Bi-Modal Biometric Authentication by Face Recognition and Signature Verification

Ibiyemi T.S
Dept. Of Electrical Engineering,
University Of Ilorin, Ilorin, Nigeria.

Ogunsakin J
Dept. Of Electrical Engineering,
University Of Ilorin, Ilorin, Nigeria.

Daramola S.A
Dept. Of Electrical &InformationEngineering,
Covenant University, Ota, Lagos.

ABSTRACT

Face and signature are still two most dominant authentication modes in banking, legal documents, or personnel records in spite availability of more robust biometric modes. Hence, it is imperative to develop low-cost and reliable automated face recognition and signature verification system. Therefore, this paper presents our work in development of a two-in-one portable low-cost dsPIC30F3013 digital signal processing microcontroller based system for real time face recognition and signature verification. The face recognition part of the system is based on eigenface method, while the offline signature verification is based on 12-dimensional feature vector derived from the signature's geometric attributes.

KEYWORDS

Authentication, face recognition, signature verification, offline, eigenface

1. INTRODUCTION

Face and handwritten signature have been the two dominant and acceptable means of personal identification in authentication and authorisation. In spite of their shortcoming in foolproof identification, they still remain the most popular particularly in financial transaction, legal document, and institutions of higher learning. A strong reason for this popularity can be attributed to the fact facial passport and handwritten signature can easily be used for personal identification in absentia of the person. The banking industry still talk about signatory to an account with the signatory's facial photograph attached; in a university system, students are required to sign in and out of examinations; and identity cards for numerous applications often carry signature and facial photograph. Hence, the recent research upsurge in provision of automatic face recognition and signature verification by machine.

This paper presents our work in development of a two-in-one portable low-cost microcontroller based system for real time face recognition and signature verification. People find it relatively easier to recognise faces of their own race but this is immaterial for face recognition by machine. The face recognition part of the system is based on the principle of principal component analysis, PCA, also known as eigenface in a face space for face recognition [1 ,2]. The eigenface method is now widely used in face recognition because of its effectiveness and modest computational requirement [1 ,2, 3,4]. However, face recognition rate using eigenface is easily degraded by variation in illumination conditions, inconsistency in size of acquired face image, and rotation in face. Hence, measures are put in place in this work to handle these sources of degradations.

Signature verification can be in two forms depending on method of acquisition for processing, namely, offline signature; and online signature. Signatures appended on papers, bank cheques, or documents and later scanned for automatic verification are referred to as offline signature verification. This verification process is based on the image of the signature, hence, susceptible to forgery. On the other hand, online signature verification is based on dynamic features of the signature extracted as the signature is being signed. It is a process that is more resilient to forgery than offline signature verification since the process is not directly visible to man but machine. Because the aforementioned applications are based on signatures signed on material for later processing, this paper is concerned with offline signature verification. There are three types of signature forgeries, namely, random forgery, simple forgery, and skilled forgery. Random forgery is a signature presented by an impostor which is neither based on the knowledge of the owner's name nor his/her genuine signature. But in the case of simple forgery, the impostor presents a signature based only on the knowledge of the owner's name. And a skilled forgery, is based on a signature presented after a desirable access to the owner's genuine signature. This work considers the three types of forgeries.

The face recognition method is based on eigneface algorithm while the offline signature verification is based on feature vectors extracted from geometric attributes.

2. EIGENFACE ALGORITHM [1,3,4]

The sequence of algorithms for face recognition using eigenface method is as follows:

(1) Pre-processing

Given K colour face images, each of size M x N:

(a) Convert each RGB colour image to grey scale:

$$\Gamma_{i,j} = \sum_{l=1}^{3} \begin{bmatrix} 0.299 \\ 0.587 \\ 0.114 \end{bmatrix}^{T} .G_{i,j,l} \quad ,i = 1,2,\cdots,M \;; \quad j = 1,2,\cdots,N \qquad (1)$$

where:

