Volume 2, Issue 7, July 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Palmprint Recognition System Using Enhanced Eigenpalms Features

Alaaga James Terna*, Dr. (Mrs) V.E Ejiofor
Nnamdi Azikiwe University,
Awka-Nigeria

Abstract— This research work is based on the field of biometrics with concentration on Palmprint as Secured biometric template for Computer Authentication. We propose a Palmprint Recognition method based on an enhanced EigenPalm Feature using Gaussian Pyramid decomposition. Our method introduces Gaussian Decomposition of images to test the effects of resolution on the Eigenpalm method. As an image pre-processing algorithm, it achieves enhanced feature extraction by filtering and down sampling the images into reduced resolutions. The Software used to implement the system is coded with MATLAB 7.5. Experiment is carried out by matching the decomposed images with their stored templates on each of the three reduced image resolution levels (128 x 128, 64 x 64, 32 x 32 pixels). An analysis of the results illustrates the effectiveness of our method in terms of a higher recognition rate at a resolution of 64 x 64 pixels.

Keywords— Authentication, Palmprint Recognition, Eigenpalm, Gaussian Pyramid, Image Resolution,

I. INTRODUCTION

As our everyday life is getting more and more computerized, automated security systems are getting more and more important. Today most personal banking tasks can be performed over the Internet and soon they can also be performed on mobile devices such as cell phones and PDAs. The key task of an automated security system is to verify that the users are in fact who they claim to be. There are three main methodologies when performing this verification. The security system could ask the user to provide some information known only to the user, it could ask the user to provide something only the user has access to or it could identify some sort of trait that is unique for the user. Of course, some sort of combination of these methodologies is also possible.

The first approach, asking for some personal information such as a password, is the classical approach. It has been used for decades in computer systems, but unfortunately this methodology has a major drawback. The problem is related to how the human memory works and what is demanded of a password for it to be considered secure. For a password to be considered secure, an imposter should not be able to guess the password within a reasonably large number of attempts. This means that it should be randomly chosen and of a certain minimum length. Unfortunately studies have shown that this secure length is longer than seven digits which make passwords hard to remember since humans usually only can hold five to nine digits in their short-term memory at any one time [1].

The second approach, asking for some personal belonging such as a smart card, has also been used for a number of years, for example when accessing high security facilities. This methodology also has a major drawback, since what is identified by the security system is not the user but actually the belonging. For example, if an imposter steal an authorized users access card and tries to enter a restricted area, there is no way for the security system to know that it

is giving access to an imposter and not the user. Of course the method can be combined with a password to get around this problem but then the previously mentioned password problem will be introduced instead.

The third approach, identifying some trait that is unique for the user, is known as biometric security and it is an attempt to get around the previously mentioned problems. A biometrics system is a pattern recognition system that establishes the authenticity of a specific physiological or behavioural characteristic possessed by a user.

The traditional secure measures, passwords or ID cards, provide only limited protection for safety systems. Thus, they cannot meet secure and automated requirements in the modern, automated world with an ever-growing need to authenticate individuals in various fields.

Fingerprints recognition which is the most popular biometric is often faced with problems such as unclear fingerprints due to physical work or problematic skin; and in some worse cases, no finger at all. These problems are addressed with Palm print recognition

At the beginning of palmprint research, the high-resolution approach was the focus because of its application in Forensics and Criminal detection. For commercial and civil applications however, the high-resolution approach is not suitable, hence the need to research on low resolution approaches. This research work uses a low-resolution approach to enhance performance and reliability of access control in civil and commercial applications.

Again, previous works on palmprint recognition focused on two aspects: (1) extracting the principle lines and creases in the spatial domain ([2]; [1]) and (2) transforming the palmprint images into the frequency domain to obtain the energy distribution feature [3]. In

the first approach, the lines and creases of a palm are sometimes difficult to extract directly from a given palmprint image with low resolution. The recognition rates and the computational efficiency are also not sufficient. In the second approach, the abundant textural details of a palm are ignored and the extracted features are greatly affected by the lighting conditions. The problems with these two approaches suggest that new methods are required for palmprint recognition. Zhang et al.'s Eigenpalms method addressed a number of these issues taking lightening condition as image rotation into cognizance. However, further experiments with different image resolutions shows conflicting results.

II. MATERIALS AND METHOD

A. Enhanced Eigenpalms Feature Extraction Method Of Palmprint Recognition Using Gaussian Pyramid Decomposition Of Images:

The image samples are decomposed into various resolutions using Gaussian pyramid decomposition so as to enhance feature extraction.

