MITIGATING FACE BIOMETRIC ON ELECTRONIC MEDICAL RECORD

Omobayo A. Esan, Tranos Zuva, Selema Ngwira, Lerato Masupa
Tshwane University of technology
Department of Computer System Engineering
X680 Pretoria/South Africa
{esanoa, zuvaT, ngwiraSM, masupaLE}@tut.ac.za

ABSTRACT
With the current movement of patient filing system from paper-based system towards Electronic Medical Record (EMR) system, it is necessary to protect patient privacy on EMR efficiently. This research incorporate faces biometric system into EMR in order to provide a two-layer security for patient confidential information. However, the issue of face with distortion such as expressions, aging, background illumination etc. which often affects the performance of face biometric system during authentication stage was addressed. We utilized optimized Principal Component Analysis and Support Vector Machine (PCA-SVM) to extract features and address this issue of patient's face with distortions. We conducted **a**n experiment with 100 test cases. This result shows that facial biometrics can be used for securing patient electronic medical record in hospitals based on the system accuracy obtained. The result demonstrated 78% system performance accuracy with distorted face, which shows that optimized PCA-SVM exhibit a reliable performance for promising security work in term of False Rejection Rate(FRR) and False Acceptance Rate (FAR).

KEY WORDS
Authentication, Distortion, Electronic Medical Record, Principal Component Analysis, Support Vector Machine.

1. Introduction

Reliable user authentication is becoming an increasingly important task in this current age [1]. The effects of an insecure authentication system in health care environment can be disastrous and may leads to loss of patient confidential information and data compromised data integrity [1].

With a fast growing in population and increase in the number of patient in hospital, the use of traditional filing record has become an obsolete technique of securing patient medical record [1].

The traditional paper-based filing technique in health care involve patient authentication using password, IDs (identifiers), identification cards, token. This prevailing technique suffers from various limitations such as it can easily be stolen, forgotten and misplaced [1]. It is obvious that the patient information are discrete and for any physician to access the patient information, such physician must adhere to the policies of Health Insurance Portability And Accountability acts (HIPAA) for proper accessing of patient information [1] .

However, securing of patient medical confidential information through paper-based filing system is challenging. In order to consider the patient's private confidential data security within the health care system, there is need to move from paper-based system. The use of Electronic Medical Record (EMR) has been the predominant method for storing and retrieving patient health information in modern medical centers [1]. EMR has a potential advantage in hospital such as improving service quality, reducing medical errors, security etc. [1].

Despite these benefits, there are some drawbacks associated with EMR such as accessibility of patient data that on internet, thus makes confidential information not to be secure as it can be accessed by anybody at any time. However, to address this issue of securing patient confidential information on Electronic Medical record, biometric system has been previously studied and found as a means of guaranteeing authentication in access control area [1]. Thus, reduce accessing patient Electronic Medical Record by unauthorized people to a minimal number.

Biometric is 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

DOI: 10.2316/J.2014.216.815-0007

[1]. 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 [2]

Biometric exhibit advantage features of if-and-if relationship; this makes the biometric to be ideal for any authentication system. In particular, face biometric utilizes spatial geometry in distinguishing face features during authentication [3]. Also, face feature extraction is relatively easy compared with other biometric features [4]. For this reason, face biometric is chosen as an adequate biometric authentication features for securing the patient information on EMR in hospitals.

However, in spite of these advantages face authentication systems still present a number of limitations, including face with distortions and back ground illumination. It is thus of special relevance to address these limitations for the benefit of patients EMR keeping in hospitals

1.1 Face Biometric

In face recognition, there are some features that are important for system recognition. These features include nose, eyes, eyebrows, mouth and nostril [5]. Each of these features has some values or weights to recognize the face. Figure 1 shows some of the features used in face recognition. The accurate estimation and extraction of human face features are very challenging.

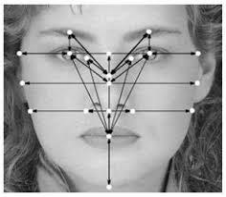

Figure 1: Some of the features used in face recognition

1.2 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 [5, 6]. 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 [5, 6].

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 [6] as illustrated in Figure 2.

Figure 2: Human face with distortion and complex background

With all these in mind, this research aim to focus on designing a face biometric authentication system which addresses the issue of distorted face images to enhance patient convenience and bolster health care institution security.

