Hybridization of Bimodal Biometrics for Access Control Authentication

T. Zuva, O. A. Esan, and S. M. Ngwira

***Abstract*—Single biometric trait for authentication is widely used in some application areas where security is of high importance. However, biometric systems are susceptible to noise, intra-class variation, non-universality and spoof attacks. Thus, there is need to use algorithms that overcome all these limitations found in biometric systems. The use of multimodal biometrics can improve the performance of authentication system. This study proposed using both fingerprint and face for authentication in access system. The study integrated fingerprint and face biometric to improve the performance in access control system. Fingerprint biometric, this paper considered restoration of distorted and misaligned fingerprints caused by environmental noise such as oil, wrinkles, dry skin, dirt, displacement etc. The noisy, distorted and/or misaligned fingerprint produced as a 2-D on x-y image, is enhanced and optimized using a hybrid Modified Gabor Filter-Hierarchal Structure Check (MGF-HSC) system model. In face biometric Fast Principal Component Analysis (FPCA) algorithm was used in which different face conditions (face distortions) such as lighting, blurriness, pose, head orientation and other conditions are addressed. The algorithms used improved the quality of distorted and misaligned fingerprint image. They also improved the recognition accuracy of distorted face during authentication. The results obtained showed that the combination of both fingerprint and face improve the overall performance of biometric authentication system in access control.**

***Index Terms*—Biometrics, multimodal, authentication, fast principal component analysis.**

I. Introduction

Biometric system is an automated technique of recognizing a person based on physiological and behavioral traits. The physiological traits include the face, fingerprint, palm print and iris, which remain permanent throughout an individual's lifetime. The behavioral 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 [2].

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]. In this regards, the problem of securing information emerged, since information needs to be managed. Thus, as the method of maintaining security increases, the threat of security breaching also increases. However, Fig. 1 in [2] shows the record of security breaches at financial institutions from 2008 to 2010 in United State.

From the Fig. 1 in [2], it can be observed that there is higher number of hacker, malware and misuse. This is not good enough, particularly for the financial institutions. This record has proved that traditional authentication system cannot handle the growing daily financial customer's transactions across the globe [2]. However, with the advances in biometrics system, it has replaced the use of traditional technique of authentication since biometrics cannot be lost and forgotten [2]. Biometric system is an automatic technique of identifying person based on biological and physiological traits. Biometric technology has presented 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 [3].

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 access control area such as financial institutions.

A. Fingerprint Alignment

Fingerprint alignment is a crucial stage in a fingerprint authentication system. Misalignment is caused by displacement in the query fingerprint image, mostly during the authentication phase. The displacement includes the translation and rotation of a fingerprint image [3]. Fig. 1(a) shows an example of a normal fingerprint image captured in database as template, Fig. 1(b) shows misaligned positions of the same fingerprint at query stage. However, during authentication phase, this misalignment often affects the matching accuracy when compared the query fingerprint with the template in database during authentication [3].

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 rectangular box in Fig. 2 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], [5].

Manuscript received May 5, 2014; revised August 13, 2014. This work was supported in part by the Department of Computer System Engineering, Tshwane University of Technology, South Africa. Paper title: Hybridization of Bimodal Biometric for Access Control Authentication.

The authors are with Tshwane University of Technology, Soshanguve Campus, South Africa (e-mail:zuvaT@tut.ac.za, esanomobayo@tut.ac.za, ngwiraSM@tut.ac.za).

(a). Normal fingerprint (b). Misaligned query fingerprint
Fig. 1. Fingerprint with normal and misalignment.

Fig. 2. Fingerprint with distortion.

C. Face Biometric

In face recognition, there are some features that are important for system recognition. These features include nose, eyes, eyebrows, mouth and nostril [6]. Each of these features has some values or weights to recognize the face. Fig. 3 shows some of the features used in face recognition. The accurate estimation and extraction of human face features are very challenging.

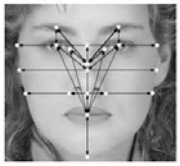


Fig. 3. Some of the features used in face recognition.

