Health Care Infrastructure Security using Bimodal Biometrics System

Omobayo A Esan, Selema Ngwira
Computer System Engineering
Tshwane University of Technology, TUT
Pretoria, South Africa
{esanoa, ngwirasm}@tut.ac.za

Tranos Zuva, Lerato Masupha
Computer System Engineering
Tshwane University of Technology, TUT
Pretoria, South Africa
{zuvaT, masuphaLE}@tut.ac.za

Abstract— **Ensuring the security of patient medical record has become an important issue with this current l electronic medical record, this is due to the fact that patient confidential health information can be access, view and edit on Personal Computer (PC) at any time. In order to protect the patient health confidential information, this research use bimodal biometric (face and fingerprint) authentication to secure patient Electronic Medical Record (EMR). The bimodal biometric (fingerprint and face) are often affected by distortions which are caused by environmental noise such as oil, wrinkles, dry skin and dirt. These often affect the biometric system accuracy during authentication stage. In order to protect and improve the accuracy of patient Electronic medical Record (EMR) in health care infrastructure, this study introduced Modified Gabor Filter (MGF), a fast Principal Component Analysis (PCA) algorithm with Support Vector Machine (SVM) to address the issues of fingerprint and face image distortion respectively. From the experiment conducted from 1000 patients with 20 fingerprint and face image from each to give 50 test cases. The result shows that the proposed bimodal biometrics approach gives a lower False Rejection Rate (FRR) and False Acceptance Rate (FAR) and this shows better constructive accuracy of our system on patient EMR in health care infrastructure.**

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 [1],[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 [1],[2]. In this regards, the problem of securing information emerged, since information needs to be managed and secured data [1].

However, in this present technological age securing of Electronic Medical Records is becoming an increasingly important problem due to the fact that most health professionals can edit and view a patient’s medical record using a tablet PC at any point of time across the network [3]. Thus, this has subjected patient’s medical information to lack of privacy and confidentiality. It is therefore of high importance to address this issue of unsecured patient medical record released to health practitioners without the permission of authorized patient [4].

According to the study conducted by High bit Security in 2011on patient privacy and data breach security in United State of America, the investigations shows that 94% of hospital survey suffers data breaches and this cost US about $7 billion annually. Fig. 1 shows the record of security breaches at health care institutions from 2008 to 2010 [5].

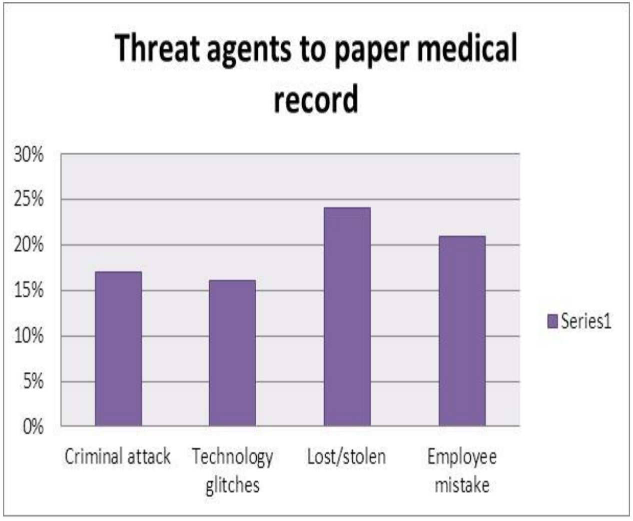


Fig. 1. Visualization of record of security breaches in High bit Security

One can see in Fig. 1 that from 2008 to 2010, that most years recorded higher number attacks exceeded 20%. This is not good enough, particularly for the health sector, where the adaptation of a fingerprint and face Electronic Medical Record (EMR) authentication system can greatly reduce the high rate of threat agents to a minimal number.

Although, the existent of the Electronic Medical Record (EMR) approach has not emerged in developing countries higher threat agents occur frequently not only in developing countries the use of paper filing systems for keeping patient records are the predominant techniques for access patient information, and this is vulnerable to theft, forgery and loss [3]. However, in the developed countries such as United State of America, United Kingdom and Canada electronic records systems are used, there is high threat rate of patient data breaching, thus subject patient medical information to theft, lost and lack of privacy [4].

