Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 5, Issue. 2, February 2016, pg.235 – 240

AN INNOVATIVE DETECTION SYSTEM FOR FINGERPRINT

Ms. R.Pavithra, Mr. V.Muneeswaran

Department of Computer Science and Engineering

Sri Krishna College of Engineering and Technology, Coimbatore, Tamil Nadu, India

pavithrasvgv@gmail.com, muneeswaran@skcet.ac.in

Abstract- Biometrics is used for security purpose. It place a major role in protecting authorized system by using the authentication of fingerprint. The biometrics is a popular research area, since there are many ways the intruders can break into a system. So it becomes mandatory to find new ideas to avoid such situation. The objective of this paper is to enhance the security of biometric recognition frameworks, by adding liveliness assessment in a fast, user-friendly, and non-intrusive manner, through the use if image quality assessment. The proposed approach presents a very low degree of complexity, which makes it suitable for real-time application, using 25 general image quality features extracted from one image to distinguish between legitimate and impostor samples. The target of the projected system is to emphasize the security of biometric recognition frameworks, by adding physical property estimate in an exceedingly quick, easy, and non-intrusive manner, through the employment of image quality assessment. The experimental results, obtained on public available data sets of fingerprint show that the proposed method is highly competitive compared with other state-of-the-art approaches.

Index Terms: Image Quality Assessment, Biometrics, Security, Attacks.

I. INTRODUCTION

In recent years, the developing interest in the evaluation of biometric systems security has led to the creation of various and very diverse initiatives focused on this major field of research [1], the aforementioned works and other analogy studies, have obviously shown the necessity to propose and develop specific protection methods against this threat. Analysis have establish on the design of peculiar countermeasures that enable biometric systems to detect fake fragment and reject them, improving this way the robustness and security level of the systems. Liveness detection methods are usually splitted into one of two groups (i) Hardware-based techniques, which add some definite device to the sensor in order to detect appropriate equality of a living trait (e.g., fingerprint sweat, blood pressure, or specific reflection equity of the eye); (ii) Software- based technique, in this case the fake trait is

© 2016, IJCSMC All Rights Reserved

detected once the sample has been collected with a normal Sensor (i.e., features used to distinguish between real and fake traits are extracted from the Biometric sample, and not from the trait itself).software-based techniques may be impacted in the feature extractor module which makes them potentially capable of recognize other types of illegal break-in attempts not automatically classified as spoofing attacks.

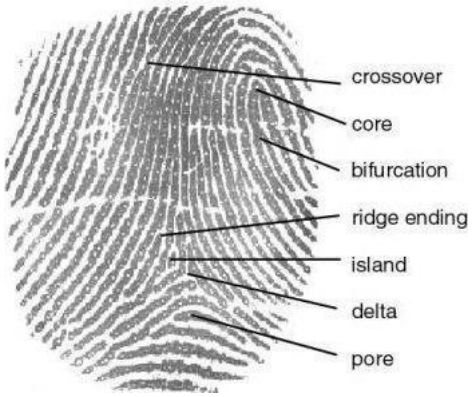

Fig.1. Fingerprint Ridge and Bifurcation

A great amount of work has been done in the field of spoofing recognize and many advances have been reached, the attacking methodologies have also evolved and become more and more sophisticated. As show in fig 1: As issue, there are still big challenges to be faced in the detection of direct intrusion. One of the usual shortcomings of most anti-spoofing meth- odds is their lack of generality. It is not rare to find that the proposed access present a very high performance detecting certain type of spoofs (i.e., gummy fingers made out of silicone), but their ability drastically drops when they are presented with a different type of fabricated training (i.e., gummy fingers made out of gelatine). This way, their error rates vary greatly when the verification terms are altered or if the evaluation database is exchanged. Moreover, the vast majority of current protection methods are based on the analysis of certain specific properties of a given trait (e.g., the frequency of ridges and valleys in fingerprints) which gives them a very reduced interoperability, as they may not be implemented in detection systems based on other biometric methods, or even on the same system with a different sensor. In the present work we propose a novel software-based biometric protection method which targets to overcome part of these drawback through the use of image quality assessment (IQA). This project focuses on how image processing techniques applied to detect the Fingerprint in the image data set. The study of related works are presented in 1.Introduction, 2.Related Works, 3.Implementation, and finally 4 describes about Conclusion and Future Work.

II. RELATED WORKS

Adebayo Daramola, Tola Sokunbi and A.U Adoghe [3], Proposed Support Vector Machine (SVM) may be a feature classification technique. Its ability to separate feature area into 2 major categories, via best hyper plane such the expected generalization error is reduced. Associate degree best hyper plane is drawn by the biggest margin of separation between the 2 categories. The training feature vectors have to lie exterior the margin, small sub-set of the feature vectors that lie specifically on the margin area unit the support vectors. Application of SVM in fingerprint image categorization downside consists of 2 phases: training and testing. Throughout coaching, the SVM takes as input fingerprint image knowledge that accommodates positive and negative samples and also the downside of separating a collection vectors happiness to 2 separate categories is solved by training algorithmic program. The algorithmic program searches for associate degree best hyper plane such the gap to the support vectors is maximized. Authentication of query fingerprint image is set by classify every of user question fingerprint feature as belong to any of the 2 categories. The choice is predicated on the gap of the query knowledge from the hyper-plane.