The system functions by projecting palmprint images onto a feature space that spans the significant variations among known images. The significant features are known as "eigenpalms"[7] because they are the eigenvectors (principal components) of the set of palmprints. [4]

B. *Gaussian pyramid decomposition:*

The image pyramid is a data structure designed to support efficient scaled convolution through reduced image representation. It consists of a sequence of copies of an original image in which both sample density and resolution are decreased in regular steps. These reduced resolution levels of the pyramid are themselves obtained through a highly efficient iterative algorithm. The bottom, or zero level of the pyramid, *G*0, is equal to the original image. This is lowpass- filtered and subsampled by a factor of two to obtain the next pyramid level, *G*1.

*G*1 is then filtered in the same way and subsampled to obtain *G*2. Further repetitions of the filter/subsample steps generate the remaining pyramid levels.

The Gaussian Pyramid block uses Gaussian pyramid decomposition to resize an image. The image reduction process involves lowpass filtering and down-sampling the image pixels. The key to Gaussian Pyramid generation is that size of the initial image (known as 'level 0') must be a square image [(2^M)+1]x[(2^M)+1]. Each subsequent level 'n' of the pyramid has a size of [(2^M-n)+1]x[(2^M-n)+1]. The exception to the rule is that when a pyramid eventually reaches a 3x3 size, the next and final level is of size 1x1. Each level of a Gaussian pyramid is of a lower resolution than the previous. A 'reduce()' function is coded in MATLAB to generate each Gaussian level. [6]

C. *The Algorithm:*

The Gaussian pyramid is computed as follows. The original image is convolved with a Gaussian kernel. The resulting image is a low pass filtered version of the original image.

The low-pass filtering is done using convolution with a Gaussian filter kernel. Where the filter overhangs the image edges we reflect the image about its edge. Since the lowest frequencies have been removed, the full-size image contains redundant pixels. One may define the REDUCE operator which is a filtering followed by elimination of unnessesary pixels. For a filter kernel $w[i,j]$ of dimension 5x5 and reduction factor 4 we have:

$$REDUCE(I)[I,j] = \sum_{m=1}^{5} \sum_{n=1}^{5} w[m,n] I[2i+m, 2j+n] \quad \textbf{(2.1) [6]}$$

There is a corresponding EXPAND operator (not used in this research work) which will reconstruct the low-pass filtered image by interpolating between pixels in the reduced image.

Let I (x, y) be the original image. The Gaussian pyramid on image I is defined as:

$$G_0(x,y) = I \quad \textbf{(2.2) [6]}$$

$$G_{i+1}(x,y) = REDUCE(G_i(x,y)) \quad \textbf{(2.3) [6]}$$

The REDUCE operation is carried out by convolving the image with a Gaussian low pass filter. The filter mask is designed such that the center pixel gets more weight than the neighboring ones and the remaining terms are chosen so that their sum is 1. [6]

III EXPERIMENTAL RESULT

To analyze the relationship between the performance of Zhang et al.'s Eigenpalm method and image resolution, the feature vector of each testing palmprint is matched against each stored template at each level. A genuine matching is defined as the matching between the palmprints from the same palm and an imposter matching is the matching between the palmprints from different palms.

This section describes a set of experiments using the CASIA Palmprint Database [5] for evaluating palmprint recognition performance of the proposed algorithm. This database consists of 600 images (384 × 284 pixels) with 100 subjects and 6 different images of each palmprint. Figure 5.1 shows some examples of palmprint images in the database.

Palmprint images in the database are captured under different lighting condition and have nonlinear distortion due to movement of a hand and fingers. Also, the images used for testing are further classified into three based on the Gaussian decomposition performed on the image samples (pre-processing). This is to illustrate the system performance based on resolution differences. To investigate the relationship between the recognition accuracy and the resolution of palmprint images, the original images are decomposed into a Gaussian pyramid and the images at each level are tested. At each level, four images of each palmprint class are randomly chosen as training samples to form the template and the remaining two images are used as testing samples. All of the experiments are conducted using the Microsoft Windows 7 home edition and Matlab 7.5 with image processing toolbox on a personal computer with an Intel Pentium IV processor (2.3 GHz).

The performance of the biometrics-based verification system is evaluated by the Receiver Operating Characteristic (ROC) curve at each pyramid level, which illustrates the False Reject Rate (FRR) against the False Accept Rate (FAR) at different thresholds on the

matching score. We first evaluate the FRR for all the possible combinations of genuine attempts; the number of attempts is 6*C*2 ×100 = 1, 500. The error ratios of impostor (FAR) and genuine (FRR) attempts are computed in table 5.1 below.

Next, we evaluate the FAR for 100*C*2 = 4, 950 impostor attempts, where we select a single image (the first image) for each palmprint and make all the possible combinations of impostor attempts. The performance is also evaluated by the Equal Error Rate (EER), which is defined as the error rate where the FRR and the FAR are equal.