$\Gamma_{i,j} \Rightarrow$ *grey scale image*

$G_{i,j,l} \Rightarrow$ *Colour RGB image*

(b) Create training image matrix (M.N x K) with each column representing a vectorised image of length , M.N :

$$F = \left[\Gamma_1, \Gamma_2, \cdots\cdots\cdots, \Gamma_K\right]$$
$$where:$$
$$\Gamma_i = \left[x_0, x_1, \cdots\cdots\cdots, x_{M.N-1}\right]^T$$

(c) Perform illumination normalisation:

$$F' = \left(F_i - \mu_0\right).\frac{\sigma_i}{\sigma_0} + \mu_i \quad , i = 1,2,\cdots,K$$
$$where:$$
$$\mu_i = \frac{1}{M.N}\sum_{j=0}^{M.N-1} x_j \quad , \sigma_i = \sqrt{\left(\frac{1}{M.N}\sum_{j=0}^{M.N-1}(x_j - \mu_i)^2\right)}$$
$$\mu_0 \Rightarrow desired\ mean, typically\ = 100$$
$$\sigma_0 \Rightarrow desired\ s\tan dard\ deviation, typically\ = 100$$

(d) Obtain zero-mean training image matrix:

$$\Phi_i = F_i' - \Psi \qquad , i = 1,2,\cdots,K \tag{4}$$
$$where:$$
$$\Psi = \frac{1}{K}\sum_{i=1}^{K} F_i'$$
$$A = \left[\Phi_1, \Phi_2, \cdots, \Phi_K\right]$$

Feature Extraction

(a) Obtain covariance matrix:

$$C = A.A^T \tag{5}$$
$$where:$$
$$C \Rightarrow M.N\ x\ M.N \quad matrix$$
$$\therefore \quad L = A^T.A$$
$$where:$$
$$L \Rightarrow K\ x\ K\ matrix$$

(b) Calculate eigenvalues and eigenvectors:

Obtaining (M.N) eigenvalues and corresponding (M.N) eigenvectors of length (M.N.) each is computationally intractable even for a modest size image. Hence, better to obtain K eigenvalues and corresponding K eigenvectors of length K each.

Let the eigenvectors of reduced matrix L be $v_i \ , i = 1,2,\cdots,K$

From the eigenvectors of the reduced matrix, the eigenvectors of large matrix C can be obtained:

$$U_i = \sum_{j=1}^{K} v_{i,j}\Phi_j \quad , i = 1,2,\cdots,K \tag{6}$$

These eigenvectors, U_i , are like the face images hence they are called eigenfaces.

Each of the eigenface has varying significance depending on the magnitude of its eigenvalue. Hence, it suffices to select a subset K' of the K eigenfaces corresponding to K' highest valued eigenvalues as characterising the entire training face images.

These reduced subset K' eigenfaces are stored , in addition to the mean face.

(2)

(c) Calculate weight vectors by projecting training face images onto the stored eigenfaces:

The contribution of a stored eigenface to an zero-mean training face image can be calculated as a scalar weight. Therefore, a weight vector of length K' whose elements represent the degree of contribution of the corresponding eigenface to that zero-mean image is obtained by projection:

(3) $$\omega_j = U_j^T.\Phi_j \quad , j = 1,2,\cdots,K' \tag{7}$$
$$\therefore \quad \Omega_i = \left[\omega_1, \omega_2, \cdots\cdots, \omega_{K'}\right] \quad , i = 1,2,\cdots\cdots,K'$$

The calculated $\left(K'\,x\,K'\right)$ weight matrix is stored as reference templates.

Recognition of a query face:

On presentation of a new face image to the system for classification, it is converted to grey scale, and then normalised. Then the zero-mean image is obtained and its weight vector is obtained by projecting it onto the stored eigenfaces.