Biometric technology has presented several advantages over conventional security methods, as there is no need for keeping the user information inside a filing cabinet or on tablet PC that could easily be access by anybody at any point or stolen [3],[4]. However, in spite of these advantages, fingerprint and face authentication systems still present a number of limitations, including fingerprint distortions as well as face with distortions and back ground illumination. It is thus of special relevance to address these limitations for the benefit of patients Electronic Medical Record (EMR) keeping in health care institutions.

A. *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. Thus, these areas with distortion, which may lead to the creation of a significant number of spurious minutiae, cause a large percentage of genuine minutia to be ignored and large error in localization[6].

B. *Face Identification*

In face recognition, the extraction of human face and valley features 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 [7].

As discussed, most fingerprint authentication systems are unable to address these challenges, while some focus only on addressing either of the two. This paper advances the existing system by mitigating both challenges, enabling especially health care sectors to address these issues. The major contributions of this paper are as follows:

- Proposal of a bimodal biometrics constituting of incorporating Modified Gabor Filter (MGF), Principal Component Analysis (PCA) with Support Vector Machine (SVM) as a two-level security for patient Electronic Medical Record (EMR) authentication.
- Extracting feature from distorted face image.

The rest of this paper is organized as follows: section II presents the theoretical background, which includes related work on the MGF, PCA with SVM algorithm; section III presents the fingerprint and face medical record authentication system model; section IV critically presents visual inspection and quantitative experimental evaluations of the approach using lightly and heavily distorted fingerprint images and section V concludes the paper.

II. THEORETICAL BACKGROUND

A. *Related Research*

Several biometric approaches have been proposed in literature for securing records. They include: research in [10], proposed a system that automated the whole process of taking attendance and maintaining its records in an academic institute. Nawaz, et al used automated method to replace manual attendance which takes longer time using fingerprint in which all the records are safe in computer server.

According to [3], a frame work for unified electronic record using biometric system was proposed. The technique replaces securing patient record from archaic paper based system with biometric technology. The approach shows a better secured technique but Dwayne et al fail to show the real-life performance of the system.

Also, research in [4], proposed a technique of securing patient medical records using biometrics system authentication by addressing the issue of health professional that usually edit and view patient record on tablet with get authorized permission from the patient. Stephen et al analyzed the performance of the proposed system by combining on-line signature and voice on Personal Computer (PC) using dynamic program and commercial software development. The approach gives an Equal Error Rate (EER) of 0.86%, although very small databases of 50 users were used.

Unlike the above-mentioned methods, this study proposes integration of MGF, PCA and SVM approach to address the fingerprint distortions and face distortion and illumination issues.

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 [8]. 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 [8]. 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 as in.

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

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 (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 as in (3).

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

C. Principal Component Analysis (PCA)

PCA is one of the most widely used techniques for face recognition. In PCA face-based authentication, 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 [7].

The 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 as in (4).

$$n = \frac{1}{k}\sum_{i=1}^{k} y \quad . \tag{4}$$

The merit of PCA is that it is faster and gives accurate face recognition.

D. Support Vector Machine (SVM)

SVM is an effective supervised learning method used in machine language for both classification and recognition processes. If a set of face samples are given, and each samples are put into a noticeable categories. SVM classification training algorithm tries to predict whether a new sample falls into one category or not [9], [10]. The SVM hyper plane that can separate two classes as in (5).

$$\min_{w,b} \frac{1}{2}\|w\|^2 \text{ Subject to } y_i(w.x_i + b) \geq 1 \tag{5}$$

For all i, where w has the same dimensionality as in (6).

$$f(x) = w.\phi(x) + b = \sum_{i=1}^{i} C_i \phi(x_i).\phi(x) + b \tag{6}$$

However, the normal hyper plane can be written as a linear combination of the training point in the feature space. Thus, for optimization, map the point into feature space by a kernel function, which can be defined by as dot product for two points in the feature space as in (7).

$$k(x_i, x_j) \equiv .\phi(x_i).\phi(x_j) \tag{7}$$

Thus, gives equation (8).

$$f(x) = \sum_{i=1}^{i} C_i k(x_i, x_j) + b \tag{8}$$

Where most of the coefficient C will be zero, only the coefficients of the points closest to the maximum margin hyper plane in the feature space will have non zero coefficients.

