Bimodal Biometrics for Financial Infrastructure Security

O.A.Esan, S.M.Ngwira
Computer System Engineering
Tshwane University of Technology, TUT
Pretoria, South Africa
esanoa@tut.ac.za, ngwirasm@tut.ac.za

I.O.Osunmakinde
School of Computing, College of Science, Engineering and Technology, University of South Africa, UNISA
Pretoria, South Africa
osunmio@unisa.ac.za

***Abstract*— This research examines whether the integration of facial and fingerprint biometrics can improve the performance in financial infrastructure security such as ATM protection. Fingerprint biometrics consider distorted and misaligned fingerprints caused by environmental noise such as oil, wrinkles, dry skin, dirt and displacement of the query fingerprint with the database fingerprint template during matching. The noisy, distorted and/or misaligned fingerprint produced as a 2-D on x-y image, is enhanced and optimized using a new hybrid Modified Gabor Filter-Hierarchal Structure Check (MGF-HSC) system model based on an MGF integrated with an HSC. However, in order to improve the accuracy of financial infrastructure, face biometrics are introduced using a fast principal component analysis algorithm, in which different face conditions such as lighting, blurriness, pose, head orientation and other conditions are addressed. The MGF-HSC approach minimizes false fingerprint matching and the dominant effect of distortion and misalignment of fingerprints to an acceptable level. The proposed bimodal biometrics increase the accuracy of the False Rejection Rate (FRR) to 98% when the False Acceptance Rate (FAR) is 0.1% in an experiment conducted with 1000 test cases. This result shows that facial biometrics can be used to support fingerprint biometrics for improving financial security based on with significant improvement in both FRR and FAR.**

Keywords - Authentication, Distortion, Misalignment, Noise, Fingerprint, Face, biometrics, Model

I. INTRODUCTION

An automated technique of recognizing a person based on physiological and behavioural traits is known as a biometrics system. The physiological traits include the face, fingerprint, palm print and iris, which remain permanent throughout an individual's lifetime. The behavioural traits are signature, gait, speech and keystroke, etc., which change over time [1].

The advantages of a fingerprint authentication system make the system the most widely used biometric system for various applications for security and access control in airports, at borders, immigration offices, houses, offices, banks and other places where security needs to be enhanced. However, face identification is also one of the acceptable biometric systems widely used in public security systems, attendance systems etc. because of its convenience and high efficiency [2].

The associated complication is the problem of securing stored and transit information in various parts of the system raising an information management need [8]. Securing of data has been of paramount importance in both the private and public sectors. Thus, as the points which are vulnerable security-wise on the system increase, so does the security threat to the system. A system which incorporates cryptographic concepts in an effort to reduce this vulnerability has been reported in [15].

A study conducted by a Verizon risk team in cooperation with the United States Security Service (USSS) recorded approximately 900 million data breaches in financial institutions from 2008 to 2010. Figure 1 shows the record of security breaches at financial institutions from 2008 to 2010 [14].

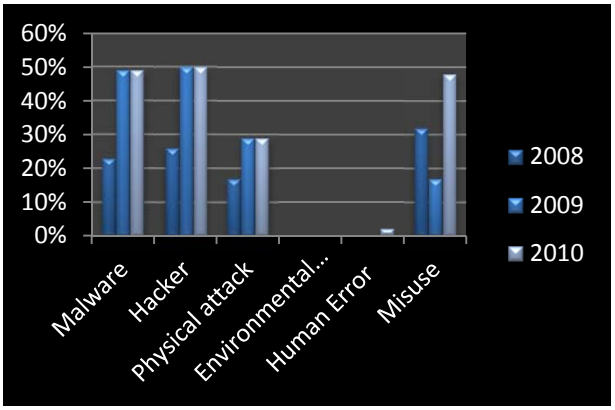


Figure 1. Visualization of security breaches in USSS

One can see in Figure 1 that in most years the number of hacker and malware attacks exceeded 35%. This is not good enough, particularly for the banking sector, where the adaptation of a fingerprint authentication system can greatly reduce the high rate of threat agents to a minimal number. Higher threat agents' percentages have been reported in developing countries such as Zimbabwe, Kenya, Nairobi, Botswana and Mozambique, where the use of identifiers (IDs), passwords and personal identification numbers (PIN) for ATM are the predominant techniques for authentication, but all these are vulnerable to theft, forgery and loss [1].

Biometric technology presents several advantages over classic security methods, as there is no need for the user to remember difficult PIN codes that could easily be forgotten or carry a key that could be lost or stolen [1,12]. However, in spite of these advantages, fingerprint authentication systems still present a number of drawbacks, including fingerprint distortions, misalignment and lack of secrecy (e.g., hackers can easily steal someone's fingerprints at any time).

It is thus of special relevance to address these drawbacks for the benefit of fingerprint users in financial institutions.

