Global Journals LaTeX JournalKaleidoscope™
Artificial Intelligence formulated this projection for compatibility purposes from the original article published at Global Journals. However, this technology is currently in beta. *Therefore, kindly ignore odd layouts, missed formulae, text, tables, or figures.*

Implementation of FPR for Safe and Secured Internet Banking

S.M.Riyazoddin[1]

[1] CMR Institute of Technology

Received: 14 December 2012 Accepted: 5 January 2013 Published: 15 January 2013

Abstract

In this paper, we present an enhanced approach for fingerprint segmentation based on Canny edge detection technique and Principal Component Analysis (PCA). The performance of the algorithm has been evaluated interms of decision error trade-off curve so fan over all verification system. Experimental results demonstrate the robustness of the system.

Index terms— FPR, canny edge detection, PCA, NN, etc.

1 Introduction

uman beings use physical characteristics such as finger, voice, gait, etc. to recognize each other from their birth itself. With new advances in technology, biometrics has become an emerging technology for recognizing individuals using their biological traits. This technology makes use of the fact that each person has specific unique physical traits that are one's characteristics which can't be lost, borrowed or stolen.

By using biometrics it is possible to confirm or establish identity based on "who the individual is", rather than by "what the individual possesses" (e.g., an ID card) or "what the individual remembers" (e.g., a password). Passwords determine identity through user knowledge, if someone knows the password, then that person can get access to some restricted areas or resources of a certain system. The drawback is that a password has nothing to do with the actual person using it. Passwords can be stolen, and users can give their passwords to others, resulting in systems that are vulnerable to unauthorized people. There is no foolproof way to make password-protected systems safe from unauthorized users. There is no way for password-based systems to determine user identity beyond doubt.

The initial intent of such schemes is, however, to ensure that the provided services are accessed only by an authorized user, and not anyone else. Several systems require authenticating a person before giving access to their resources.

Biometrics has been long known to recognize persons based on their physical and behavioral characteristics. Examples of different biometric systems include fingerprint recognition, finger recognition, iris recognition, retina recognition, hand geometry, voice recognition, signature recognition, etc. Finger recognition in particular, has received a considerable attention in recent years both from the industry and the research communities. The real-life challenge here is the identification of individuals in everyday settings, such as offices or living-rooms. The dynamic, noisy data involved in this type of task is very different to that used in typical computer vision research, where specific constraints are used to limit variations. Historically, such limitations have been essential in order to limit the computational burden required to process, store and analyze visual data. However, enormous improvements in computers in terms of speed of processing and size of storage media, accompanied by progress in statistical techniques, is making it possible to realize such complex systems. a) Applications 1. Commercial applications such as computer network login, electronic data security, ecommerce, Internet access, ATM, credit card, physical access control, cellular phone, PDA, medical records management, distance learning, etc., 2. Government applications such as national ID card, correctional facilities, driver's license, social security, welfare-disbursement, border control, passport control, etc., and 3. Forensic applications such as corpse identification, criminal investigation, terrorist identification, parenthood determination, missing children, etc.

Finger recognition has received considerable interest as a widely accepted biometric, because of the ease in collecting finger images of persons. Finger recognition is being used in various applications like crowd surveillance, criminal identification, and criminal record, access to entry etc. Finger recognition developers, however, have to

consider a number of major issues before finger recognition systems become standard systems. The requirements for a useful, commercial finger recognition and identity logging system, for small groups of known individuals in busy unconstrained environments, (such as domestic living rooms or offices) can be split into several groups: Proposed a method to select pixels used for camera identification according to the texture complexity to improve the accuracy of camera identification. In this method camera identification accuracy is reduced by the image processing engine such as motion blur correction, contrast enhancement, and noise reduction.

Also suggested a method for improving the identification accuracy by the image restoration method.