The advantage of SVM is that it can achieve a better generalization performance compare to other methods.

III. PROPOSED BIMODAL BIOMETRICS MODEL

The system model described in Fig. 2 for a bimodal biometrics authentication system is divided into two stages: - (A) fingerprint authentication using the MGF approach and (B) face recognition using PCA and SVM.

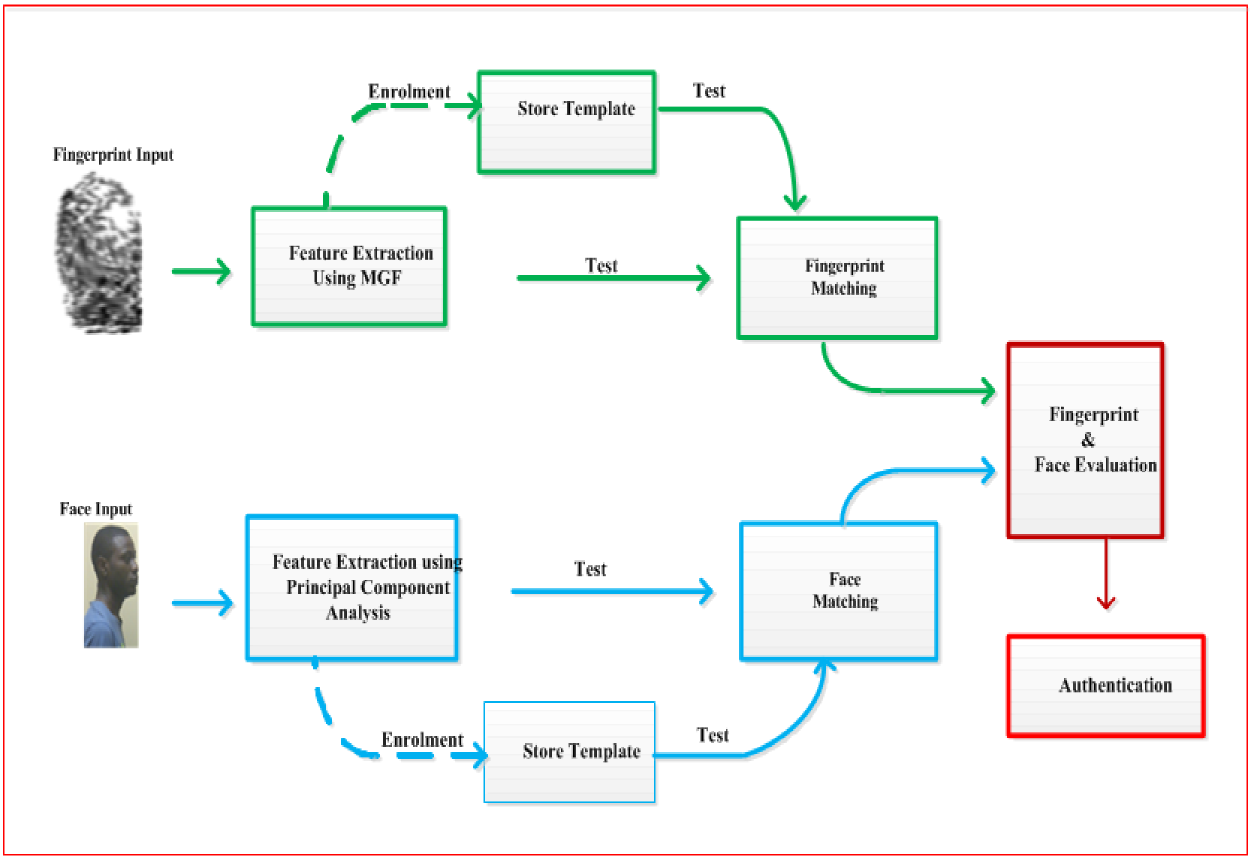


Fig. 2. System Model

A. *Fingerprint Authentication using MGF*

As indicated in Fig. 2, the fingerprint authentication phase is divided into two phases, namely the. (i) enrolment phase and (ii) authentication phase.

