi^2}{2\sigma_{\varphi j}^2}) \tag{9}$$

where σ_{ri}^2 and $\sigma_{\varphi j}^2$ are the Gaussian parameters. Similar to face template generation, a bitwise iris template is generated using the phase information of the iris image extracted from 1D log Gabor wavelet. An example of an iris template is shown in Fig. 10.

Fig. 10. Iris Template using 1D log Gabor

The iris matching score is calculated using,

$$MS(iris) = (1 - AHD_{iris}) \tag{10}$$

where AHD is the Adaptive Hamming Distance. This score is used to compute the iris recognition accuracy and to validate the functional integrity of the extracted iris image from the composite biometric image generated by the fusion algorithm.

3.4 Signature Verification Algorithm

The proposed signature verification algorithm uses 1D Gabor wavelet [5] for feature extraction [27]. Signature images are preprocessed using a low-pass filter to eliminate spurious noise inherent in the acquisition process [2]. For generating the Signature Code using 1D Gabor wavelet, the 2D signature pattern is decomposed into a number of 1D signals. Each 1D signal is then demodulated using 1D Gabor wavelet to extract its phase information. A 1D Gabor wavelet, with width parameter w and frequency parameter ν is defined as,

$$\psi(x) = w^{-1/2} e^{-\pi(x/w)^2} e^{i2\pi(\nu x)/w} \tag{11}$$

It is a complex function and its real part $\psi_R(x)$ and imaginary part $\psi_I(x)$ are given by,

$$
\begin{aligned}
\psi_R(x) &= w^{-1/2} e^{-\pi(x/w)^2} \cos 2\pi(\nu x/w) \\
\psi_I(x) &= w^{-1/2} e^{-\pi(x/w)^2} \sin 2\pi(\nu x/w)
\end{aligned}
\tag{12}
$$

After applying Gabor wavelet, phase information of the signature image is extracted and converted into the binary form using the demodulation process. The binary information is a bitwise template containing a number of bits of information called the Signature Code. Fig. 11 shows an example of a Signature Code.

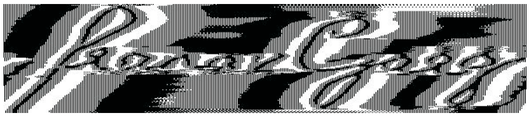

Fig. 11. Signature Code using 1D Gabor Wavelet

To determine the matching score,$MS(sign)$, the Hamming Distance HD_{sign} is calculated from Equation 13.

$$MS(sign) = (1 - HD_{sign}) \tag{13}$$

This score is used to calculate the recognition accuracy and serves as a metric to quantitatively verify the integrity of the extracted signature image from the composite fused image.

4 Experimental Results

The proposed biometric fusion algorithm is validated using the algorithms described in Section 3 and other well known algorithms described in the literature [15,18]. The experiment is performed using a multimodal database of fingerprint, face, iris and signature images. In addition, we included a commercial database with Sagem Morpho automatic fingerprint identification system [23], and other widely used databases in this research [3,19].

4.1 Description of Databases

The first set of experiments is performed using a multimodal database of fingerprint, face, iris, and signature images of 100 individuals. The multimodal database consists of seven images of each biometric for every individual. The size of all images is 512 x 512. The database is created in three different sessions with a time interval of four weeks each; three images of each biometric trait are captured in session one, two images in session two and the remaining two in session three. Frontal face images with around 10^0 of rotation are captured under varying lightning conditions and facial expressions. For preparing the database, fingerprint images are captured using the process described in [7] and iris images are captured using the process described in [3]. For preparing the signature database, the signatures are first collected on white paper and then scanned at 500 dpi. The three images of the first session are used for training purposes and the remaining four images of face, fingerprint, iris and signature from the last two sessions are used for testing. Fig. 12 shows an example of the multimodal database used in experiment.

The second set of experiments is performed using individual databases of fingerprint, face, iris and signature images. A database of 2.8 million fingerprints collected by law enforcement officials is used with Sagem Morpho's commercial automatic fingerprint identification system (AFIS) for fingerprint verification and computing the matching scores [23]. For face verification, the frontal and the semi-profile face images are selected from the FERET color face database [19]. The Local Feature Analysis [18] algorithm is used for verification to calculate the EER. For iris verification the CASIA iris image database [3] is used and the EER is calculated using the algorithm described in [15]. For signature verification, the signature image database and the signature recognition algorithm described in Section 3.4 is used.