D. Face Distortions

The extraction of the human eye at grey level is obtained from valley features. The relationship between human face and other facial feature is that the size of the human face is equivalent to the distance between the eyes that contains the region of eyebrows, eyes, nose and mouth [6], [7]. Consequently, extraction of these features can be affected by several variables such as glasses, facial hair; face impressions etc., these makes extracting and positioning of facial features not to be accurately estimated[6], [7]. Moreover, human face is a 3-D object which is vulnerable to distortion and uneven illumination that can make detecting of true face to be difficult [7]

As discussed, most fingerprint authentication systems address these two challenges separately. This research therefore provides a new bimodal biometric authentication system which has the potential of mitigating the challenges of fingerprint and face which are distortion, misalignment, face feature extraction and illumination for users' access control.

This paper advances the existing bimodal authentication system by addressing problem of distortion and misalignment in fingerprint to improve the security of access control area such financial institutions. The major contributions of this paper 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 (FPCA) 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 FVC 2000a methods and facial images.

The rest of this paper is organized as follows: Section II presents the theoretical background, which includes related work on the MGF algorithm and HSC algorithm; Section III presents the fingerprint authentication system model; section IV 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, and Section V compares the proposed method with related methods. We conclude the paper in Section VI.

II. Theoretical Background

A. Related Research

Several fingerprint approaches have been proposed in 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 in [8]. The proposed bimodal system authentication utilized a neural network for obtaining the matching score between the two biometric traits before performing fusion scores. At the fusion level, the sum Max and product rule were used in fusing the two traits together and the result obtained shows a significant improvement of bimodal biometrics matching when compared with that of direct matching score.

A robust bimodal biometric authentication system based on speech and signature biometric traits was developed [9]. The extraction of speech biometric was done by training the Mcl Frequency Cepstral Coefficient (MFCC) and Wavelet Octave Coefficient of Residual (WOCOR) as a feature vector. The MFCCs and WOCORs from the trained data are modelled using vector Quantization (VQ) and Gaussian Mixture Modelling (GMM) techniques. The signature based biometric system is developed by using Vertical Projection Profile (VPP), Horizontal Projectile Profile (HPP) and Discrete Cosine Transform (DCT) as feature. From the experiment conducted the result shows that bimodal person authentication gives higher performance compared with a single biometric system.

Single modal biometric traits are affected by noisy sensor data, non-universality and thus are susceptible to spoof attack are introduced in [10]. However [10], addressed these issues [10] integrated iris and signature traits, the two bimodal traits were then fused together using user-specific weighting technique which also increases the accuracy of the proposed bimodal biometric system. Although the efficacy of the approach was only tested on iris and signature and not on other biometric modalities.

B. Modified Gabor Filtering Algorithm

The advantage of spatial and frequency properties exhibited by Gabor makes it an important tool in computer vision and image processing. The 2-D Gabor function have

harmonic oscillator consists of a sinusoidal plane wave of specific frequency and orientation in a Gaussian envelope [2].

A ridges and valleys structure has a defined frequency and orientation estimation which helps in removing undesired noise. However it is appropriate to use Gabor filters as a band pass filters to remove the noise and preserve true ridge or valley in the area of the fingerprint where there is no appearance of minutiae [2]. 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.

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

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 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).

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

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 distortion are expressed in equation (4) as T in harmonic oscillation and also the frequency domain in equation (1) is represented with a cosine function in equation (3). Modulating the periodic function $F(X_1, X_2, T)$ to obtain;

$$\begin{aligned} g(x, y, T, \varphi) &= h_x(x, T, \varphi).h_y(y, \varphi) \\ &= \left\{exp\left(-\frac{x_\varphi^2}{2\sigma_x^2}\right)cos\left(\frac{2\pi x_\varphi}{T}\right)\right\}\cdot\left\{exp\left(-\frac{y_\varphi^2}{2\sigma_y^2}\right)\right\} \end{aligned} \quad (3)$$

The merit of Modified Gabor filter approach is it 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 [2]. A minutia-matching algorithm based on composite features can be used to address the issue of rotation and geometrical transformation. Fig. 4 shows a typical example of composite feature representation.