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:

Image acquisition stage

As reflected in Fig. 2, the fingerprint images of users are captured with a fingerprint reader and are saved in a database with other relevant information.

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. 2, 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 as 1's respectively. The cross number (CN) concept is used for extraction of fingerprint features as either ridge-ending or bifurcation.

Authentication Phase

According to the system model depicted in Fig. 2, 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 and this is done during the matching stage.

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.

B. *Face Recognition using PCA-SVM algorithm*

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

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.

Testing Stage

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.

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.

C. *Evaluation Techniques*

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 [22]: (i) the False Rejection Rate (FRR) and (ii) the False Acceptance Rate (FAR) [6]; the schemes in [6] are computed by the following formulas:

$$FRR = \frac{G}{N} \tag{9}$$

where G is number of genuine fingerprint rejected and N is total number of genuine tested

$$FAR = \frac{I}{N} \tag{10}$$

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 measuring distorted fingerprint and face enhancement.

IV. EXPERIMENTAL EVALUATIONS

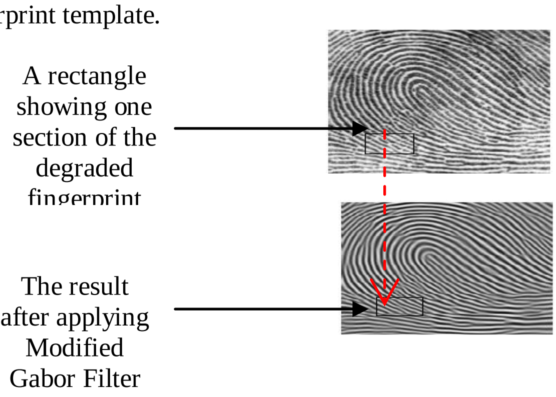
One of the objectives of this paper is to apply the theory of our approach in practice by emphasising applications and carrying out practical work on fingerprints and face with distortions, as well as face recognition using MATLAB.

During the experiment thousand (1000) good fingerprint images were enrolled into the database. A second set of the same one thousand (1000) fingerprint images were captured but without consideration of their state, these were then used as query fingerprint images. Some samples of the fingerprint images captured for querying the database are shown in Fig. 3 with various degree of degradation. One thousand (1000) more fingerprint images were collected but were not part of the database. These one thousand (1000) fingerprint images where used as query to the database to measure FAR of our system. All of the second set fingerprint images were used as query fingerprint images to measure the FRR of the system.

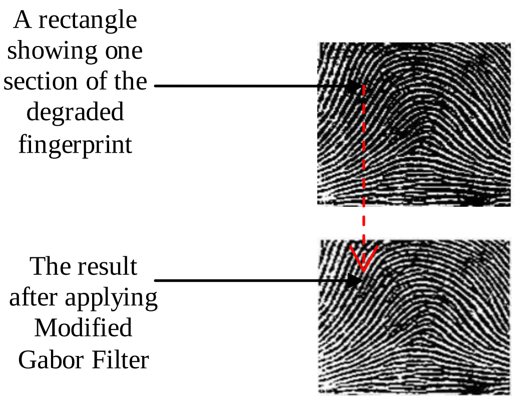
However, this work focuses on bimodal biometrics and enhancing distorted fingerprint and face images. In terms of performance measures, the result of the proposed MGF approach, as shown in Fig. 3, 6 and 7 respectively, the accuracy of the face with distortion is computed in Fig. 5 when evaluating using proposed PCA-SVM algorithm,

Experiment 1: Qualitative inspection of Fingerprint Identification using MGF

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


A rectangle showing one section of the degraded fingerprint
The result after applying Modified Gabor Filter

(a)


A rectangle showing one section of the degraded fingerprint
The result after applying Modified Gabor Filter

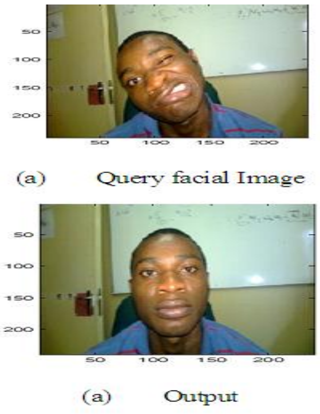
(b)

Fig. 3. Images (a) and (c) are real-life fingerprints with distortion and misalignment; images (b) and (d) are the enhanced fingerprint.