A. *Fingerprint Alignment*

Fingerprint alignment is a crucial stage in a fingerprint authentication system. Misalignment is caused by displacement in the fingerprint image, mostly during the authentication phase. The displacement includes the translation and rotation of a fingerprint image [9]. Figure 2 shows an example of misaligned positions of the same fingerprint, which often affect the matching accuracy of a query fingerprint captured in the authentication phase with the database fingerprint template captured in the enrolment phase [3].

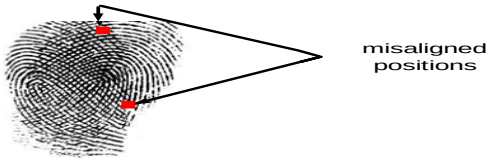


Figure 2. Fingerprint with misalignment

B. *Fingerprint Distortions*

Distortions in fingerprints are caused by poor quality input, which might be due to variations in skin condition caused by accidents, cuts or bruises. The ridge structure in such fingerprint images is consequently not well-defined and correctly detected. The red or dotted circles in Figure 3 indicates areas of distortion, which may lead to the creation of a significant number of spurious minutiae, causing a large percentage of genuine minutia to be ignored and large error in localization [4].

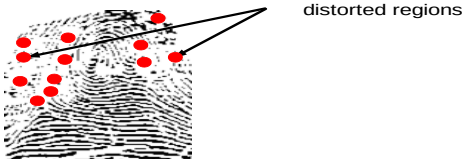


Figure 3. Fingerprint with distortion

C. *Face Identification*

In face recognition, the extraction of a human face and valley features of the face are very important. The extraction of the human eye at grey level is obtained from valley features. However, since the size of the human face is proportional to the distance between the two eyes, a possible face region that contains the eyebrows, eyes, nose and mouth can be formed based on this relationship. Face features extraction fails owing to facial images with glasses, which might affect the eyebrows; lighting conditions, which highly affect nostril detection and moustaches covering the corners of the mouth [16]. A typical example of this is shown in Figure 4.

Figure 4. Human face covered with glasses and mouth covered with moustache

Since none of the biometric systems are 100% accurate [8] the extracting of multiple biometric features from an individual can advertently lead to improved performance and robustness of an authentication system compared to one using a single biometric system [8].

The motivation of the experiment presented in this paper is to address issue of distortions and misalignment in bimodal biometrics system using less expensive computational algorithm to improve on the limitation of [5].This paper advances the existing bimodal authentication systems by addressing the problem of distortion, misalignment in fingerprints as well as the problem due to light on a facial image with glasses. This is in a bid to improve the security of the resultant system with applications in financial institutions. The major contributions of this paper therefore are as follows:

- Proposal of a bimodal biometrics constituting a hybrid Modified Gabor filter-Hierarchical Structural Check (MGF-HSC) matching and a fast Principal Component Analysis (PCA) as a two-level security authentication.
- Experimental evaluations of the bimodal biometrics with application to financial systems using real-life fingerprint images and benchmarking with publicly available datasets using Fingerprint Verification Competition (FVC) 2000a methods and facial images.

The deployment analysis of this approach with application to financial institutions, especially in developing countries, is unheard of.

The rest of this paper is organized as follows: section 2 presents the theoretical background, which includes related work on the MGF algorithm and HSC algorithm; section 3 presents the fingerprint authentication system model; section 4 critically presents visual inspection and quantitative experimental evaluations of the approach using lightly and heavily distorted fingerprint images. Our MGF-HSC is also benchmarked with the Gabor filtering method. We conclude the paper in section 6.

II. THEORETICAL BACKGROUND

A. *Other Related Research*

Several fingerprint approaches have been proposed in the literature. These include methods based on point pattern matching, transform features and structural matching.

A new method of personal authentication using face and palm print images is presented in [9]. The proposed bimodal system authentication uses a feed-forward neural network to

integrate individual matching scores, which generates combined decision scores. During the fusion stage the technique uses the claimed identity of the user as a feature. The experimental result obtained shows the sum Max and the product rule can be used to achieve significant improvement of bimodal biometrics when using consolidated matching scores instead of a direct matching score.

Related to this work is also a research done on speech and face feature bimodal biometric authentication in [5] using the Mel-frequency cepstral coefficient (MFCC) with delta for feature extraction and the Gaussian Mixture Model (GMM) but it leaves out issue of genuine user being denied access to their database due to degradation in any of the bimodal biometric used during authentication. Consequently, the enhancement of the degraded fingerprint is not mentioned, perhaps due to this limitation. The purpose therefore of the experiment presented in this paper is to address the fingerprint distortions and misalignments and contribute on the reduction of their negative effects on the system while optimizing the whole system with the inclusion of the facial biometric parameters. Added security aspects would make the system attractive for use in financial institutions.

B. Modified Gabor Filtering Algorithm

Computer image processing uses the Gabor function for analyzing image texture, because of the frequency selective property and orientation selective property [7]. With the selective property exhibited by MGF, the fingerprint image and invariant coordinates for ridges in the local neighborhood are defined.