Thus, the local structure matching for query fingerprint minutiae and template minutia is represented in triplet form, as shown in equation (4):

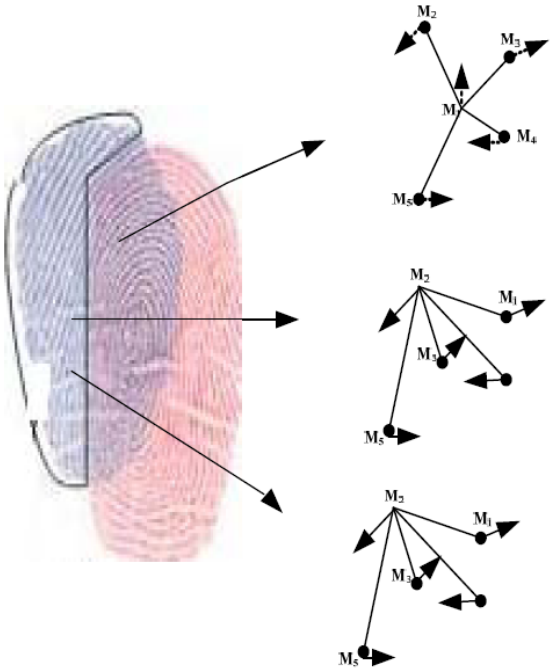


Fig. 4. Composite feature representation [2].

$$d_{i\_j}, \varphi_{i\_j}, \theta_{i\_j} \quad (4)$$

d_{i_j} is the length of l_{i_j} connecting M_i and M_j .Mathematically expressed in equation (5).

$$d = \sqrt{(x_j - x_i)^2 + (y_j - y_i)^2}, \quad (5)$$

φ_{i_j} is the difference between angle of M_i and M_j as in equation (6).

$$\varphi = \alpha - \beta_0 \quad (6)$$

$$\alpha_i = \tan^{-1}\left(\frac{y_j - y_i}{x_j - x_i}\right) \quad (7)$$

β_0 is the angle of M_i and β_1 is the angle of M_j, θ_{i_j} is the counter-clockwise angle between the orientation of M_i and direction from M_i and M_j

The merit of Hierarchical Structure Check is it addresses issue of rotation and translation pf parameter in fingerprint image.

D. Face recognition Using Fast Principal Component Analysis (FPCA)

The Fast Principal Component Analysis (FPCA) procedure consists of taking a sample of a grey scale image in $2D$ matrix and transformed into $1D$ column vector of size $N^2 \times 1$ by placing the matrix column consecutively [6].

These column vectors of n images are placed column wise to form the data matrix (image set) X of dimension $N^2 \times n$.

The mean q be the mean vector of the data vectors in matrix X given in equation (5)

$$q = \frac{1}{n}\sum_{i=1}^{k} x^i \tag{5}$$

The vector of data matrix X are centered by subtracting the mean vector Q from all the column vectors of X to obtain covariance matrix C of the column vector in equation (6).

$$C = \overline{YY^t} \tag{6}$$

The Eigen values and corresponding eigenvectors are computed for covariance matrix as in equation (7).

$$CV = \Lambda V \tag{7}$$

where Λ is the set of eigenvectors associated with eigenvalues Λ.

Set the order of the Eigen vectors according to their corresponding eigenvalues from high to low. This matrix of eigenvalues is Eigen space V. The data matrix X is projected onto the Eigen space to get P consisting n columns as in equation (8).
where

$$P = V^t X \tag{8}$$

In the recognition phase, the image I to be recognized is converted to 1D vector and form J which is projected onto the same Eigen space to get Z in equation (9).

$$Z = X^t J \tag{9}$$

The Euclidean distance d between Z and all projected samples in P is measured using norm of an image A and B given in equation (10).

$$L_2(A,B) = \sum_{i=1}^{N} (A_i - B_i)^2 \tag{10}$$

The projected test image is compared to every projected training image and the training that is found closet to the test image is used to identify the training image.

The advantage of Fast Principal Component Analysis (FPCA) is that it is faster when used on large database and also gives accurate face recognition result.

III. Proposed System Architecture

The system architecture described in Fig. 6 for a bimodal biometric authentication system is divided into two stages: (i) fingerprint authentication using MGF-HSC approach and (ii) Face recognition using fast PCA.

A. Fingerprint Authentication Using MGF-HSC Approach

As indicated in Fig. 5, the fingerprint authentication phased is divided into two modules, namely: (i) enrolment module and (ii) authentication module

1) The enrolment phase

According to the system architecture in Fig. 5, 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:

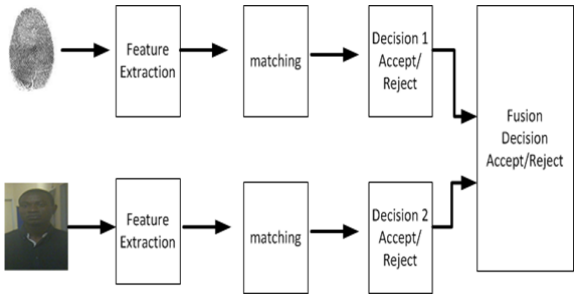


Fig. 5. System architecture.