The results of enhancing a degraded fingerprint using Gabor filter can be seen in Fig. 3. The top fingerprint image shows the original image and rectangle indicates a degraded section of the image. When Modified Gabor Filter (MGF) was applied the bottom fingerprint image was obtained and rectangle indicates the repaired section of the degraded part.

Experiment 4: Performance of PCA- SVM algorithm on face image

In this experiment the study endeavoured to find the performance of the PCA-SVM on distorted query face images. Fig. 4(a) illustrates a distorted face image and Fig. 4(b) gives the image that was retrieved. This showed how the system was able to bring the original image of the distorted image.



(a) Query facial Image

(a) Output

Fig. 4. Facial image with distortion and trained using PCA-SVM algorithm

The result in Fig. 5 shows the graphical performance of our PCA-SVM approach when a certain percentage of the images of the database are distorted and then used as query images. The graph in Fig. 5 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.

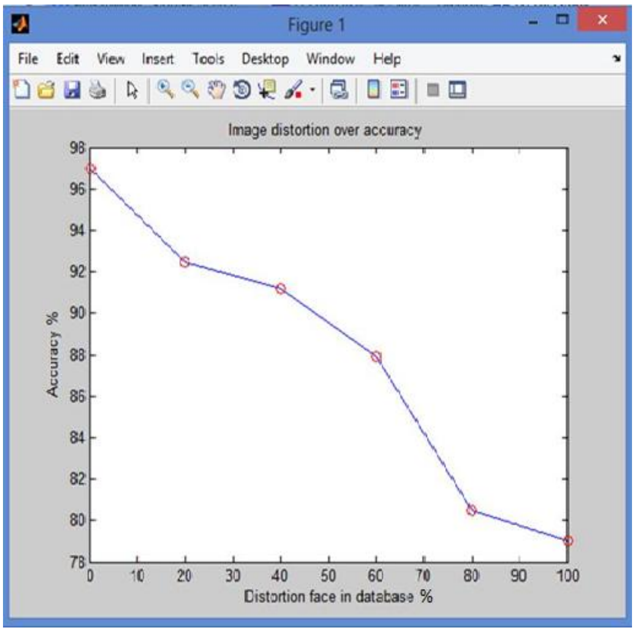


Fig. 5. Graph showing the accuracy of distorted faces

Experiment 5: Performance of the bimodal biometrics system

AUTHORIZED USER ATTEMPT:

FINGERPRINT & FACE IN DATABASE

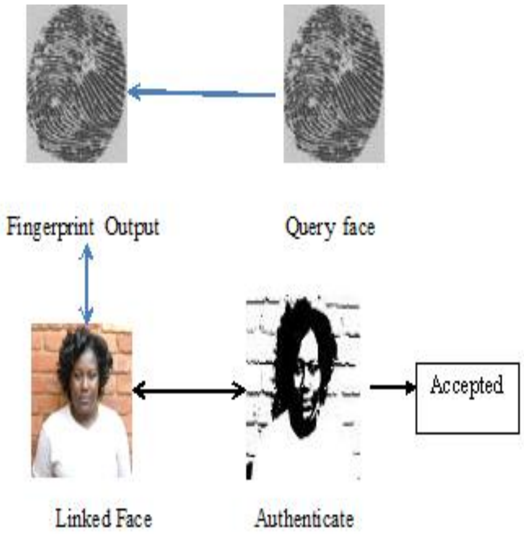


Fig. 6. Combined face with fingerprint image for authorized user

IMPOSTOR USER ATTEMPT:

FINGERPRINT & FACE IN DATABASE

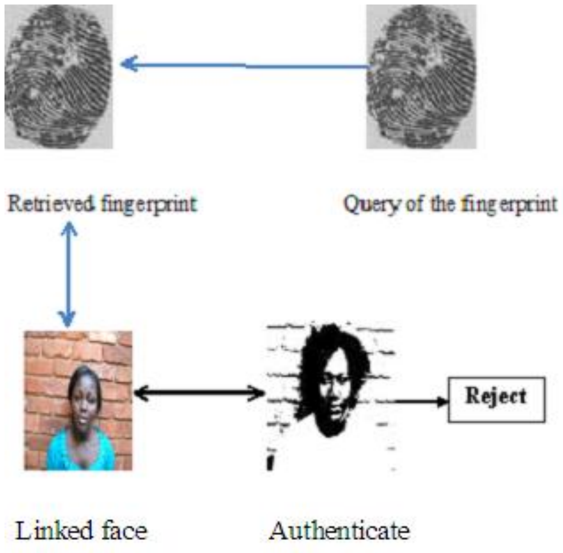


Fig. 7. Combined face with fingerprint image accessing by unauthorized user

In the database the fingerprint is linked with face image. When the database is queried with the fingerprint the system retrieves the matching fingerprint with the face but the face is hidden from the user. The system then does authentication of the retrieved face against the query face image. If they are the same then the system gives accept otherwise reject. This can be seen in Fig. 6 and Fig. 7. In Fig. 6 there is acceptance because the fingerprint retrieved is linked with face which is the same as the query face image. Fig. 7 is a reject showing an excellent performance of the bimodal authentication system.

V. CONCLUDING REMARKS

We have proposed and demonstrated the use of a bimodal biometric approach for addressing the issue of record keeping in Electronic Medical Record (EMR) for health care infrastructure. We conducted experiments using the MGF, PCA-SVM algorithm to address the issue of distortions in fingerprints and face during authentication.

The experiment conducted on distorted fingerprint image shows that modified Gabor Filter gives more accurate in preserving the fingerprint topology. And advantage of MGF helps in parameter selection for image –independent. The Principal Component Analysis helps in authenticating the retrieved face against the query face image as shown in Fig. 6 and Fig. 7 respectively.

In future work, the research can be explored further in different forms, including (i) using multi-biometrics for authentication (ii) the correct algorithm for matching score of multimodal authentication can be looked into and (iii) also in future, the proposed bimodal biometric can be applied to other application such as student attendance, Home affair, voters registration and other access control area.

ACKNOWLEDGMENTS

The authors gratefully acknowledge the financial support of Tshwane University of Technology.

REFERENCES

[1] O. A. Esan, T. Zuva, S. M. Ngwira, and K. Zuva, "Performance Improvement of Authentication of Fingerprints using Enhancement and Matching Algorithms," *International Journal of Emerging Technology and Advanced Engineering,* vol. Vol. 3, 2013.

[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. 3, 2011.

[3] D. C. Leonard, "A Framework for the Creation of a Unified Electronic Medical Record Using Biometrics," *Data Fusion and Belief Theory,* 2007.

[4] S. Krawczyk and A. K. Jain, "Securing Electronic Medical Records using Biometric Authentication," masters, Computer System Engineering, Michigan State University, East Lansing MI 48823, USA,, 2007.

[5] H. B. Security, "2/3 of all data breaches Preventable with Proactive Security Testing, new Ponemon Institute Study Documens Breach Causes and Costs," 2013.

[6] 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.

[7] Neerja and E. Walia, "Face Recognition Using Improved Fast PCA Algorithm," presented at the 2008 Congress on Image and Signal Processing, 2008.

[8] J. Yang, L. Liu, T. Jiang, and Y. Fan, "A modified Gabor filter design method for fingerprint image enhancement," *Elsevier Science,* 2003.

[9] X. Weimin, " Facial Expression Recognition Based on Gabor Filter and SVM " *Chinese Journal of Electronics* vol. 15, 2006.

[10] P. J. Philips, "Support Vector Machines Applied to face Recognition," *Advances in Neural Information Processing System II* 1999.