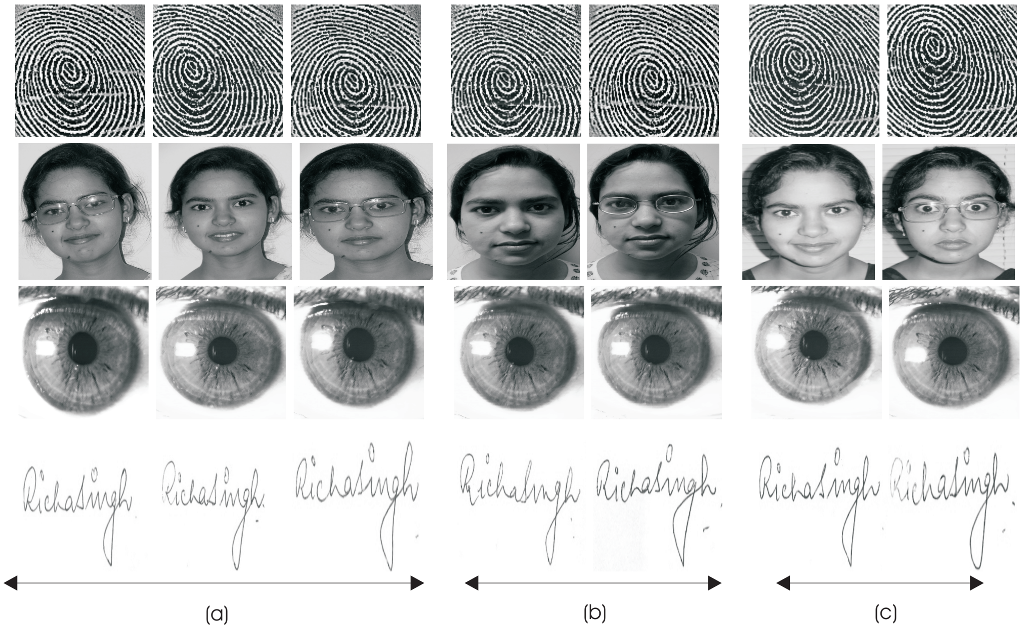

Fig. 12. Example of Multimodal Biometric Database with Images collected during (a) first month (b) second month and (c) third month

4.2 Validation of Proposed Fusion Algorithm

The effectiveness of the proposed algorithm is validated using diverse databases that include a dedicated multimodal database, well known individual biometric databases, and a commercial database. We also validate our proposed fusion algorithm using verification algorithms that we developed, existing algorithms in the literature, and commercial algorithm used in AFIS.

To determine the performance accuracy of fingerprint, face, iris, and signature we calculate the equal error rates before fusion. This represents the reference metric before the composite image is created using the proposed fusion algorithm. The error rates are calculated after reconstructing individual biometric images from the fused composite image. One of the advantages of our proposed approach, besides saving memory due to fusion, is the robustness to geometric and frequency attacks such as JPEG 2000, filtering, cropping and smoothing.

In a biometric system, images are stored in a database either locally or remotely and can also be distributed over servers. These stored images are vulnerable to attacks or can be intentionally tampered for misrepresenting one's identity. Also, when images or templates are sent over communication channels for matching, there could be errors introduced or the templates could be subjected to attacks [21,26]. These different attacks can cause degradation in performance and affect the reliability of the system. It is therefore imperative to verify that the composite fused biometric image is secure and resilient to tampering.

The composite image is subjected to different attacks, such as compression attack in which the image is compressed by 50% using JPEG 2000 standard and then reconstructing the individual images to evaluate the performance. Similarly, filtering and smoothing operations are performed separately using a 3 x 3 kernel. For cropping attack, the fused image is cropped by 10% from all four sides. The error rates are calculated after reconstructing individual biometric images from the fused composite image with these attacks.

Table 1 summarizes the equal error rates of biometric images before fusion and after reconstruction of individual images without attacks and with attacks. The results show that compared to the error rates before fusion, the error rates marginally increase when the fused biometric image is reconstructed without attacks and when subjected to attacks. The experimental results show that the proposed fusion algorithm does not affect the integrity of the biometric images. It is robust to tampering and has negligible effect on the verification performance.