TABLE 1: FAR and FRR error rates at given thresholds on a resolution of 128 x 128

THRESHOLD	FAR (%)	FRR (%)
1	0.16	0
2	0.12	0
3	0.1	0.07
4	0.08	0.13
5	0.04	0.2
6	0.02	0.2
7	0	0.27
8	0	0.33
9	0	0.4
10	0	0.47

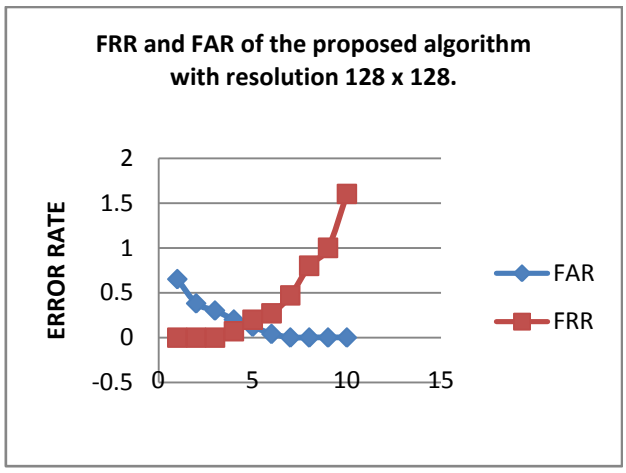

Fig 1. Roc curve (FAR and FRR error rates vs threshold) of resolution 128 x 128.

TABLE 2: FAR and FRR error rates at given thresholds on resolution of 64 x 64.

THRESHOLD	FAR (%)	FRR (%)
1	0.72	0
2	0.35	0
3	0.14	0
4	0.1	0
5	0.08	0.07
6	0.04	0.13
7	0	0.2
8	0	0.33
9	0	0.53
10	0	0.67

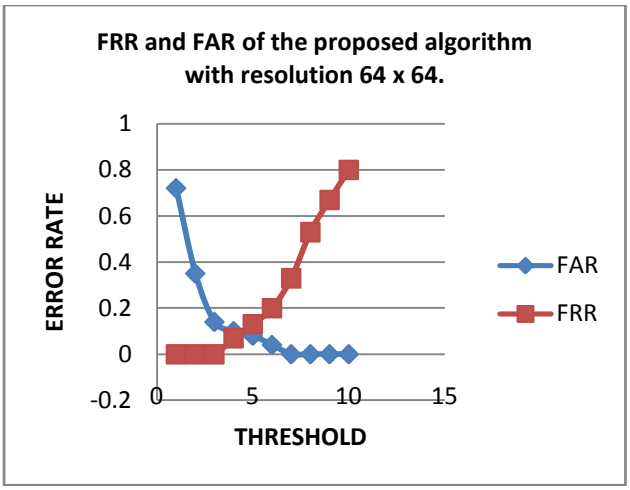

Fig 2: Roc curve (FAR and FRR error rates vs threshold) of resolution 64 x 64.

TABLE 3: FAR and FRR error rates at given thresholds on resolution of 32 x 32.

THRESHOLD	FAR (%)	FRR (%)
1	0.85	0
2	0.45	0
3	0.37	0
4	0.31	0.1
5	0.19	0.28
6	0.05	0.35
7	0	0.52
8	0	0.8
9	0	1.0
10	0	1.6

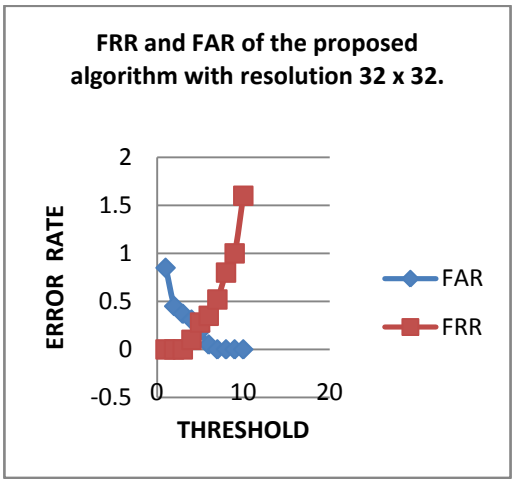

Fig 3: Roc curve (FAR and FRR error rates vs threshold) of resolution 32 x 32

Based on the above matching schemes (resolution of 128 x128, 64 x 64, and 32 x 32), an EER of 0.1 is achieved given rise to a high recognition rate (99.9%) with a resolution of 64 x 64 pixels as against 99.8%(EER=0.2), 99.71% (EER=0.29) with resolution of 128 x 128 and 32 x 32 pixels respectively. It is evident that the image resolution can play an important role in

the matching process. Low resolution images lead to a high recognition rate. However, this principle only holds to a certain point as the experimental results show that the recognition rate remains unchanged, or even becomes worse, when the resolution is further reduced to 32 x 32 pixels.