2) Image acquisition stage

As reflected in Fig. 5, the fingerprint images of users are captured with a fingerprint reader and are saved in a database with other relevant information.

3) 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 Fig. 5, 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.

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

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

STEP1: 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 $w \times l$ is built at each center. The second derivatives and the magnitude of fist 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.

B. Authentication Phase

According to the system architecture depicted in Fig. 5, 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:

1) Alignment stage using a composite hierarchal structural check (HSC)

Fingerprint misalignment shown in the bottom left area of Fig. 4 is a main stage in the fingerprint authentication system, caused by the displacement of the fingerprint image during the authentication stage. The performance of the fingerprint-matching algorithm relies heavily on the accuracy of fingerprint alignment. In order to improve the performance of the fingerprint authentication system, the template and query fingerprint should be aligned. This process occurs in the following ways:

The HSC that consists of triplet composite features, which are the Euclidean distance (d), the angle between two minutiae and the angle between orientations (θ), is constructed. A reference region is located and an adaptive box is drawn around the reference point. The radius R is located, all minutiae M_i are marked and the composite features are constructed inside. The composite feature forming a series of coordinate points and corresponding similarities between the query fingerprints with the template in the database is estimated with respect to all minutia, rotated and translated at different angles and in different directions.

2) Matching stage

Algorithm 2: Composite Matching of two Fingerprints by Hsc

INPUT: ML=Minutiae-List,Pt=predefined threshold, M_{ax}=Minutiae-a.x,May=Minutiae-a.y, MM=Matched-minutiae, M_{by}=Minutiae-b.y, M_{bx}=Minutiae-b.x, NM_a=NORMALIZE(minutiae a.angle)