In this paper, we have shown the improved camera identification method. The identification accuracy is improved by selecting pixels used for correlation calculation according to the texture complexity. And the identification accuracy is also improved by the image restoration which restores the PNU noise varied by the image processing engine. But still there is big concern to have a systematic method to correctly estimate the restoration function. is left to the future work. Developed a fast algorithm for finding if a given fingerprint already resides in the database and for determining whether a given image was taken by a camera whose fingerprint is in the database. Here they realized that in worst-case complexity is still proportional to the database size but does not depend on the sensor resolution. The algorithm works by extracting a digest of the query fingerprint formed by the most extreme 10,000 fingerprint values and then approximately matches their positions with the positions of pixels in the digests of all database fingerprints. The algorithm requires a sparse data structure that needs to be updated with every new fingerprint included in the database. The algorithm is designed to make sure that the probability of a match and false alarm for the fast search is identical to the corresponding error probabilities of the direct bruteforce search. After that they also claim that the fast algorithm does not rely on any structure or special properties of the fingerprints in the database. Hence it can be utilized in any application where a database contains n-dimensional elements and n is a fixed large number. The only requirement is that the elements consist of real numbers or integers from a large range.

But integers from a small range would lead to ill-defined ranks. An extreme case when the rank correlation and consequently, the fast search algorithm cannot be used, are binary vectors.

2 d) Sara et.al. (2010)

3 Suggested

a reliable authentication mechanism which is not dependent on a series of characters, but rather on a technology that is unique and only possessed by the individual called FingerID. This technique is aims to promote the convenience for the internet user since he/she will not have to remember multiple passwords for a multiple number of accounts.

The accessibility, usability and security guidelines have been tested on the Fingered website and browser by means of numerous activities and found that the web accounts a more secure, accessible and usable one. But this increases the cost of the system. Proposed a method to represent sensor fingerprints in binary-quantized form as the large size and random nature of sensor fingerprints makes them inconvenient to store. In their work they analyzed the change in the performance caused due to loss of information due to binarization. Hence, binarization of sensor fingerprints is an effective method that offers considerable storage gain and complexity reduction without a significant reduction in fingerprint matching accuracy. But this will not be effective for noisy or information lost fingerprints leading to the misclassification. Proposed a new technique to fingerprint recognition based a window that contain core point this window will be input ANN system to be model. This method is aadaptive singular point detection method that increases the accuracy of the algorithm. This robust method for locating the core point of a fingerprint. The global threshold reduces chances of falsely locating a core point due to presence of discontinuities like scars or wrinkles, which may occur in the existing processes.

Since the detection is based on a global threshold, the method only gives us an approximate location of the core point. For exact detection of the core point, we use the geometry of region technique over a smaller search window using ANN. They show that as image size window that contain core point in center decreases the system performance also III.

4 Fingerprint Classification Algorithm

In this section, we introduce a basic version of the algorithm for fingerprint classifying (FPC), which has aspreliminary input a database of fingerprint images (Train Database). A test fingerprint image (Test Database) is then entered, and the algorithm returns whether or not the test image is in the stored finger print bank. The steps followed in this process of classification are. Let we have a data set S= {s1, s2, s3, Sn} then mean denoted by SM will be.? = n S SM i / n i ,..... 3 , 2 , 1 = (2.1)

Standard deviation SD will be as ( )1 / 2 ? ? = n SM S SD i n i ,..... 3 , 2 , 1 = (2.2)

Variance is very similar to the standard deviation and the formula for the data set S can be calculated as ( ) ( ) dimensional data where as the Covariance is similar measures between 2 dimensional data. Let consider S and L two data sets then the covariance will be as.? ? ? = 1 2 n SM i S S Var / n i ,..... 3 , 2 , 1 = (2.( ) ( )( ) 1 / ? ? ? = ? n LM L SM S S Cov i n i . 3 , 2 , 1 = (2.4)

If covariance is calculated for one dimensional data then it will be equal to the variance **??**27].