The selective orientation property helps in modeling the grey level along the ridges and valleys into a sinusoidal-shaped wave in the area of the fingerprint where there is no appearance of minutiae [7]. Equation (1) represents an even-symmetric real component of a 2–D Gabor filter in the spatial domain that can be used in removing noise and preserving the true ridge/valley structure in fingerprint images.

$$G(x, y, f_0, \theta) = \exp\left(-\frac{1}{2}\left[\frac{x_\theta^{\,2}}{\sigma_x^{\,2}} + \frac{y_\theta^{\,2}}{\sigma_y^{\,2}}\right]\right)\cos(2\pi f_0 x_0)\cdot \tag{1}$$

Where θ is the ridge with respect to the vertical axis, f_0 is the frequency of the sinusoidal plane wave in the x_θ direction; σ_x and σ_y are the standard deviation of Gaussian function along the x_θ and y_θ axes respectively. However, in the MGF approach a pixel-wise scheme is used to estimate the orientation field of the distorted fingerprint image correctly, as in equation (2).

$$\theta_{(i,j)} = \frac{1}{2}\frac{\left(\sum_{v=i-\frac{w}{2}}^{i+\frac{w}{2}}\sum_{u=j-\frac{w}{2}}^{j+\frac{w}{2}} w\ 2G_x(u,v)\right)G_y(u,v)}{\left(\left(\sum_{v=i-\frac{w}{2}}^{i+\frac{w}{2}}\sum_{u=j-\frac{w}{2}}^{j+\frac{w}{2}} w\ G_x^{\,2}(u,v)\right) - G_y^{\,2}(u,v)\right)}. \tag{2}$$

W is the image block size; G_x and G_y are the gradient at each (x, y) in each block, u and v are the distance along x and y respectively. Derived from equation (1), the areas with distortions are expressed in equation (4) as T in harmonic oscillation. Also, MGF explicitly explains equation (1) in frequency domain for enhancing the fingerprint image by representing it with a cosine function in equation (3). Modulating the periodic function $F(X_1, T_1, T_2)$ to obtain:

$$g'(x_1; T_1, T_2, \varphi) = h'_x(x_1, T_1, T_2, \varphi)\bullet h'_y(y; \varphi) = \left\{\exp\left(-\frac{x_\theta^{\,2}}{2\sigma_x^{\,2}}\right)f(x_\sigma; T_1, T_2)\right\}\bullet\left\{\exp\left(\frac{-y_\varphi^{\,2}}{2\sigma_y^{\,2}}\right)\right\}. \tag{3}$$

The merit of Modified Gabor Filter approach is that it's parameter selection is image-independent.

C. Hierarchical Structural Check Matching Algorithm

Matching two fingerprints in minutiae-based representation presents a problem with aligning the two pairs of corresponding fingerprints' minutia points [3, 13]. A minutia-matching algorithm utilizes local structure matching based on composite features.

Thus, the local structure matching based on composite features are represented in triplet form, as shown in equation (4):

$$C_M = d, \vartheta, \theta,\ C_M^1 = d^1, \vartheta^1, \theta\ . \tag{4}$$

The hierarchal structure check addresses the issue of rotation and translation of parameters in the fingerprint image.

D. Fast Principal Component Analysis with Fuzzy Edge Detection

Fast PCA is one of the most widely used techniques for face recognition. In fast PCA and fuzzy edge detection face-based recognition, some features of interest in the face are used and sub-grouped into the database. Only the sub-grouped face features are used in the PCA algorithm for recognition [16].

The fast principal component analysis procedure consists of taking a sample of the grey scale image in 2D matrix and transforming it into a 1D column vector of size $N^2 \times 1$. The image matrix is then place in the 1D column vector. The column vector of the K image is placed in columns to form the data matrix Y of dimension $N^2 \times k$.

The mean n vector of the data vector in matrix K is given in equation (5):

$$n = \frac{1}{k}\sum_{i=1}^{k} y \quad . \qquad (5)$$

The merit of fast PCA with fast fuzzy edge detection is that it is faster and gives accurate face recognition [16].

III. PROPOSED BIMODAL BIOMETRICS MODEL

The system model described in Figure 6 for a bimodal biometrics authentication system is divided into two stages: - (1) fingerprint authentication using the MGF-HSC approach and (2) face recognition using fast PCA.