This paper advances the existing face authentication system by addressing problem of distortion as well as problem of lightning and facial image with glasses to improve the security of patient medical information on EMR. The major contributions of this paper are as follows:

This paper advances the existing face authentication system by addressing problem of distortion as well as problem of lightning and facial image with glasses to improve the security of health care on Electronic Medical Record.

The major contributions of this paper are as follows:

- Development of a new face biometric using optimized PCA-SVM feature extraction system model, which addresses issue of distorted faces for authentication.
- Deployment of optimized PCA-SVM on specific distorted face for ease of implementation.
- Experimental evaluations of face biometric on EMR with application to hospitals.

2 Theoretical Background

2.1 Related Research

There are several fingerprint approaches to access control area using fingerprint biometric system. This section presents them as shown in Table 1.

RELATED WORKS	PROBLEM ADDRESSED	METHODOLOGY	EXPERIMENTAL RESULT	LIMITATIONS
Securing Medical Records on smart phones[7]	• Maintaining privacy of patient medical records and making record available during emergency.	The approach used face, finger, break-the-glass and password stored on smart phone to retrieved patient EMR.	Experimental result confirms that proposed approach enables a person to view her records at any time, and emergency medical personnel can view the record as long as the person is present.	• The drawback of the proposed is explained in [7].
Biometrics Access control for e-health record in pre-hospital care[3]	• Biometric to access a central health record database featured by privacy policies.	The approach used a fingerprint on mobile device.	Experimental result shows as in [3].	• The approach is not flexible it involves enforcing patient to comply with the same policy as in [3]
Protection of patient and privacy using vascular biometric[8].	• Protecting patient privacy and preventing identity theft.	The approach utilized multi-biometric system which consists of hand vein and fingerprint.	Experimental result shows that the approach improved the speed performance and reduced the cost of the system hygiene.	• The drawback of the proposed is explained in [8].
Proposed PCA-optimized SVM	• Protecting patient confidential information on EMR without revealing all patient to all physicians except the only the portion the patient want physician to see. • Addressing issue of face with distortion.	Using PCA and SVM algorithm.	Experimental result shows that our proposed approach addressed the issue of face with distortion during authentication	• In a situation of heavy distortion of the face such as aging process affects the performance of the proposed system during authentication.

Unlike the above-mentioned methods, this study proposes face biometric on EMR using optimized PCA-SVM approach to address face distortion. Insufficient work has been done in literature to address issue of distorted face on EMR.

2.2 Optimized Principal Component Analysis (PCA)

Optimized PCA is one of the most widely used techniques for face authentication. In optimized 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 optimized PCA algorithm for recognition [4].

The optimized PCA 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 (1).

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

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

2.3 Support Vector Machine (SVM)

The 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].

The SVM hyper plane that can separate two classes as in (2).

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

For all i , where w has the same dimensionality as in (3).

$$f(x) = w.\phi(x) + b = \sum_{i=1}^{i} C_i \phi(x_i).\phi(x) + b \tag{3}$$

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 (4).

$$k(x_i, x_j) \equiv .\phi(x_i).\phi(x_j) \tag{4}$$

Thus, gives equation (5).

$$f(x) = \sum_{i=1}^{i} C_i k\left(x_i, x_j\right) + b \tag{5}$$

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.

3 Proposed Face Biometric System Architecture on EMR

The propose face biometric authentication system on EMR system architecture is described in Figure 3. The system architecture is divided into four stages: (i) image acquisition (ii) image pre-Processing stage (iii) feature extraction using optimized PCA-SVM (iv) face database and patient EMR