Principal Component Analysis is defined as a dimensionality reduction technique which transforms a random vector say x, say of size n, to a random vector of y, say of size k where k is chosen smaller than n. This transformation is defined below:

Principal Component Analysis is defined by a transformation obtained as follows:) (mx x W y T ? = (2.6)

The transformation given by equation 2.6 has several important properties. The first property we examine here is the covariance matrix of the random vector y. This is defined as]))([(T y my y my y E C ? ? = (2.7)

Wheremy is equal to zero vector 0, since: The second important property deals with reconstruction of random vector x from random vector y. Since we consider x whose observations are real, the covariance matrix X C is real.It follows that the set of eigenvectors of X C form an orthonormal basi] [y E my =)] ([mx x W E T ? = m W x E W T T ? =] [0 = (2.8)

5 By substituting 2.6 and 2.8 into 2.7 gives the following expression for

Y C in terms of X C T T T T T y mx W x W mx W x W E C))((? ? = W mx x mx x W E T T]))(([? ? = W mx x mx x E W T T]))([(? ? = W C W X T = (2.T W W = ?1

Using this property, x can be reconstructed from y by using the relation:x y m W x + = (2.10)

Suppose, however, that instead of using all eigenvectors of X C ,we construct W from the first k eigenvectors corresponding to the largest eigenvalues.

The y vector will then be k dimensional and the reconstruction giving by equation follows:mx y W X k + = ? (2.11)

X ?Represents an approximation of x obtained from the transformation matrix W composed of first k eigenvectors of X C .

6 c) Euclidean Distance for FPC

The mean square error between x and is given by the expression [30]:? ? = = ? = k j i n j j ms e 1 1 ? ? ? + = = n k j j 1 ? (2.12)

The first line of equation 12 indicated that the error is zero, if k = n. additionally since the ¸j's decrease monotonically, equation 12 also shows that the error can be minimized by selecting the k eigenvectors associated with the largest eigenvalues. Thus PCA is optimal in the sense that it minimizes the mean square error between the vector x and its approximation Implementation of FPR for Safe and Secured Internet Banking X.

7 ?

Thus Recognition of images using PCA takes three basic steps. The transformation matrix is first created using the training images. Next, the training images are projected onto the matrix columns. Finally, the test images are identified by projecting these into the subspace and comparing them to the trained images in the subspace domain. But finding the finger discriminating features like minutia, valleys or ridges is very difficult task using PCA whose basic task is dimension reduction and also used as a classifier. To mitigate this problem a new method is proposed where the finger features are located first with help of canny edge detection technique and then classification is done using PCA.

IV. Depending on the noise level, no clear separation can be found, thereby restricting the use of the Euclidean distance. In this section we show that the use of type canny edge or Sobel edge detection [10] can help mitigating the influence of noise. The edge detection is applied at the moment that the image is inserted into the base and when the test image is acquired. With the inclusion of edge detection component the complete sequence of the algorithm is:

8 Proposed Method

Step 1: Store previously the fingerprint database

Step 2: Apply Edge Detections: Stepv3: Build the image space by using the PCA Step4: Define the criteria for classification using neural networks.

Step5: Acquire, apply edge detection and project thefingerprint testing image into image space Step6: Decide whether Test Imagebelongs or not to the stored base. We apply "Canny" edge detection component of the a) Canny edge detection algorithm i. Detection

The probability of detecting real edge points should be maximized while theProbability of falsely detecting non-edge points should be minimized. This corresponds toMaximizing the signal-to-noise ratio.

9 ii. Localization

The detected edges should be as close as possible to the real edges.

10 iii. Number of responses

One real edge should not result in more than one detected edge Canny's Edge Detector is optimal for a certain class of edges (known as step edges).

Step I: Noise reduction by smoothing Noise contained in image is smoothed by convolving the input image I (i, j) with Gaussian filterG. Mathematically, the smooth resultant image is given by) , (*) , (j i I G j i F =

Prewitt operators are simpler to operator ascompared to sobeloperator but more sensitive tonoise in comparison with sobel operator. Non maximum suppression is carried out to reserves all local maxima in the gradient image, anddeleting everything else this results in thin edges. For a pixel M (i, j):

1. Firstly round the gradient direction ? nearest45°, then compare the gradient magnitude of the Pixels Implementation of FPR for Safe and Secured Internet Banking

The purpose of edge detection in general is to significantly reduce the amount of data in an image, while preserving the structural properties to be used for further image processing. The aim of John F. **??**anny [ref1, **??**ef2] was to develop an algorithm that is optimal with regards to the following criteria:

-ba in positive and negative gradient directions i.e.If gradient direction is east thencompare with gradient of the pixels in east and west directions say E (i, j) and W (i,j)respectively. 2. If the edge strength of pixel M (i, j) is largest than that of E (i, j) and W (i, j), then preservethe value of gradient and mark M (i, j) as edge pixel, if not then suppress or remove.