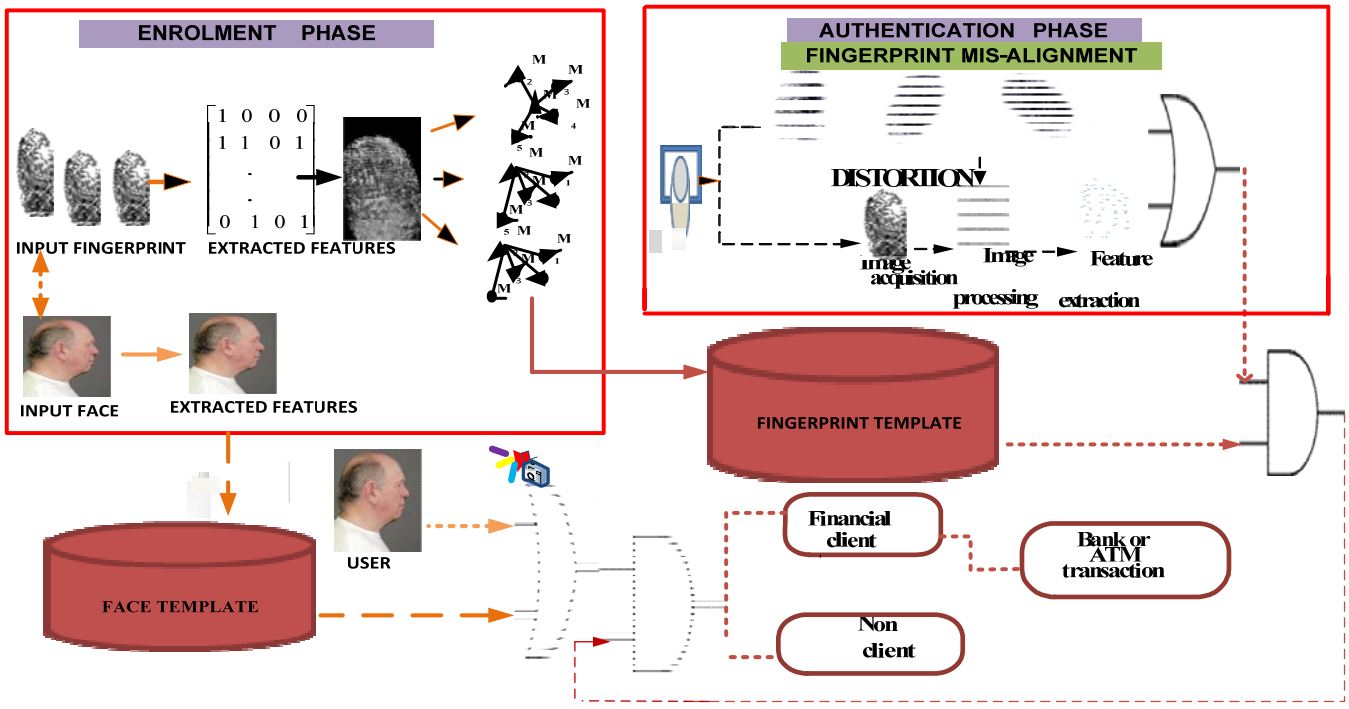


Figure 6. System Model

1. *FINGERPRINT AUTHENTICATION USING MGF-HSC*

As indicated in Figure 6, the fingerprint authentication phase is divided into two phases, namely the. (i) Enrolment phase and (ii) Authentication phase.

A. The Enrolment Phase

According to the above system model, it is at this stage that the fingerprints are rotated in different directions to avoid rotational and directional invariance of the user fingerprint during the authentication stage, as the direction used for the registered user fingerprint on the template of the stored user fingerprint is captured using a fingerprint scanner or fingerprint reader and this is stored together with other relevant information on the user. The enrolment module is sub-divided into:

B. Biometric Feature Extraction Stage

Before feature extraction, the image is passed through image enhancement stages, which include normalization, binarization, segmentation and thinning.

After these stages follows feature extraction, represented in Figure 6, in which the most important features, such as ridges and valleys, are extracted from the fingerprint by subjecting it to image processing and extraction algorithms. The extracted features are set as binaries in which the grey region is represented as 0's and the white region is represented as1's respectively. The cross number (CN) concept is used for extraction of fingerprint features as either ridge-ending or bifurcation.

C. Authentication Phase

According to the system model depicted in Figure 6, during the authentication module the system requires the user to present his or her fingerprint physically again for the system to confirm whether he/she is who he/she claims to be. This module is subdivided into two stages in D and E.

D. Distortion Enhancement

A good quality fingerprint is important for a fingerprint authentication system to work properly.

The distorted fingerprint presented on the bottom left side of Figure 6 is introduced during the image acquisition stage, as smudgy difficulties could be created by an over-inked area, breaks in the ridge created by an under-inked area, dry skin, which leads to a fragmented and low contrast ridge, wounds causing ridge discontinuities and sweat on the fingerprint, which also leads to smudge marks.

These fingerprint distortions change the position and orientation of fingerprint minutia. Fingerprint enhancement with MGF is used to improve the contrast between ridges and valleys and reduce the degradation in the fingerprint images.

E. Matching Stage

At this stage the query fingerprints are compared with the bank fingerprint in the database (template) to determine if the person is who he claims to be. This is done by using the matching algorithm and matching score of two minutia pairs of composite features in triplet form to determine if they are identical.