The fusion algorithm is further validated using a commercial Automatic Fingerprint Identification System with 2.8 million fingerprints. The top 10 matching scores from the AFIS are obtained for the original fingerprint before fusion. The experiment is repeated using the reconstructed fingerprint from the fused

Table 1
Performance of the Biometric Images Before Fusion and After Reconstruction

Database	Verification Algorithm	EER (%) Before Fusion	EER (%) After Reconstruction No Attacks	Equal Error Rate (%) After Reconstruction - With Attacks			
				JPEG	Filtering	Cropping	Smoothing
Multimodal	Fingerprint [7,12]	0.55	0.62	1.09	1.27	0.86	0.71
Multimodal	Face [24]	4.26	4.53	5.16	5.65	5.12	4.81
Multimodal	Iris [28]	0.51	0.69	1.06	1.27	0.84	0.78
Multimodal	Signature [27]	9.80	10.18	11.03	11.31	10.48	10.27
FERET	Face [18]	5.21	5.88	6.59	6.99	6.33	6.16
CASIA	Iris [15]	0.79	0.93	1.65	1.87	1.52	1.07

image without attacks. Next, the same set of experiments is performed when the fused composite image is subjected to various attacks. Fig. 13 shows that the fingerprint matching scores before fusion and after reconstruction represents the best scores, denoting a genuine match. The second best match in each set generates significantly lower matching scores. Fig. 14 shows that when the composite fused image is tampered, the proposed fusion algorithm is resilient to common attacks such as compression, smoothing, cropping, and filtering. There is very slight degradation in verification performance. We also compared the performance of the proposed fusion algorithm with image compression technique. For this, the biometric images were subjected to WSQ compression [20] followed by scrambling and then the same four attacks were performed on the scrambled images. The error rates of these images were computed using the verification algorithms. In the experiments we found that the WSQ compression technique was not able to handle the attacks and the error rates increased from 1.74% to 5.32% for different biometric images. The next section addresses the improvement in performance accuracy by using multimodal biometric information for verification purposes.