Step IV: Hysteresis thresholding:

The output of non-maxima suppression still contains the local maxima created by noise. Insteadchoosing a single threshold, for avoiding the problem of streaking two thresholds high t and low t are used. For a pixel M (i, j) having gradient magnitude G following conditions exists to detect pixel as Edge: Image complexity, the bias is not considered in the following analysis. We can see from (2.17) and (2.18) that the outputs of an RBF neural classifier are characterized by a linear discriminant function. They generate linear decision boundaries (hyperplanes) in the output space. Consequently, the performance of an RBF neural classifier strongly depends on the separability of classes in the k-dimensional space generated by the nonlinear transformation carried out by the u RBF units. ? If G < than discard the edge. ? If G > than keep the edge. ? If low t < G <

11 Method

12 Conclusion

We have presented an enhanced Canny edge detection based fingerprint segmentation method and PCA is used for accurate classification and authentication of the individual for safe and secured internet banking. The performances of the proposed and existing algorithms have been evaluated interms of True classifications using a database with medium-high quality fingerprint images .Experimental results show that the proposed enhanced algorithm robust than the existing system.

Figure 1:

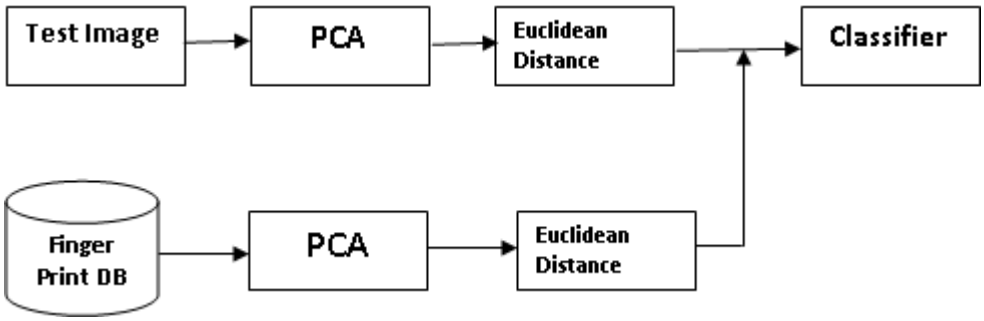

Figure 2: F

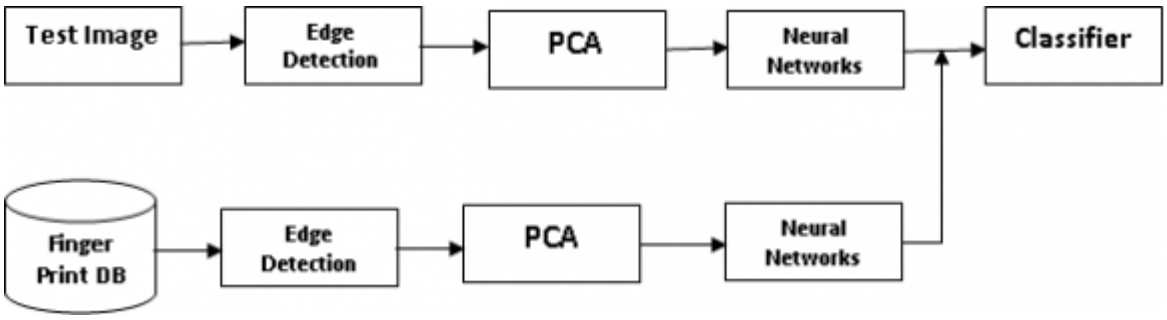

Figure 3:

Figure 4:

3

Figure 5: 3)F

[Lindsay and Smith (2002)] , I Lindsay , Smith . *A tutorial on Principal Components Analysis* February 26, 2002.

[Morizet et al.] *A Comparative Implementation of PCA Face Recognition Algorithm*, Nicolas Morizet , Frédéricamiel , Thomas Insafdrishamed , Ea . ICECS&#39. p. 7.