ALGORITHM 1: Computation of ridges and valleys for MGF-HSC

INPUT: G=normalized image, block size=W*W
OUTPUT: Ridge and valley

STEP 1: divide G image into W*W centered (i, j)
STEP 2: for each (i, j)
STEP 3: compute l*w
STEP 4: for each block centered (i, j);
STEP 5: compute $\partial_x(i, j)$ and $\partial_y(i, j)$ of each pixel
STEP 6: compute the magnitude of $\partial_x(i, j)$ and $\partial_y(i, j)$ at each pixel
STEP 7: set a local threshold value
STEP 8: if magnitude $\partial_x(i, j)$ and $\partial_y(i, j)>$ threshold value, ridge is obtained
STEP 9: else
STEP 10: valley is obtained

In algorithm 1, the ridges and valley in minutiae are computed by dividing the image into block-sized centered (i, j), and an oriented window of w*l is built at each center. The second derivatives and the magnitude of first derivatives are obtained. A local threshold value is set to determine ridge width and valley width: if the magnitude of the first derivative is greater than the threshold, it is a ridge, otherwise it is a valley.

ALGORITHM 2: COMPOSITE MATCHING OF TWO FINGERPRINTS BY MGF-HSC

INPUT: ML= Minutiae-List, M_{by}=Minutiae-b.y, Pt=predefine threshold,T=tolerance M_{ax}=Minutiae-a.x, May=Minutiae-a.y, MM=Matched-minutiae, M_{bx}=Minutiae-b.x, NM_a=NORMALIZE (minutiaea.angle), NM_b=NORMALIZE (minutiae-b.angle), ΘT=ANGLE-TOLERANCE, X_T=X-tolerance, Y_T=Y-tolerance,
OUTPUT: TRUE MATCH

STEP 1: MM← 0
STEP 2: for each x-source-ML
STEP 3: for each y target-ML
STEP 4: Matches(x, y) MM←MM+1
STEP 5: if MM ≥ Pt
STEP 6: return true
STEP 7: else
STEP 8: return false
STEP 9: if $(M_{ax} - M_{bx}) \leq X_T$ and
STEP 10: if $(M_{ay} - M_{by}) \leq Y_T$ and
STEP 11: if $NM_a - NM_b \leq \theta_T - T$
STEP 12: return true

In matching two fingerprints, the algorithm returns true if it matches (as determined by diverse parameters in the algorithm) and false if it does not match.

2.FACE RECOGNITION USING FAST PCA ALGORITHM

Face recognition is divided into two stages: (i) training stage and (ii) testing stage

A. Training Stage

In the training stage, the image is acquired. The acquired image is passed through an image pre-processing stage such as histogram normalization to adjust the contrast process of the image such that the output image will contain a uniform distribution of gray values and the variation and light intensity level in the gray image are reduced.

B. Recognition Phase

During this phase, the image to be recognized is passed through the testing stage by passing the image again through image pre-processing and features extraction, as done in the training phase. This occurs in the Enrolment phase as well as in the Authentication stage of Figure 6.

The extracted features are converted to an image vector and the image is projected to the Eigen space. The Euclidean distance between the tested image and all projected trained images is estimated to find the corresponding closest one and this is used for recognition.

ALGORITHIM 3: FACE FEATURE EXTRACTION USING FUZZY SOBEL EDGE

INPUT: face image N
OUTPUT: face edge extraction

STEP 1: input face image N
STEP 2: Compute mask G_x, G_y
STEP 3: Apply Sobel detection algorithm and gradient

STEP 4: Manipulate mask G_x, G_y on image N

STEP 5: Compute absolute magnitude of gradient $/G/$

STEP 6: obtain N edge detection

From algorithm 3, the facial features are extracted using sobel edge detection in which the input image is separated using mask G_x, G_y to obtain gradient component $/G/$ in each orientation and then combined together to produce absolute magnitude and orientation gradient at each point.

3. Scoring and Evaluation Scheme

In this section, the performance of the proposed bimodal biometric is studied through visual inspection as well as quantitatively. During visual inspection, one compares the quality of the pixel value of distorted and misaligned fingerprints with enhanced fingerprint images [4]. The following evaluation models were chosen as quantitative schemes [10, 13]: (i) the false rejection rate (FRR), (ii) the false acceptance rate (FAR) and (iii) the receiver operating characteristics (ROC) curve [6]; the schemes in [6] are computed by the following formulas:

FRR is the fraction of number of false rejections to the number of accesses and is calculated as

$$\text{FRR} = \frac{\text{Number of False Rejections}}{\text{Number of acesses}} \quad (6)$$

.

FAR is the fraction of number of false acceptances to number of accesses and is calculated as:

$$\text{FAR} = \frac{\text{Number of False Acceptances}}{\text{Number of acesses}} . \quad (7)$$

The ROC is a plot of the FRR against FAR at different operating points.

The percentage of system accuracy is computed by the following formula [10]:

$$\text{SA} = \frac{\text{Total No. of organized fingerprint sample}}{\text{Total No. of fingerprint sample}} \times 100 \quad (8)$$

Where SA is system accuracy.

These equations are used as objective evaluation schemes for measuring distorted and misaligned fingerprint enhancement.