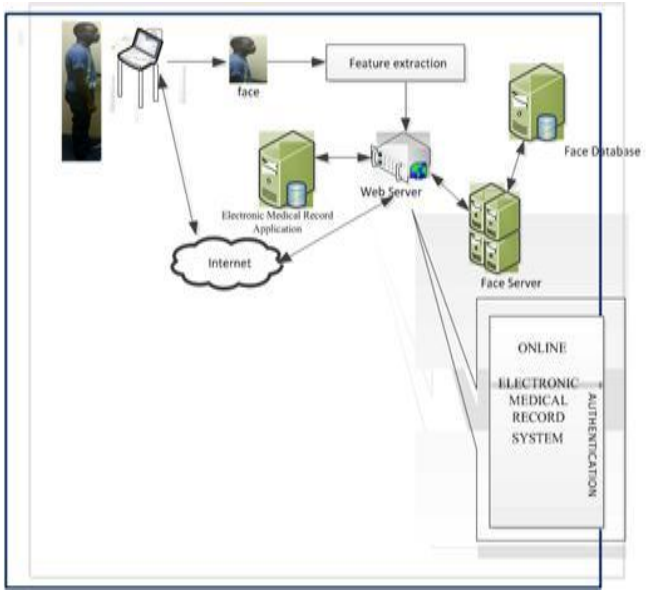

Figure 3: Proposed face biometric on EMR System Architecture

3.1 Image Acquisition Stage

As reflected in Figure 3, the first stage is acquisition of facial image from patient. This is done using a digital camera and is saved in database before passing through image pre-processing stage.

3.1.1 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.

3.2 Feature Extraction using Optimized PCA-SVM

The fingerprint image is passed through the stages of training and testing stage which are in order to extract the facial features.

3.2.1 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 1: Training Stage Face using optimized PCA-SVM

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 1, 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.

3.2.2 Testing Stage using Optimized PCA-SVM

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.

ALGORITHM 2: Test Face Image

INPUT: $T = \varphi_i \times \gamma$, $\mu = \tau^T \times \nu$,

γ = eigenvecto r

E_1 = normalized image ,

Euclidean distance, E_2,

T = proposed eigenfaces

μ = space vector

OUTPUT: Test face image

STEP 1: input trained image

STEP 2: reshape and centred image v=reshaped-mean

STEP 3: centre project test vector into face space $\mu = T^{\tau} * \nu$

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

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

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

From algorithm 2, 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.

3.3 Database and Patient EMR

As shown in figure 3, the trained face image is stored in face database and saved with a patient medical record and with some other relevant information about the patient. The database and patient EMR is then transferred to the web server for patient to access electronically over internet.

4 Scoring and Evaluation Scheme

In this section, the performance of the proposed face biometric is studied through visual inspection as well as quantitatively. During visual inspection, one compares the quality of the pixel value of distorted face with enhanced fingerprint images [10]. The following evaluation models were chosen as quantitative schemes [11] [12]:

(i) False Rejection Rate (FRR) and

(ii) False Acceptance Rate (FAR)

The schemes in [11] are computed by the following formulas in equations (6)-(7).

$$FRR = \frac{G}{N} \quad (6)$$

where G the number of valid users face who are incorrectly denied access and N is total number of genuine tested.

$$FAR = \frac{I}{N} \quad (7)$$

where I the number of imposter's face that are incorrectly granted access 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 (8).

$$SA = \frac{M}{P} \times 100 \quad (8)$$

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.

4.1 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 face with distortions using MATLAB. The face images are captured with a cannon digital camera.

Original faces with distortions are shown in Figure 1 and Figure 2 respectively. Hundred (100) good face images were enrolled into the database. A second set of the same Hundred (100) face images were captured but without consideration of their state, these were then used as query face images. Some samples of the face images captured for querying the database are shown in Figure 4 with various degrees of distortions. One hundred (100) more face images were collected but were not part of the database. These one hundred (100) face images where used as query to the database to measure FAR of our system. All of the second set face images were used as query faces images to measure the FRR of the system.

However, this work focuses on face biometrics on EMR and enhancing distorted face images. In terms of performance measures, the FAR, FRR and accuracy are computed when evaluating the result of the proposed optimized PCA-SVM approach, as shown in Figure 4 and 5 respectively.

Experiment 1: Performance of Optimized PCA-SVM on face image

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

Figure 4: Facial image with distortion and trained using optimized PCA-SVM approach

Experiment 2: Quantitative Performance of Optimized PCA-SVM approach

We specifically access the quantitative performance of our optimized PCA-SVM approach from three experiments conducted with respect to different distortion level.