NM_b=NORMALIZE(minutiae-b.angle), X_T=X-tolerance,Y_T=Y-tolerance, T=tolerance,ΘT=ANGLE-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 (Max . Mbx) ≤ XT and
STEP 10:   if (May . Mby) ≤ YT and
STEP 11:    if NMa- NMb≤ θT-T
STEP 12:  return true
```

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.

From algorithm 2, 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.

C. Face recognition Using Principal Component Analysis (PCA) Algorithm

In developing face recognition system there are stages that are very crucial in contributing to the success of the system. The following system architecture of face recognition process in Fig. 5 Face recognition is divided into the following stages: (i) Image pre-Processing stage (ii) Feature extraction using fast Principal Component Analysis (FPCA) and (iii) Face matching

1) Image pre-processing stage

The acquired images are aligned at the pre-processing stage and the cropping operations are performed at this stage before face image is passed to feature extraction stage.

2) Training stage

In the training stage, the acquired image that has passed through an image pre-processing stage such as histogram normalization to adjust the contrast process of the image in order for the image output to have a uniform distribution of grey values and to reduce the light intensity variation level in the grey.

Algorithim 3: Training Stage Face Using Fast PCA

INPUT: Face image N

OUTPUT: Trained face

STEP 1: input face image N

STEP 2: for each x_1, compute its projection $\{u_1\}_1^N = 1 \in R^D$ for image vector dimension y

STEP 3: compute the weight w from each vector

STEP 4: compute the mean vector m

STEP 5: subtract each x_1 by m to get φ_1

STEP 6: calculate the variance matrix Σ of all φ_1 (D-by-D) matrix

STEP 7: calculate set of $\Sigma\,(D-by-N-1)$ matrix

STEP 8: Preserve the M largest Eigen vector based on the Eigen value

STEP 9: $U_{\varphi_1}^T$ is Eigen face representation

From algorithm 3, M is vector dimensional representation and M projection is an Eigen face having a basis $(M << D)$. The D-dimensional vector is used for dimension reduction. The same procedure is followed during the training stage before comparing the image vector obtained with the image in the database to determine their corresponding similarities.

3) Testing stage

During this stage, 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. 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.

From algorithm 4, the face image passed through the image pre-processing stages and features are extracted again in which the features are represented in a vector form. The vector obtained during the testing is classified if normalized face image E_1 is greater than Euclidean distance E_2 the image is recognized as face and if otherwise it is recognized as non-face.

Algorithm 4: Test Face Image

INPUT: $T = \varphi_i \times \gamma$, $\mu = \tau^T \times v$,
$\gamma =$ eigenvector,
$E_1 =$ normalized image,
E_2 =Euclidean distance,
$\mu =$ space vector

OUTPUT: Test face image

STEP 1: input trained image
STEP 2: reshape and centered image v=reshaped-mean
STEP 3: center project test vector into face space $\mu = T^r * v$
STEP 4: Calculate square norm of E_1, $E_1 = [\text{norm}(\eta - \mu)]^2$
STEP 5: Project μ to another space by multiply it by T, $\varsigma = \mu \times T$
STEP 6: Calculate Euclidean distance, E_2 between v and ς

$$E_2 = \|v - \varsigma\| = \sqrt{\|v\|^2 + \|\varsigma\|^2 - 2 * v\varsigma}$$

STEP 7: Normalized E_1 and E_{21} for classification

$$\frac{E_1}{\|T\|}, \frac{E_2}{\|T\|}$$

STEP 8: Compare E_1 to E_2
STEP 9: If $E_1 > E_2$
STEP 10: image is face
STEP 11: Otherwise
STEP 12: Non face

4) Matching Stage

At the matching stage the tested facial image is compared to every projected training image, the training image that is similar to the test image is then used to identify the training face image.

IV. 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 [2]. The following evaluation models were chosen as quantitative scheme [2]: (i) the False Rejection Rate (FRR) and (ii) the False Acceptance Rate (FAR) [9]; the schemes are computed by the following formulas in equations (11)-(12):

$$FRR = \frac{G}{N} \tag{11}$$

where G the number of imposter's fingerprint is rejected and N is total number of genuine tested.

$$FAR = \frac{I}{N} \tag{12}$$

where I the number of imposter's fingerprint is accepted and N is total number of genuine tested.