IV. EXPERIMENTAL EVALUATIONS

One of the objectives of this paper is to apply the theory of our approach in practice by emphasising applications and carrying out practical work on fingerprints with distortion and alignment, as well as face recognition using MATLAB, as shown in experiments 1-3.

The fingerprint images are captured with a Futronic fingerprint scanner and the captured fingerprint produces a stream of distortions and misalignments on the x-y axis. An original fingerprint with distortions and overlapping is shown in Figures 2 and 3.

In calculating the percentage of the noisy region, the fingerprint image is divided into 3*3 window size; the region with distortion is estimated using a noise detector scheme in equation (9). The scheme states that: (i) if a pixel x has at least one pixel y among the other eight pixels in the neighbourhood, then x is considered an original pixel and y is deemed similar to pixel x; and (ii) if x does not have at least one similar pixel among its neighbours, it is considered to be distorted; this is shown using equation (9):-

$$x = \begin{cases} x_{ij}^{0} & K\{|x - y| \le D_1\} \ge N_1^{th} \\ x_{ij}^{n} & \text{else} \end{cases} . \quad (9)$$

D_1 is adopted as the maximum depth difference between the similar x and y pixels and is often assumed to be eight pixels in the neighborhood. N_1^{th} is 1 as every pixel is assumed to be similar to at least 1 pixel, and K is the number of y pixels that satisfies equation (9) while the distorted pixel is eliminated.

For alignment, all minutiae in the fingerprint template and the corresponding query minutiae are searched for. A fixed reference point is selected; all the minutiae which are close to that minutia position within T1 pixels (T1 is the threshold chosen in the experiment) are then searched for. A minutia in the template is mapped to the query template to get a new minutiae point. All the surrounding minutiae around new minutiae within T1 pixels are selected and the hamming distance is calculated for each pair of minutiae using equation (10).

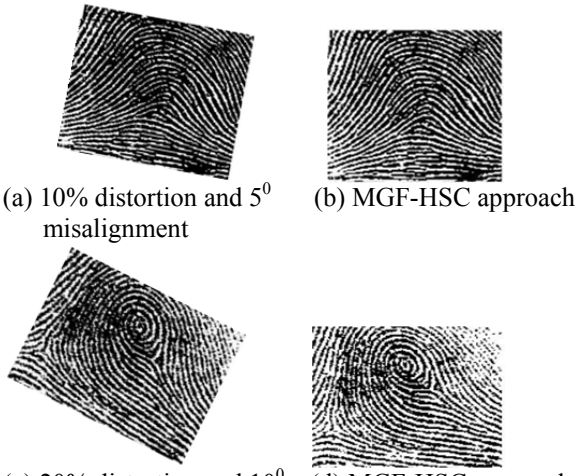
$$\text{Hamming distance} = \frac{\text{SUM}(\text{block1 XOR block2})}{\text{size of block}} . \quad (10)$$

The hamming distance [12] is used to measure the dissimilarity between the two binary blocks. The minutia in the query image that has the smallest hamming distance value is considered and a minutia template with this value possibly forms a pair. Then all possible minutiae pairs are searched and the average rotation angle of these blocks is obtained. Finally the query fingerprint image is rotated by that average rotation angle.

However, this work focuses on bimodal biometrics and enhancing distorted and misaligned fingerprint images. In terms of performance measures, the FAR, FRR, and ROC are computed when evaluating the result of the proposed MGF-HSC approach and fast PCA algorithm, as shown in Figure 9.

Experiment 1: Visual inspection of Fingerprint Identification using MGF-HSC and Benchmarking with Gabor Filter

The objective here is to access the qualitative performance of the MGF-HSC approach on a real-life distorted and misaligned fingerprint template.

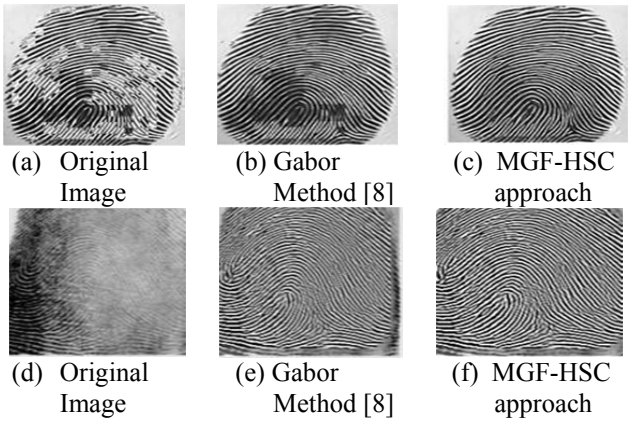


(a) 10% distortion and 5^0 misalignment (b) MGF-HSC approach

(c) 20% distortion and 10^0 misalignment (d) MGF-HSC approach

Figure 7. Images (a) and (c) are real-life fingerprints with distortion and misalignment; images (b) and (d) are the enhanced fingerprint.