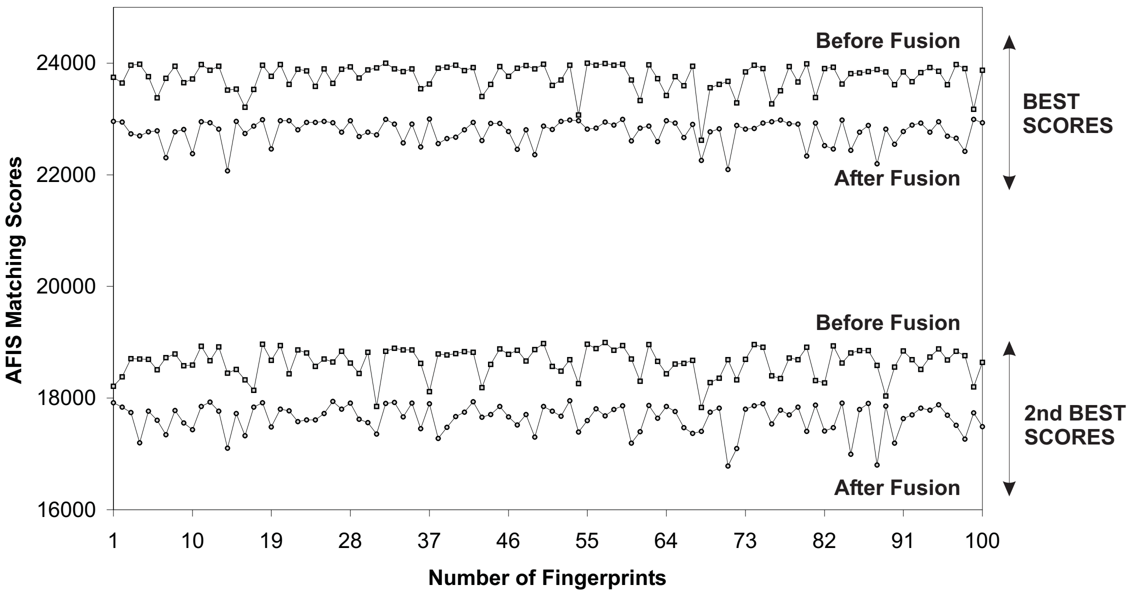

Fig. 13. Best and Second Best AFIS Matching Score before and after Fusion

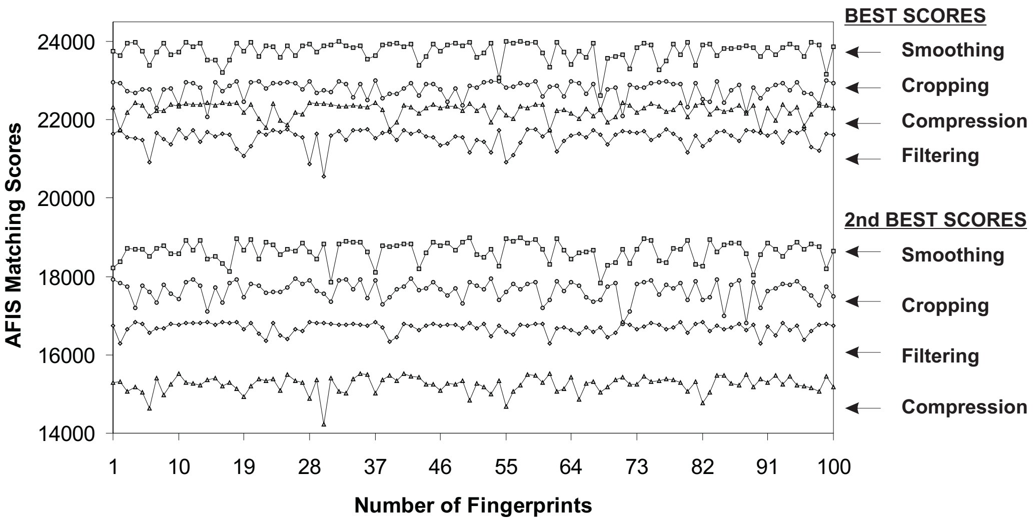

Fig. 14. Best and Second Best AFIS Matching Score when subjected to Attacks

5 Improving Verification Performance using Multiple Biometric Images

A single biometric introduces the problem of non-universality and circumvention. To overcome this problem, multiple biometric traits are used for user verification. The proposed fusion algorithm uses fingerprint, face, iris and signature to generate a composite image. To validate the fusion and reconstruction process, the matching score of multimodal biometrics algorithm fuses the matching score of the individual biometric algorithms and gives the fused score which is used for verification. There are several classifiers for the fusion process. Analysis of several classifier rules is conducted in [13,22]. It is suggested that the weighted sum rule is more effective and outperforms other fusion schemes based on empirical observations [9]. The weighted sum rule is defined as,

$$MS_{fusion} = \sum_{i=1}^{N} \omega_i MS_i \tag{14}$$

where, ω_i is the weight factor of the i^{th} biometric trait.

For multimodal fusion, we use the user specific weighted sum rule because the performance of this algorithm is found to be more effective in terms of false acceptance rate and false rejection rate. The matching score for the multimodal fusion algorithm is calculated using Equation 15.

$$\begin{aligned} MS_{fusion} = & \, a * MS(finger) + b * MS(face) + \\ & c * MS(iris) + d * MS(sign) \end{aligned} \tag{15}$$

where a, b, c and d are the user specific weight factors for fingerprint, face, iris and signature respectively.

For every individual the separation point is different for each biometric trait and this makes the process user specific. By defining the separation points, t_1, t_2, t_3 and t_4 during enrollment, we calculate the user specific weight factors. Here t_1 is the separation point for fingerprint of a particular individual. Similarly t_2, t_3 and t_4 are the separation points of face, iris and signature respectively. The weight factors are obtained using Equations 16 - 19 and are further used to calculate the matching scores.

$$a = \left[\frac{1-(FAR_{finger}+FRR_{finger})}{1-FAR_{finger}}\right]_{t_1} \tag{16}$$

$$b = \left[\frac{1-(FAR_{face}+FRR_{face})}{1-FAR_{face}}\right]_{t_2} \tag{17}$$

$$c = \left[\frac{1-(FAR_{iris}+FRR_{iris})}{1-FAR_{iris}}\right]_{t_3} \tag{18}$$

$$d = \left[\frac{1-(FAR_{sign}+FRR_{sign})}{1-FAR_{sign}}\right]_{t_4} \tag{19}$$

FAR denotes the false acceptance rate and FRR denotes the false rejection rate for an individual. The identity of a person is verified if,

$$MS_{fusion} \geq \eta \tag{20}$$

where η is the user specific matching threshold. The matching threshold is adjusted for each user such that it is sensitive enough to reduce the false acceptance and false rejection and hence improve the performance of the system.