All these equations are used as objective evaluation schemes for degraded and fingerprints matching.

The percentage of System Accuracy (SA) is computed by the following formula in equation (13).

$$SA = \frac{M}{P} \times 100 \tag{13}$$

where SA is the system accuracy, M is the total number of organized fingerprint image sample and P is the total number of fingerprint sample.

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

V. Experimental Evaluations

One of the objectives of this paper is to apply the theory of our approach in practice by emphasizing applications and carrying out practical work on fingerprints with distortion and alignment, as well as face recognition using MATLAB, as shown in Fig. 6 and Fig. 8 respectively. The fingerprint and face images are captured with a Futronic fingerprint scanner and canon digital camera respectively. An original fingerprint with distortions and overlapping is shown in Fig. 2 and 3.

In calculating the percentage of noisy region, the fingerprint image is divided into 3× 3 window size; the CN method extracts the ridge endings and bifurcations by examining the local neighborhood of each ridge pixel using a 3 × 3 window. After extraction using the CN concept, the region with distortion is estimated using a noise detector scheme in (14). The scheme states that: (i) if a pixel x has at least one pixel y among the other eight pixels in the neighborhood, 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 neighbors, it is considered to be distorted; this is shown using equation (14):

$$x = \begin{cases} x_{ij}^0 & K\{|x - y| \le D_1\} \ge N_1^{th} \\ x_{ij}^n & \text{else} \end{cases}. \tag{14}$$

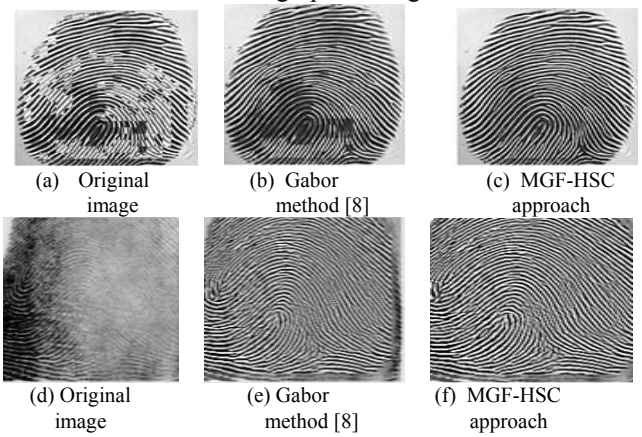
D_1 is adopted as the maximum depth difference between the similar x and y pixels and is often assumed to be eight pixels in the neighborhood. N_1^{th} is 1 as every pixel is assumed to be similar to at least 1 pixel, and K is the number of y pixels that satisfies equation (14) while the distorted pixel is eliminated.

However, this work focuses on bimodal biometrics and enhancing distorted and misaligned fingerprint images. In terms of performance measures, the FAR and FRR, are computed when evaluating the result of the proposed MGF-HSC in Fig. 6.

A. Experiment 1: Benchmarking our Approach with Publicly Available Templates and Methods

The aim of benchmarking is to access the qualitative

performance of our proposed approach on FVC 2000a DB2 fingerprint database where fingerprint are noticeably different from real-life fingerprint images.



(a) Original image (b) Gabor method [8] (c) MGF-HSC approach

(d) Original image (e) Gabor method [8] (f) MGF-HSC approach

Fig. 6. Images (a), (c), and (e) are real-life fingerprints with distortion and misalignment; images (b), (d) and (f) are the enhanced fingerprints.

The original fingerprints in Fig. 6 (a) and Fig. 6(d) respectively contain distortion. Gabor filtering and our MGF-HSC approach were used to enhance and filter the distorted regions. Fig. 6 (b), Fig. 6 (c), Fig. 6 (e) and Fig. 6 (f) show the result of Gabor filtering and our MGF-HSC approach respectively.

In Fig. 5, the MGF-HSC approach is benchmarked with the Gabor method. One can see the result of the MGF-HSC approach in Fig. 6(c) and Fig. 6 (f) respectively, which show better enhancement clarity compared to the images in Fig. Fig. 6 (b) and Fig. 6 (e) respectively.

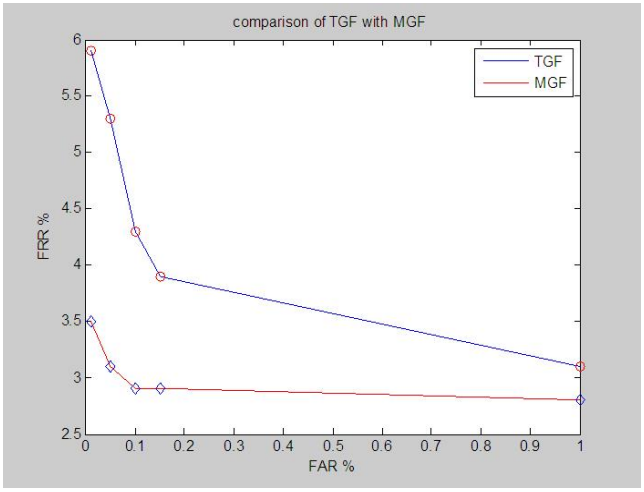


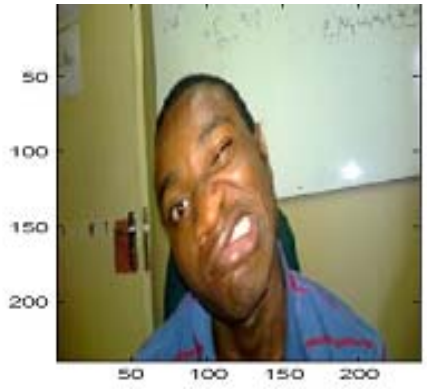
Fig. 7. Graph for comparing modified gabor filter with traditional gabor filtering.

The graph in Fig. 7 shows that MGF-HSC approach gives a lower FAR and FRR compared to the Tradition Gabor this is due to the fact that the parameter selection are not based on assumption. Also the MGF-HSC approach is able to enhanced and extract feature better than TGF.

B. Experiment 2: Performance of Fast PCA on Face Image

In this experiment the study endeavored to find the performance of the fast PCA on distorted query face images. Fig. 8(a) illustrates a distorted face image and Fig. 8 (b) gives the image that was retrieved. This showed how the system was able to bring the original image of the distorted image.