(a) Calculate weight vector for the new image:

$$\Omega_{new} = U_i.\left(F_{new}' - \Psi\right) \quad , i = 1,2,\cdots,K' \tag{8}$$

(b) Perform classification by matching using Euclidean distance metric:

$$\varepsilon = \arg\min{}_i \left\|\Omega_{new} - \Omega_i\right\|_2 \quad , i = 1,2,\cdots\cdots,K' \tag{9}$$
$$if\ \ \varepsilon < T\ then\ F_{new}\ recognised\ as\ \mathrm{i} - th\ \ training\ \ image\ else\ unknown$$

3. OFFLINE SIGNATURE ALGORITHM [5,6,7,8]

Offline signature algorithm consists of the following sequence:

(1) Pre-processing

Given K training colour signature images, each of size M x N:

(a) Convert each RGB colour signature image to grey scale using eqn(1)

(b) Invert the grey scale of each image such that the signature image has higher grey levels:

$$S_{i,j}' = 255 - S_{i,j} \quad , i = 1,2,\cdots,M \quad ; j = 1,2,\cdots,N \tag{10}$$

(c) Perform signature segmentation:

(i) Obtain row zero-mean of the signature image:

$$S_{i,j}'' = S_{i,j}' - \frac{1}{M}\sum_{l=1}^{M} S_{l,j}' \quad ; i = 1,2,\cdots,M \ ; \ j = 1,2,\cdots,N \tag{11}$$

(ii) Segment signature:

$$S_{i,j}'' = \left\{\begin{matrix} S_{i,j}'' & , if\ \ S_{i,j}'' > 0 \\ 0 & , otherwise \end{matrix}\right\} \tag{12}$$

(d) Smooth Signature Image using 3 x 3 averaging window

$$S'''_{i,j} = \frac{1}{9}\left(\sum_{h=i-1}^{i+1}\sum_{k=j-1}^{j+1} S''(h,k)\right), i = 1,2,\cdots,M; \quad j = 1,2,\cdots,N \qquad (13)$$

(e) Perform Binarisation using global threshold [ ]:

$$S'''_{i,j} = \left\{\begin{matrix} 1 & ,if\ S'''_{i,j} > T \\ 0 & ,otherwise \end{matrix}\right\} \qquad (14)$$

(d) Apply thinning algorithm of [ ]

(2) Feature Extraction

Some geometric features are extracted and used as a feature vector:

(i) Aspect Ratio, η :

Aspect ratio, η , is the ratio of signature width to signature height which is considered fairly consistent.

(a) Compute horizontal projection and vertical projection:

$$x_i = \sum_{j=0}^{N-1} S'''_{i,j} \quad , i = 0,1,\cdots,M-1$$

$$y_j = \sum_{i=0}^{M-1} S'''_{i,j} \quad , j = 0,1,\cdots,N-1 \qquad (15)$$

(b) Determine width from horizontal projection and height from vertical projection:

Signature Width, Δw **:**

for i=1 to M do scan x_i *to find first position where* $x_i \geq 3$ *and let* $i_{low} = i$;

for i=M downto 1 do scan x_i *to find first position where* $x_i \geq 3$ *and let* $i_{high} = j$;

$$\Delta w = i_{high} - i_{low} \qquad (16a)$$

Signature height, Δh **:**

for j=1 to N do scan y_j *to find first position where* $y_j \geq 3$ *and let* $j_{low} = j$;

for j=N downto 1 do scan y_j *to find first position where* $y_j \geq 3$ *and let* $j_{high} = j$;

$$\Delta h = j_{high} - j_{low} \qquad (16b)$$

(c) Obtain aspect ratio:

$$\eta = \frac{\Delta w}{\Delta h} \qquad (17)$$

(ii) Slant Angle, φ :

The angle that the signature images makes with the horizontal line is known as the slant angle. It is the angle at which the ratio of horizontal projection to the width projection as the angle is varied becomes maximum.

(a) Find the slant angle, φ :

$$\varphi = \arg\max_{\varphi}\left(\frac{\sum_{j=0}^{N-1} S'''_{i,j}(\theta)}{\Delta w(\theta)}\right), i = 1,2,\cdots,M \ ; -\theta_1 \leq \theta \leq \theta_2 \qquad (18)$$

where :

$\Delta w(\theta) \Rightarrow$ *width of signature image (see eqn.*16*a) at angle* θ

(b) Rotate every pixel of signature image by φ :

$$\begin{bmatrix} \vec{S}'''_x \\ \vec{S}'''_y \end{bmatrix} = \begin{bmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{bmatrix} . \begin{bmatrix} S'''_x \\ S'''_y \end{bmatrix} \qquad (19)$$