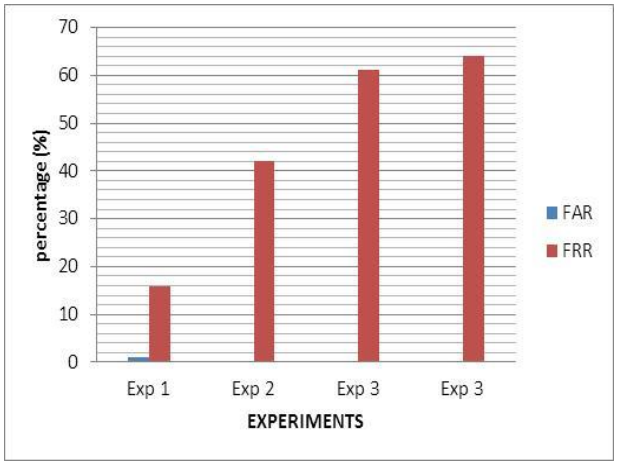

Figure 5: Performance of the proposed optimized PCA-SVM on distorted face

The result in Figure 6 shows the graphical performance of our optimized PCA-SVM approach when a certain percentage of the images of the database are distorted and then used as query images. The graph in Figure 6 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.

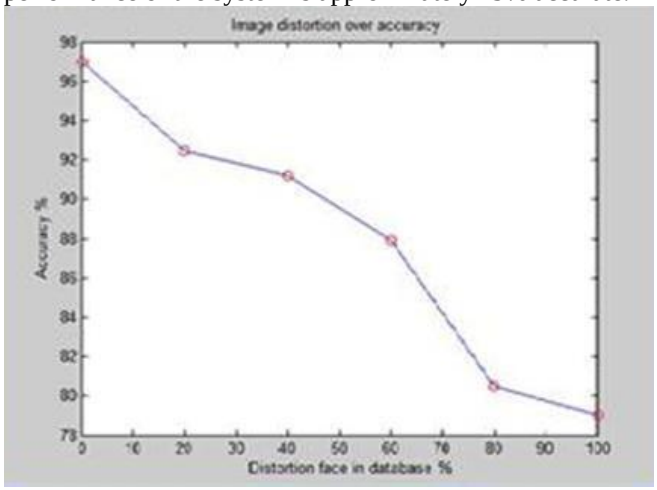

Figure 6: Graph showing the accuracy of distorted faces

4. Conclusion

We have demonstrated the use of face biometric approach on EMR to secure patient confidential information in hospital. We conducted experiments using optimized PCA-SVM approach to address the issue of distortion in the face during authentication.

The experiment conducted on distorted face image shows that optimized PCA-SVM approach gives more accurate in extracting face feature as shown in Figure 4.1. However, the performance accuracy of our approach was also tested on distorted free face to give 98% system accuracy. This performance shows that optimized PCA-SVM exhibits a reliable performance for promising security work on EMR in hospital.

Consequently, the future work can be focused on developing smart systems that can modify the biometric facial template to simulate aging effect in order to ensure that face templates are always consistent with the current facial appearance of the patient.

Acknowledgement

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

References

[1] 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.

[2] O. A. Esan, S. M. Ngwira, T. Zuva, "Bimodal Biometrics for Health Care Infrastructure Security," in *Proceedings of the International MultiConference of Engineers and Computer Scientists 2014*.

[3] J. R. Ciaz-Palacios, R.-A. Victor J, and A. H. Chinaei, "Biometric Acess Control for e-Health Records in Pre-hospitals Care," presented at the EDBT/ICDT, 2013.

[4] Neerja and E. Walia, "Face Recognition Using Fast PCA Algorithm," in *2008 Congress on Image and Signal Processing*, 2008.

[5] Neerja and E. Walia, "Face Recognition Using Improved Fast PCA Algorithm," *Congress on Image and Signal Processing*, 2008.

[6] 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.

[7] R. W. Gardner, S. Garera, and M. W. Pagano, "Securing Medical Records on Smart Phones," presented at the SPIMACS 09, 2009.

[8] C. L. Deepika, A. Kandaswamy, and C. Vimal, "Protection of Patient Identity and Privacy using Vascular Biometrics," *International Journal of Security (IJS)*, vol. 4, pp. 64-84, 2009.

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

[10] 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.

[11] A. S. Awad and H.Man, "Similar neighbour Criterion for Impulse noise Removal in Images," *International Journal of Electronics and Communication,* vol. 64, pp. 904-915, 2010.

[12] 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.