The result in Fig. 9 shows the graphical performance of our fast PCA approach when a certain percentage of the images of the database are distorted and then used as query images. The graph in Fig. 9 shows that the system gives 97.86 % accuracy when the original faces (0% distortion) are used as query images. The worst case scenario when all the images in the database are deformed and used as the query images, the performance of the system is approximately 79% accurate.



(a). Query facial image.

(b). Output.

Fig. 8. Facial image with distortion and trained using fast PCA technique.

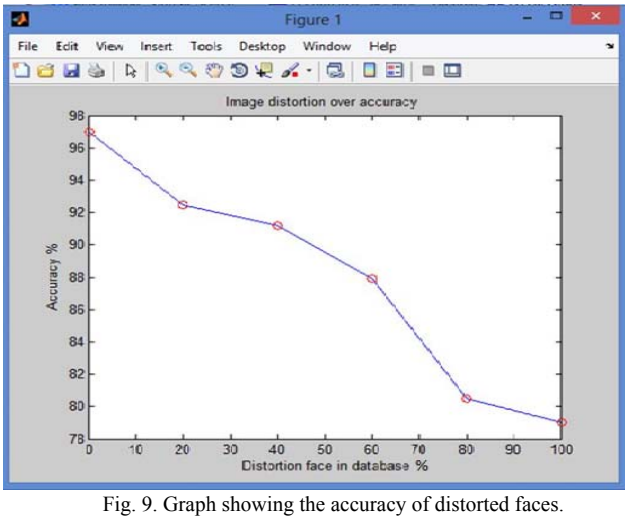


Fig. 9. Graph showing the accuracy of distorted faces.

VI. Concluding Remarks

In this research, bimodal biometric system for user access control authentication was the main interest. An effective and efficient authenticating system for a user access control entails user having an effective physiological or biological

traits as a component of biometric system. The fundamental components of bimodal biometric system are image pre-processing, image segmentation, image feature extraction and image matching. In order to fulfil the objective of this research work reviews of literature, designing of new system model was done. And evaluation of the system was done. The following section elucidate on the work done to fulfil the main objective of bimodal biometric system for authentication in access control.

A prototype biometric system which integrates fingerprints and faces in authenticating a person for user access control has been developed. The system overcomes the laxities of both fingerprint authentication system and face recognition systems. The proposed system works in authentication mode. Experimental results demonstrate that the proposed system perform very well. It meets the security as well as accuracy requirements.

The bimodal biometric system for authentication was finally built. The system was tested on users with distorted fingerprint. The challenges come when a fingerprint is completely distorted. To tackle this challenge a hierarchal structural check algorithm was used for matching and this only utilized the available query minutiae to compare with the template minutia for authentication. The fingerprint authentication system performed well. Integrating fingerprint authentication as well as face recognition system was done. The evaluators were satisfied with the system.

REFERENCES

[1] V. B. R. T. A. U. S. S. Service, "A Study of Data Breach Investigation Record in Financial Institution," 2010.

[2] O. A. Esan, S. M. Ngwira, and I. O. Osunmakinde, "Bimodal biometrics for financial infrastrucutre security," presented at the Information Security South Africa (iSSA), South Africa, 2013.

[3] L. Hong and A. Jain, "Integrating faces and fingerprints for personal identification," *IEEE transaction on Pattern Analysis and Machine Intelligence,* vol. 20, p. 12, 1999.

[4] H. A. Aboalsamh, "Vein and fingerprint biometrics authentication-future trends," *International Journal of Computer and Communications,* vol. 3, 2009.

[5] A. Senior and R. Bole, "Improved fingerprint matching by distortion removal," *IEICE Trans. Inf. System,* vol. 8, pp. 825-831, 2001.

[6] Neerja and E. Walia, "Face recognition using improved fast PCA algorithm," *Congress on Image and Signal Processing,* 2008.

[7] K. W. Wong, K. M. Lam, and W. C. Siu, "An efficient algorithm for human face detection and facial feature extraction under different conditions," *The Journal of Pattern Recognition,* vol. 34, 2004.

[8] B. Biggio, Z. Akthar, G. Fumera, G. L. Marcialis, and F. Roli, *Security Evaluation of Biometric Authhentication Systems Under Realistic Spoofing Attacks,* 2009.

[9] M. N. Eshwarappa and M. V. Latte, "Bimodal biometric person authentication system using speech and signature features," *International Journal of Biometrics and Bioinformatics (IJBB),* vol. 4, pp. 147-160, 2005.

[10] S. Viriri and J.-R. Tapamo, *Integrating Iris and Signature Traits for Personal Authentication using User-Specific Weighting,* 2006.

Tranos Zuva is with the Department of Computer Systems Engineering at Tshwane University of Technology, Soshanguve South Campus, and South Africa. He has published many articles in local and international conferences and journals.

Omobayo A. Esan is currently a doctoral student in the Department Computer Systems Engineering, University of Technology, Soshanguve South Campus, South Africa.

Seleman M. Ngwira is working as a professor in the Department of Computer Systems Engineering, University of Technology, Soshanguve South Campus, South Africa