(iii) Normalised Area of signature, A' :

The normalised area is defined as the ratio of the area occupied by actual signature image to the area of its bounding box. This is can be inferred from eqns(15,16,17):

$$A' = \frac{\sum_{i=i_{low}}^{i_{high}}\sum_{j=0}^{M-1} x_j}{\Delta w.\Delta h} \qquad (20)$$

(iv) Centre of Gravity, (X,Y):

The centre of gravity of a signature image can be inferred from eqns (15,16,17) as:

$$X = \frac{\sum_{j=0}^{N-1} y_j.j}{\Delta w.\Delta h} \quad , \quad Y = \frac{\sum_{i=0}^{M-1} x_i.i}{\Delta w.\Delta h} \qquad (21)$$

(v) Slope of line joining centres of gravity of two halves of signature, m :

(a) Divide signature image within bounding box into two (left, right) halves. The left box is defined by $((i_{low}, i_{high}), (j_{low}, l'))$, and right box by $((i_{low}, i_{high}), (l', j_{high}))$ as inferred from eqns(15,16,17).

$$l' = \frac{j_{high} - j_{low}}{2} \qquad (22)$$

(b) Using eqn (21), obtain the centre of gravity (X1,Y1) of the left box; and the centre of gravity (X2,Y2) of the right box.

(c) Calculate slope

$$m = \tan^{-1}\left(\frac{X1 - X2}{Y1 - Y2}\right) \qquad (23)$$

(vi) Number of edge points, γ :

An edge point is a signature pixel having only one neighbour in the 8-neighbour window. A 3 x 3 structuring window with all its element 1's is slided over the the signature box to obtain these edge points.

(vii) Number of cross points, χ :

A cross point is a signature pixel having three neighbours in the 8-neighbour window. A 3 x 3 structuring window with all its element 1's is slided over the signature box to obtain these cross points.

A 12-dimensional feature vector, $F = [\eta, \varphi, A', X, Y, X1, Y1, X2, Y2, m, \gamma, \chi]$ is used to characterised each signature.

(3) Signature Classification

When a questionable signature is presented to the system, it pre-processed and the 12-elements feature vector extracted. Then, the distance measure between this feature vector of this questionable signature and those feature vector templates are taken using eqn (24):

$$\delta = \arg\min_i \left\| F_{questionable} - F_i \right\|_2 \quad , i = 1,2,\cdots\cdots,K \qquad (24)$$

$$if\ \ \delta < T'\ then\ F_{questionable}\ recognised\ as\ signature$$

$$of\ \ i-th\ \ authentic\ else\ impostor$$

Decision Fusion

The decision fusion depends on the percentage of closeness to the threshold of the corresponding biometric mode in question. If the closeness is within 10% and the classification result for the same person in the other mode is okay, then the correct result of that mode is accepted the final decision otherwise the final decision is not recognised/forgery.

4. SYSTEM DESIGN AND IMPLEMENTATION

5. EXPERIMENT AND RESULT

The system was used to capture face images from 100 persons, these images were downloaded to host PC in order to test the developed algorithm for face recognition. Out of these training faces, 40 most significant eigenfaces were stored. The recognition rate was 97% using face recognition mode alone. In case of signature verification, the same 100 persons were used to sign 5 times on A4 paper. Also, 20 of them were used as impostors to give simple, random, and skilled forged signatures. These signatures are then scanned by the in-built signature camera module of the system and downloaded to the PC. The recognition rate was 95%, simple and random forgeries gave FAR of 1%, while skilled forgeries has FAR of 45%. However, when the decision fusion was activated the recognition rate was about 98%. After these tests, 30 most significant eignefaces, and 100 weight vectors were ported to the system flash memory for face, while 100 signature feature vectors were ported to the system flash memory.