A further analysis was made by calculating the standard error rates (false acceptance rate (FAR) and the false rejection rate (FRR)) [2]. Obviously, for an effective method both rates must be as low as possible, but they are actually antagonists and lowering these errors is part of an intricate balancing act. For example, if you make a system more difficult to enter for an impostor (reducing FAR), you also make the system more difficult to enter for a valid enrollee (i.e., FRR raised). This process operates in the reverse sense too. For a given system, this becomes a question of probabilities, and a company deploying such a system will generally adjust the matching threshold depending on the level of security needed. For instance, a bank needs a very secure system, so it would adjust the threshold very low to reach an FAR close to zero. However, the banks employees will have to accept false rejections, and they may have to try several times to enter the system.

Compared to the approach in [8], which used a set of feature points along the prominent palm lines and the associated line orientation of palmprint images to identify the individuals, where a matching rate about 95% was achieved, but only 30 palmprint samples from three persons were collected for testing. It seems that the testing set is too small to cover the distribution of all palmprints. An average recognition rate 91% was achieved by the technology proposed in [1], which involved a hierarchical palmprint recognition fashion. In the EigenPalm feature approach used by Zhang [4], a fixed resolution was used to obtain the results. Altering the image sample resolution using our enhanced EigenPalm method, results in a higher performance at a low resolution of 64 x 64 pixels compared to Zhang et al.'s 128 x 128[4] for all matching schemes. The recognition rate of our method is more efficient, as illustrated in Table 4.

Table 4: Comparison of different Palmprint recognition methods

METHOD	FEATURE POINT (Duta et al., 2002)	Hierarchical Identification (You et al., 2002)	Eeigenpalm Proposed (Zhang et al., 2002)	Enhanced EigenPalms (Our Research Work)
Database (Samples)	30	200	3056	600
Features	Feature points	Global texture features and feature points	Eigenpalms	Enhanced Eigenpalms
Recognition Rate (%)	95	91	99.149	99.9
Resolution	128x 128	128 x 128	128 x 128	64 x 64

IV CONCLUSIONS

we have proved with this research work that the importance of biometrics in general and palmprint recognition in particular cannot be over-emphasized. also, our proposed method- enhanced eigenpalms features using gaussian pyramid decomposition proved a more robust algorithm in terms of performance.

also, our system achieved maximum performance rate of 99.9% at a resolution of 64 x 64 pixels hence the conclusion that low resolution images enhances system performance to an extent (to an extent because it must not be too low) as demonstrated in the experiment.

V ACKNOWLEDGMENT

I wish to express my profound appreciation to my amiable Supervisor and Head of Computer Science Department, Dr. Mrs. V.E Ejiofor, whose untiring support, assistance, guidance and encouragement helped towards the successful completion of this research work.

Also, may I commend the astute leadership qualities of the Dean, Faculty of Natural Science, Prof. P.A.C Okoye; and the Dean, School of Postgraduate Studies, Prof. L.O. Anike. Not also forgetting the final touch from the external examiner, Prof. E.O. Nwachukwu. They have been so supportive.

Lastly, may commend the Scholars, whose referenced works have been of immense benefit to my research work. I am indebted to you all.

REFERENCES

[1] You J. Zhang D. Kong W.K, and Wong M. (2003) On-line palmprint identification. IEEE Transactions on Pattern Analysis and Machine Intelligence, 25(9):1041-1050.

[2] David Zhang and Shu W. (1999) Two novel characteristics in palmprint verifcation: Datum point invariance and line feature matching. *Pattern Recognition*, 32(4):691-702.

[3] David Zhang Wenxin Li and Zhuoqun Xu. (2002) Palmprint identification by Fourier transform. *International Journal of Pattern Recognition and Artificial Intelligence*, 16(4):417-432.

[4] David Zhang. Lu, G. Wang K. (2002): Palmprint Recognition Using Eigenpalm Features, Pattern Recognition Lett. Pg1463-1467.

[5] CASIA Palmprint Database is available at: http://www.cbsr.ia.ac.cn/PalmDatabase.htm

[6] Kuanquan Wang Xiangqian Wu and David Zhang. (2006) Palmprint texture analysis using derivative of gaussian Filters. In *The IEEE Proceedings of International Conference on Computational Intelligence and Security (ICCIS2006)* volume 1, pages 751-754.

[7] Matthew Turk and Alex Pentlad, (1991) "Eigenfaces for Recognition": Journal of Cognitive Neuroscience pp.71-86.

Duta. N, Jan. A.K Mandia. K.V, (2002) Matching of Palmprint, Pattern Recognition Lett. Pg 477-485