The aim of this experiment was to demonstrate the performance of our MGF-HSC approach on lightly and heavily distorted and misaligned fingerprint images. In particular Figures 7(a) and 7(c) contain 10% distortion and 5^0 misalignments and 70% distortion and 25^0 misalignments respectively. Figures 7 (b) and 7(d), on the other hand, are the fingerprint results obtained after enhancement with the MGF-HSC approach. This could be extended to 90% distortions and our algorithm could still be effective.



(a) Original Image (b) Gabor Method [8] (c) MGF-HSC approach

(d) Original Image (e) Gabor Method [8] (f) MGF-HSC approach

Figure 8. Images (a) and (d) are real-life fingerprints with distortion images (b); (c), (e) and (f) are the enhanced fingerprints.

Having benchmarked MGF-HSC approach with the Gabor method in Figure 8, one can see the result of the MGF-HSC approach in Figures 8(c) and 8(f) respectively, which show better visual enhancement clarity compared to the images in Figures 8(b) and (e) respectively.

Experiment 2: Quantitative Performance of MGF-HSC Approach

From the result in Table 1, we specifically access the quantitative performance of our MGF-HSC approach with respect to noise level, ranging from 10%+5^0 to 90%+40^0(distortions and misalignments).

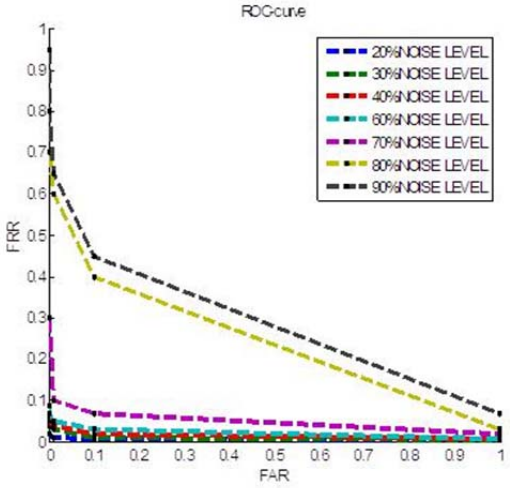


Figure 9. ROC for proposed MGF-HSC model

The graph in Figure 9 shows the result of FRR and FAR of the enhanced fingerprints at various forms of distortion and misalignment. At 90% noise level, the FRR is 97.5% at FAR of 0.1%. This trend show that FRR is slightly increasing, the FAR is decreasing and it suggests a better constructive result for security in financial institutions.

Experiment 3: Performance of the Combined Biometrics

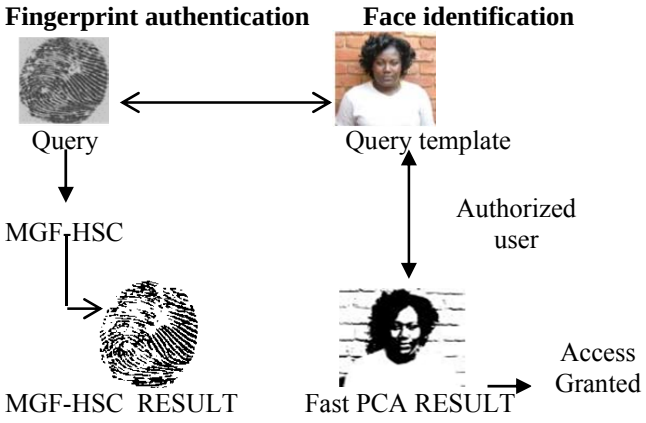


Figure 10. Combined face with fingerprint image

From Figure 10, the face and fingerprint of the user match to the one in the database. However, if the fingerprint of user is the same as the fingerprint in database but the face is different the system recognizes the user as an imposter.

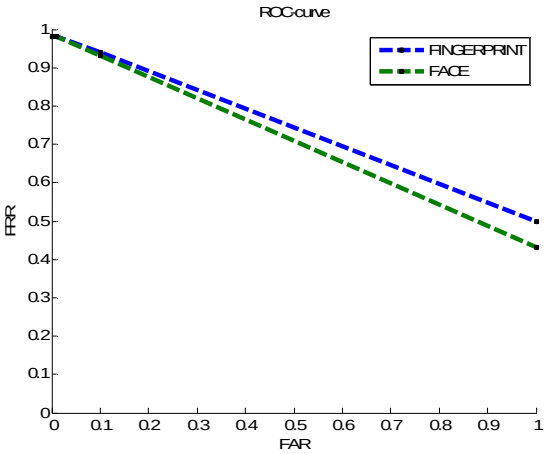


Figure 11. The ROC verification graph for proposed bimodal biometrics system model

The ROC verification result is shown in Figure 11. One can see that the result of the fingerprint is slightly higher than that of the face at certain levels. Specifically at FAR of 0.1%, the FRR is 98%. The FAR less than one show a complementary result of our bimodal biometrics which substantiates the belief of a stronger security in financial institutions than single biometrics. This is comparable to result obtained by Lin Hong et al [17] on the bimodal biometric approach used.