Fig.2 shows the block diagram of face recognition and signature hardware system. The hardware core is the Microchip 16bit dsPIC30F3013 digital signal controller with an in-built DSP, microcontroller, 24 KB on-chip flash program memory, 1 KB on-chip non-volatile data EEPROM, and can operate up to 30 MIPS. Two C3188A colour camera modules are interfaced to the dsPIC30F3013 DSC, one camera captures face image while the other camera is either used as an offline signature scanner or as ID card scanner. The C3188A camera module is based on OV7620 image sensor with f6mm, f1.6 lens fitted , and 664 x 492 pixels digital data output. The signature scanner supports 300 dpi. Two set of external banks of memory are serially interfaced to the DSC. One set has 2 MB flash memory, and 2 MB serial SRAM for signature images. The second set has a similar configuration for face images.

The face images captured by the face camera are down sampled into 200 x 160 pixels, while the signature scanner operates at 300 dpi. The eigenface algorithm and the signature algorithm as described in sections 2 and 3 are coded in C language using MikroC Pro for dsPIC and ported to dsPIC30F3013 on EasydsPIC6 development system.

6. CONCLUSION

A portable low-cost embedded system based on dsPIC30F3013 DSC with two digital colour camera has been developed for face recognition and offline signature verification. The recognition results for face recognition and signature verification are satisfactory both on the host PC and on the target embedded system.

7. ACKNOWLEDGEMENT

We acknowledge with great appreciation the generous research and development grant received from Federal Government of Nigeria through the STEP-B project to execute this work.

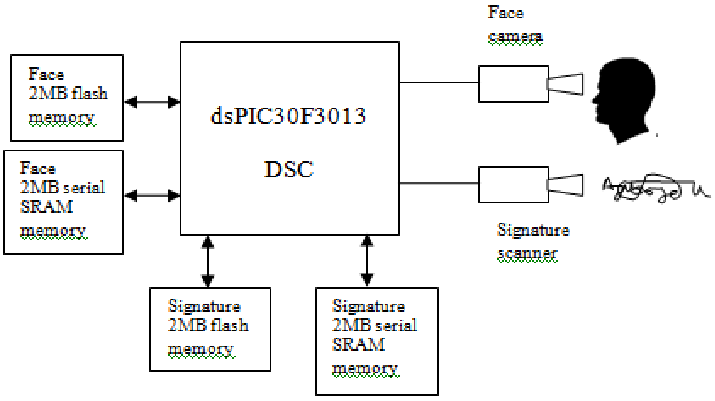
Face camera
Face 2MB flash memory
Face 2MB serial SRAM memory
dsPIC30F3013
DSC
Signature scanner
Signature 2MB flash memory
Signature 2MB serial SRAM memory

Fig.1. The Face Recognition and Offline Signature Verification Hardware Architecture

8. REFERENCES

[1] Ibiyemi T.S., Aliu S.A.(2003), "Automatic Face Recognition by Computer", Abacus: Mathematics Series, vol 30, no. 2B, September, pp180-188

[2] Ibiyemi T.S., Aliu S.A..(2002), "On Computation of Optimum Basis Vector for Face Detection and Recognition", Abacus: Mathematics Series, 29(2), pp 144-149

[3] Turk M., Pentland A., (1991), “Eigenfaces for Recognition”, Journal of Cognitive Neuroscience, vol. 3, no.1, pp71-86

[4] Brian Harding, Cat Jubinski, “A Standalone Face Recognition Access Control System”, ECE4760 Final Project Report, URL: http://people.ece.edu/land/courses/ece4760

[5] Daramola S., Ibiyemi T.S., (2010), “Novel Feature Extraction Techniques for Offline Signature Verification”, International Journal of Engineering Science and Technology, vol.12, no.7, pp3137-3143.

[6] Daramola S., Ibiyemi T.S., (2010), “Person Identification System using Static and Dynamic Signal Fusion”, International Journal of Computer Science & Information Security, vol.6, no.7, pp88-92.

[7] Ashish Dhawan, Aditi R. Ganesan, (2004), “Handwritten Signature Verification”, ECE533 Project Report

[8] Huang K., Yan H., (1997), “Offline Signature Verification based on Geometric Feature Extraction and Neural Network Classification”, Pattern Recognition 30, pp.9-17.