Table 2 shows the equal error rate of the proposed multimodal biometric algorithm before fusion and after reconstruction of biometric images from the composite fused image. Using this approach we further reduce the EER to 0.27% from the individual EER of 0.51% previously obtained for iris and 0.55% obtained for fingerprint, as shown in Table 1. Additional validation is performed using a recent multimodal biometric algorithm [9]. While the performance of the proposed multimodal biometric algorithm is better, the existing algorithm provides a good baseline reference for comparison and validation. Table 2 shows that when the composite fused image is subjected to various attacks, there is negligible degradation in performance of the reconstructed images with both algorithms. The results in Tables 1 and 2 show that the fusion and reconstruction algorithms are effective and did not affect the

Table 2
Performance Accuracy of the Fused Biometric Images Before and After Fusion

Multimodal Fusion of Biometric Scores	EER (%) Before Fusion	EER (%) After Reconstruction No Attacks	Equal Error Rate (%) After Reconstruction - With Attacks			
			JPEG	Filtering	Cropping	Smoothing
Proposed Algorithm	0.27	0.27	0.38	0.45	0.31	0.29
Existing Algorithm [9]	0.49	0.51	0.62	0.70	0.55	0.54

integrity of the original images. The high level of verification performance of images obtained after reconstruction and with attacks validate that the biometric features are not compromised even when the total memory requirement is reduced by 75%.

6 Conclusions

In this paper we proposed computationally efficient biometric fusion algorithm which fuses information from four biometric images into a single composite image using multi-level discrete wavelet transformation. The proposed algorithm not only reduces the memory requirement by 75% but is also resilient to common tampering attacks such as smoothing, cropping, JPEG 2000 and filtering. The performance of the fusion algorithm is validated using different verification algorithms including algorithms we developed, existing algorithms and commercial algorithm. Experiments are carried out on a multimodal biometric database and other existing databases such as FERET face database, CASIA iris database, and fingerprint database from Sagem Morpho. The quantitative validation process establishes that the integrity of the biometric features used for personal verification is not compromised. We also proposed a multimodal biometric algorithm based on user specific weighted sum rule to further reduce the equal error rate compared to individual biometric images.

Acknowledgements

This research (Award No. 2003-RC-CX-K001) is supported by the Office of Science and Technology, National Institute of Justice, Office of Justice Programs, US Department of Justice. The authors wish to acknowledge Prof. T. Tan for providing the Iris database and Sagem Morpho for providing the AFIS and the fingerprint database. Portions of the research in this paper use the Color FERET database of facial images collected under the FERET program. The authors thank the reviewers for their valuable comments and suggestions for improving the quality and technical content of this paper.

References

[1] J. Bigun and J.M.H. du Buf, N-folded symmetries by complex moments in Gabor space and their applications to unsupervised texture segmentation, *IEEE Transactions on Pattern Analysis and Machine Intelligence* **16(1)** (1994) 80-87.

[2] J.-J. Brault and R. Plamondon, Segmenting Handwritten Signatures at their Perceptually Important Points, *IEEE Transactions on Pattern Analysis and Machine Intelligence* **15(9)** (1993) 953-957.

[3] CASIA Iris Image Database, http://www.sinobiometrics.com

[4] J.G. Daugman, High confidence visual recognition of persons by a test of statistical significance, *IEEE Transactions on Pattern Analysis and Machine Intelligence* **15(11)** (1993) 1148-1161.

[5] D. Gabor, Theory of Communication, *Journal of IEE* **93** (1946) 429-457.

[6] P. Gutkowski, Algorithm for retrieval and verification of personal identity using bimodal biometrics, *Information Fusion* **5(1)** (2004) 65-71.

[7] A. Jain, R. Bolle and L. Hong, Online Fingerprint Verification, *IEEE Transactions on Pattern Analysis and Machine Intelligence* **19(4)** (1997) 302-314.