V. CONCLUDING REMARKS

We have proposed and demonstrated the use of a bimodal biometric approach for addressing the issue of security in financial infrastructure. We conducted experiments using the MGF-HSC algorithm to address the issue of distortions and misalignment of fingerprints during authentication. At first the enhancements of noisy images seemed discouraging, but experimental results on moderately or less heavily noisy images were encouraging.

Our findings indicate that the MGF-HSC approach can completely remove noise from a light noisy image from 1% to 60%, but is limited when the fingerprint is contaminated with heavy noise ranging from 70% upward. In a situation with heavy distortion the fingerprint orientation field is hard to estimate. The accurate computation of the ridge width and valley width is challenging. However, this approach exhibits reliable authentication performance with application to banks in terms of quantitative performance. Moreover, due to some advantages exhibited by the face and fingerprint combined system such as non-intrusive, robustness, acceptability, low-cost and accuracy; this makes the proposed bimodal biometric system outweigh other bimodal biometric system.

This research is a proof of a concept and was simulated on customers' fingerprints in a bank. In future work, research can be explored further in the following directions: (i) using multi-biometrics for authentication and (ii) putting a fingerprint software code on embedded hardware to improve the speed as an effort to contribute to the reduction of the overall infrastructure of the system.

REFERENCES

[1] A.M. Baze, G.T.B. Verwaaijen, S.H. Gerez, L.P.J. Veelenturf and B.J. Van der Zwaag, "A Correlation-Based Fingerprint Verification System", in Proc. proRISC2000 Workshop on Circuits, Systems and Signal Processing, 2000.

[2] A. El-Sisi, "Design and Implementation Biometric Access Control System using Fingerprint for Restricted Areas based on Gabor Filter", International Arab Journal of Information Technology, vol.8, No 4. Egypt, 2011.

[3] M. Fons, F. Fons and E. Canto, "Design of an Embedded Fingerprint Matcher System", Department of Electronic Electrical and Automation Engineering, University of Rovirai Virgili (URV), 2006.

[4] L. Hong, Y. Wan, and A. Jain, "Fingerprint Image Enhancement: Algorithm and Performance Evaluation", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol.20, pp. 777-789, 1998.

[5] S.K. Sahoo and S.R Mahadava Prasanna, "Bimodal Biometric Person Authentication using Speech and Face under Degraded condition", IEEE Transactions, 2011.

[6] J-M. Ramirez-Cortez, P. Gomez-Gil, V. Alarion-Aquino, D. Baez-Lopez and R. Enriquez-Caldera, "A Biometric System Based on Neural Networks and SVM Using Morphological Feature Extraction From Hand-Shape Images", Informatica, Vol. 22, No. 2, pp. 225-240, 2011.

[7] S.K Sahoo and S.R Mahadava Prasanna, "Bimodal Biometric Person Authentication using Speech and Face under Degraded Condition", IEEE Transactions 2011.

[8] M.N Eshwarappa and M.V Latte, "Bimodal Biometric Person Authentication System using Speech and Signature Features", International Journal of Biometric and Bioinformatics (IJBB), Vol.4, issue 4.

[9] B. Biggio, Z. Akthar, G. Fumera, G.L Marcialis and F. Roli, "Security Evaluation of Biometrics Authentication System under Realistic Spoofing Attacks"

[10] A. Chatterjee, S. Mandal, G.M.A Rahaman & A.S Mohammad Arif, "Fingerprint Identification and Verification System By Minutiae Extraction using Artificial Neural Network", JCIT, ISSN 2078-5828, Vol. 1, Issue 1, 2010.

[11] I. Sarkar, F. Alisherov, T. Kim and D. Bhattacharyya, "Palm-vein Authentication System: A Review ", International Journal of Control and Automation, Vol. 3, No.1, 2010.

[12] S. Shukla and P. Mishra," A Hybrid Model of Multimodal biometric system using Fingerprint and Face trait", International Journal of Soft Computing and Engineering, Vol. 2, issue 1, ISSN: 2231-2307, 2012.

[13] S. Khalil, "A Back Propagation Neural Network for Computer Network Security", Journal Computer Science 2(9):710-715, ISSN 1549-3636, 2006.

[14] Veron Business Risk Team and United State Secret Service "A Study of Data Breach Investigation Record in Financial Institution", 2010.

[15] J. Li, X. Yang, J. Tian, P. Shi and P. Li, "Topological Structure-based Alignment For Fingerprint Fuzzy Vault", Institute of Automation, Chinese Academy of Science, Beijing China, 2008.

[16] Neerja and E. Walia, Face Recognition Using Fast PCA Algorithm". 2008 Congress on Image and Signal Proces,2008.

[17] L. Hong and A. Jain, "Integrating Faces and Fingerprints for Personal Identification", IEEE transactions on pattern analysis and machine intelligence, Vol. 20, N0. 12, 1998.