[Canny (1986)] 'A computational approach to edge detection. Pattern Analysis and Machine Intelligence'. John Canny . *IEEE Transactions* Nov. 1986. (8) p. .

[Ernande et al. ()] *A Fingerprintbased Access Control using Principal Component Analysis and Edge Detection*, F Ernande , H M Melo , De Oliveira . 2011. 30.

[Singh and Malhotra ()] 'Adoption of Internet banking: An empirical investigation of Indian banking Sector'. B Singh , P Malhotra . *Journal of Internet Banking and Commerce* 2004. 9 (2) .

[Dr et al. ()] 'Advanced Networking and Applications Volume. 02, Issue. 06, pg'. . E Dr , K Chandra , Kanagalakshmi . *Int. J* 2011. p. . (Noise Elimination in Fingerprint Image Using Median Filter)

[Yoon et al. (2012)] 'Altered Fingerprints: Analysis and Detection'. Soweon Yoon , Anil K Jianjiangfeng , Jain . *IEEE Transactions on Pattern Analysis and Machine Intelligence* March 2012. 34 (3) p. .

[Matsushita and Kitazawa (2010)] 'An Improved Camera Identification Method based on the Texture Complexity and the Image Restoration'. Kazuya Matsushita , Hitoshi Kitazawa . *International Journal of Hybrid Information Technology* January, 2010. 3 (1) .

[Canny Edge Detection, 09gr820 (2009)] *Canny Edge Detection, 09gr820*, March 23, 2009.

[Computer Engineering and Intelligent Systems www.iiste.org ()] ISSN 2222-2863. *Computer Engineering and Intelligent Systems www.iiste.org*, 2012. Online. 3.

[Sachin et al.] *Digital Design of Fingerprint Recognition Based on Eigen Vector Transform*, J Sachin , Katharki , H R Shashidhara , A R Aswath .

[Bay Ram and By (2012)] 'Efficient Sensor Fingerprint Matching through Fingerprint Binarization'. Sevinç Bay Ram , Hüsrevtahasencar , Nasirmemon By . *IEEE Transactions on Information Forensics and Security*, August 2012. 7.

[Yager and Amin ()] 'Fingerprint Classification: a Review'. N Yager , A Amin . *Pattern AnalApplic* 2004. 7 p. .

[Neeta Murmuand ()] *Fingerprint Recognition*, Abhaotti Neeta Murmuand . 2010. Department of Electrical Engineering National Institute of Technology Rourkela

[ChiragDadlani, Arun Kumar Passi, Herman Sahota, MitinKrishan Kumar (ed.) ()] *Fingerprint Recognition Using Minutiae-Based Features by*, ChiragDadlani, Arun Kumar Passi, Herman Sahota, MitinKrishan Kumar (ed.) 2006.

[Chong et al. ()] 'Geometric Framework for Fingerprint Image Classification'. M M S Chong , T H Ngee , L Jun , R K L Gay . *Pattern Recognition* 1997. 30 (9) p. .

[Goljan et al. ()] 'Managing a large database of camera fingerprints'. M Goljan , J J Fridrich , T Filler . *Proc. SPIE-IS&T Conf. Electronic Imaging: Media Forensics and Security XII*, (SPIE-IS&T Conf. Electronic Imaging: Media Forensics and Security XII) 2010. 7541 p. 754108.

[Kumar et al. (2010)] 'SabyasachiPattanaik by "Fingerprint Verification based on Fusion of Minutiae and Ridges using Strength Factors'. Shashi Kumar , DR , R K Chhotaray , K B Raja . *International Journal of Computer Applications* July 2010. 4 (1) p. .

[Terjekristensen] 'Two Different Regimes of Fingerprint Identification -a Comparison'. Terjekristensen . 10.5923/j.ajcam.20120202.01. *American Journal of Computational and Applied Mathematics* 2012 (2) p. .

[Jezaalotaibi and Wald (2010)] 'Using Fingerprint Recognition in a New Security Model for Accessing Distributed Systems'. Sara Jezaalotaibi , Mike Wald . *International Journal of Intelligent Computing Research* December 2010. 1 (4) . (David Argles by)