[8] A.K. Jain, L. Hong and Y. Kulkarni, A Multimodal Biometric System using Fingerprints, Face and Speech, *Proceedings of International Conference on Audio- and Video-based Biometric Person Authentication* (1999) 182-187.

[9] A.K. Jain and A. Ross, Learning User-specific Parameters in a Multibiometric System, *Proceedings of IEEE International Conference on Image Processing* (2002) 57-60.

[10] A.K. Jain and A. Ross, Multibiometric Systems, *Communications of the ACM, Special Issue on Multimodal Interfaces* **47** (2004) 34-40.

[11] A.K. Jain, A. Ross and S. Prabhakar, An Introduction to Biometric Recognition, *IEEE Transactions on Circuits and Systems for Video Technology* **14(1)** (2004) 4-20.

[12] X.D. Jiang, W.Y. Yau, and W. Ser, Detecting the Fingerprint Minutiae by Adaptive Tracing the Gray Level Ridge, *Pattern Recognition* **34(5)** (2001) 999-1013.

[13] J. Kittler, M. Hatef, R.P.W. Duin and J. Mates, On combining classifiers, *IEEE Transactions on Pattern Analysis and Machine Intelligence* **20(3)** (1998) 226-239.

[14] A.S. Lewis and G. Knowles, Image compression using the 2D wavelet transform, *IEEE Transactions on Image Processing* **1(2)** (1992) 244-250.

[15] L. Ma, T. Tan, Y. Wang and D. Zhang, Efficient Iris Recognition by Characterizing Key Local Variations, *IEEE Transactions on Image Processing* **13(6)** (2004) 739-750.

[16] B.R. Meena, M. Vatsa, R. Singh and P. Gupta, Iris Based Human Verification Algorithms, *Lecture Notes in Computer Science* **3072** (2004) 458-466.

[17] A. Noore, An improved method to watermark images sensitive to blocking artifacts, *International Journal of Signal Processing* **1(2)** (2004) 129-134.

[18] P.S. Penev, and J.J. Atick, Local Feature Analysis: A general statistical theory for object representation, *Network: Computation in Neural Systems* **7(3)** (1996) 477-500.

[19] P.J. Phillips, H. Moon, S.A Rizvi and P.J. Rauss, The FERET evaluation methodology for face recognition algorithms, *IEEE Transactions on Pattern Analysis and Machine Intelligence* **22(10)** (2000) 1090-1104.

[20] N.K. Ratha, J.H. Connell, and R.M. Bolle, Secure data hiding in wavelet compressed fingerprint images, *Proceedings of the ACM Workshops on Multimedia* (2000) 127-130.

[21] N.K. Ratha, J.H. Connell, and R.M. Bolle, An analysis of minutiae matching strength, *Proceedings of the AVBPA* (2001) 223-228.

[22] A. Ross and A.K. Jain, Information Fusion in Biometrics, *Pattern Recognition Letters* **24(13)** (2003) 2115-2125.

[23] http://www.morpho.com/

[24] R. Singh, M. Vatsa and A. Noore, Textural Feature based Face Recognition for Single Training Images, *IEE Electronics Letters* **41(11)** (2005) 23-25.

[25] S.K. Singh, D.S. Chauhan, M. Vatsa and R. Singh, A Robust Skin Color Based Face Detection Algorithm, *Tamkang Journal of Science and Engineering* **6(4)** (2003) 227-234.

[26] U. Uludag and A.K. Jain, Attacks on biometric systems: a case study in fingerprints, *Proceedings of the SPIE-EI 2004, Security, Steganography and Watermarking of Multimedia Contents VI* (2004) 622-633.

[27] M. Vatsa, R. Singh, P. Mitra and A. Noore, Signature Verification using Static and Dynamic Features, *Proceedings of International Conference on Neural and Information Processing* (2004) 350-355.

[28] M. Vatsa, R. Singh and A. Noore, Reducing the False Rejection Rate of Iris Recognition using Textural and Topological Features, *International Journal of Signal Processing* **2(1)** (2005) 66-72.

[29] R.P. Wildes, Iris Recognition, An Emerging Biometric Technology, *Proceedings of the IEEE* **85** (1997) 1348-1363.

[30] J. Zou, R. K.Ward, and D. Qi, A New Digital Image Scrambling Method Based on Fibonacci Numbers, *Proceedings of IEEE International Symposium on Circuits and Systems* **3**(2004) 965-968.