Hoi Le et al. [4], proposed on-line fingerprint identification with a fast and distortion tolerant hashing technique. National ID card, electronic commerce, and access to pc networks square measure some situations

© 2016, IJCSMC All Rights Reserved

wherever reliable identification may be a should. Existing authentication systems wishing on knowledge-based approaches like passwords or token-based like magnetic cards and passports contain serious security risks attributable to the vulnerability to engineering social attacks and also the easiness of sharing or compromising passwords and PINs. Statistics like fingerprint, face, eye retina, and voice provide a lot of reliable means that for authentication. However, attributable to giant biometric information and complex biometric measures, it's troublesome to style high and quick biometric recognition. Significantly, quick fingerprint categorization is one amongst the foremost difficult issues featured in fingerprint authentication system. In this paper, they present a particular contribution by introducing a new robust indexing scheme that is able not only to fasten the fingerprint detection process but also improve the accuracy of the system.

Wei Cui et al. [5], proposed the analysis of edge detection rule for fingerprint pictures. This paper introduces some edge detection operators and compares their component and performances. At last the experiment show that every formula has its advantages and disadvantages, and therefore the appropriate formula have to be selected according the characteristic of the pictures detected, in order that it will perform accurately. The Canny Operator is not susceptible to the noise interference; it can detect the real weak edge. The advantage is that it uses two different thresholds to detect the strong edge and the weak edge, and the weak edge will be combined in the output image only when the weak edge is connected to the strong edge. The Sobel Operator has a good performance on the images with grey gradient and high noise, but the location of edges is not very accurate, the edges of the image have more than one pixel. The Binary Image Edge Detection Algorithm is simple, but it can detect the edge of the image accurately, and the processed images are not need to be thinned, it particularly adapts to process various binary images with no noise. So each algorithm has its advantages and disadvantages, and the applicable algorithm should be selected according to the characters of the images been detected, then it can performance perfectly.

Asker M. Bazen et al. [6], proposed a correlation-based fingerprint authentication system. In this paper, a correlation-based fingerprint authentication system is presented. Dissimilar the historic minutiae-based systems, this system directly uses the richer grey-scale data of the fingerprints. The correlation-based fingerprint verification system first selects appropriate impression in the primitive fingerprint, uses template matching to locate them in the secondary print, and compares the template location of both fingerprints. Dissimilar minutiae-based systems, the correlation-based fingerprint verification system is capable of handling with bad-quality images from which no minutiae can be extracted reliably and with fingerprints that suffer from non-uniform shape misuse. Experiments have shown that the performance of this system at the moment is comparable to the execution of many other fingerprint authentication systems.

III. FINGERPRINT MATCHING

Among all the biometric techniques, fingerprint-based description is the oldest method which has been successfully used in numerous function. Everybody is known to have unique, immutable fingerprints. A fingerprint is made of a series of ridges and furrows on the exterior of the finger. The uniqueness of a fingerprint can be determined by the pattern of ridges and furrows including the minutiae points. Minutiae points are local ridge characteristics that occur at either a ridge bifurcation or a ridge ending. Fingerprint matching technique can be placed into two categories: minute- based and correlation based. Minutiae-based technique first find minutiae points and then map their relative placement on the finger. However, there are some trouble when using this approach. It is difficult to extract the minutiae points exactly when the Fingerprint is of low quality. Also this design does not take into account the global pattern of ridges and furrows. The correlation-based method is capable to overcome some of the difficulties of the minutiae-based approach. However, it has some of its own start up monies. Correlation-based technique require the precise location of a registration point and are affected by image translation and rotation. Fingerprint matching based on minutiae has problems in matching different sized minutiae patterns. Local ridge design cannot be absolutely characterized by minutiae. We are trying an alternate representation of fingerprints which will taking more local instruction and yield a fixed length code for the fingerprint. The matching will then hopefully become an almost simple task of scheming the Euclidean distance will between the two codes.

© 2016, IJCSMC All Rights Reserved

Algorithms which are more prosperous to noise in fingerprint images and deliver increased accuracy in real-time. As show in fig 2:

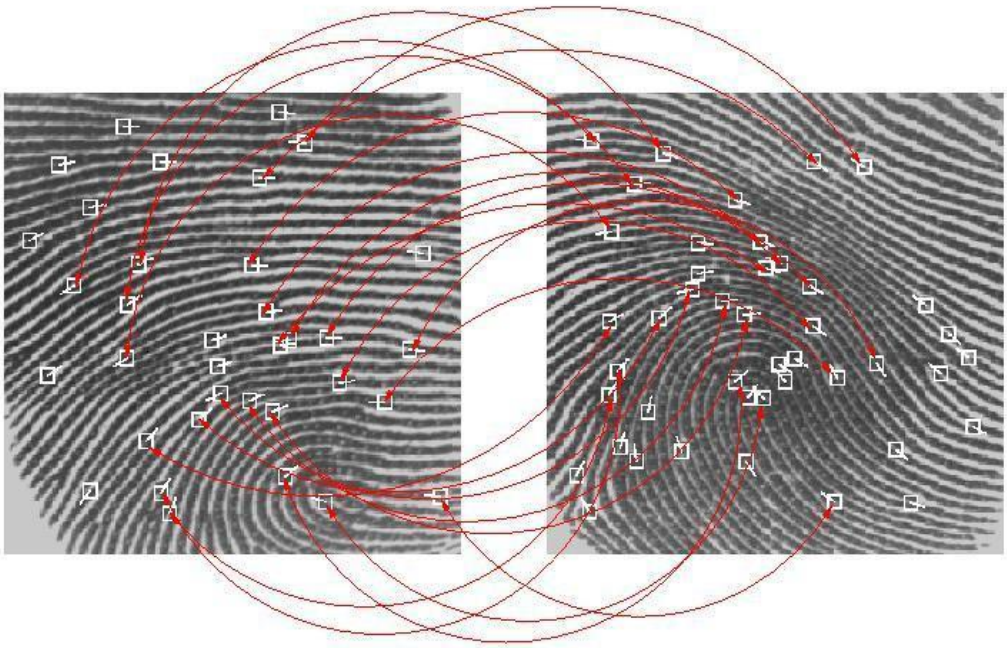

Fig.2.FingerPrint Matching

A commercial fingerprint-based certification system requires a very low False Reject Rate (FRR) for a given False Accept Rate (FAR). This is very difficult to obtain with any one technique. We are inspecting methods to pool evidence from various matching techniques to development the overall accuracy of the system. In a real application, the sensor, the acquisition system and the variation in achievement of the system over time is very critical. We are also field testing our system on a limited number of users to classify the system performance over a period of time.

IV. MINUTIAE EXTRACTION TECHNIQUE

A fingerprint authentication system using minutiae extraction technique. Most fingerprint recognition techniques are based on minutiae comparable and have been well studied [2]. However, this technology still suffers from problems associated with the handling of poor character impressions. One problem besetting fingerprint matching is distortion. Distortion changes both geometrical position and adaptation, and leads to difficulties in establishing a match among multiple impressions captured from the same fingertip. Indicating all the minutiae accurately as well as rejecting false minutiae is another issue still under analysis. Our work has united many methods to build a minutia extractor and a minutia matcher. The combination of multiple methods comes from a wide review into research papers. Also some novel changes like segmentation using semantic operations, enhanced thinning, false minutiae removal methods, minutia marking with special considering the triple branch counting, minutia unification by fester a branch into three terminations, and matching in the unified x-y coordinate system after a two-step changeover are used in the work.

© 2016, IJCSMC All Rights Reserved

V. IMPLEMENTATION

The proposed system aims to detect the fake identities by analysing the finger print of the person as shown in figure 3:

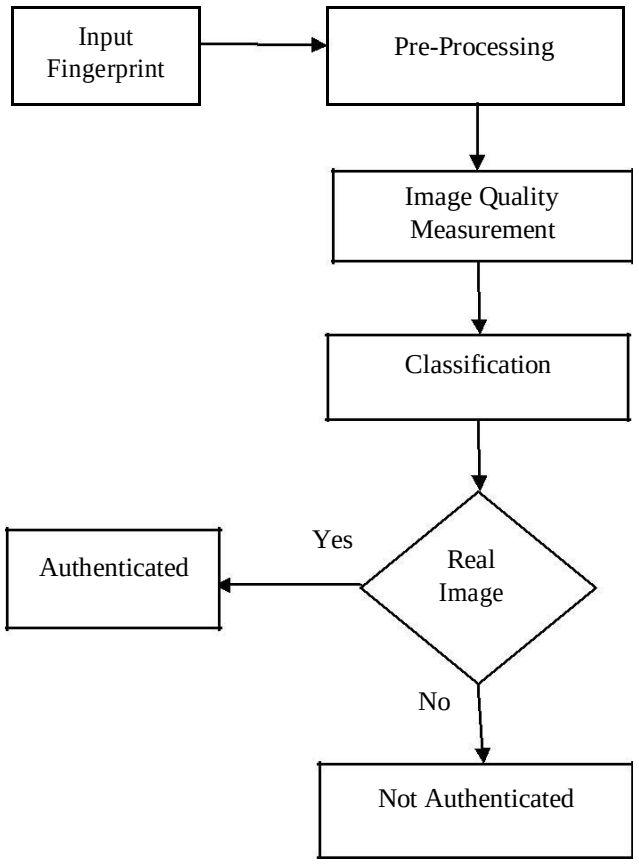

Fig.3. System Architecture

A. Pre-Processing

Pre-Processing is the initial stage where we remove the noise from the image by using median filter. Using adaptive histogram equation the image quality will be enhanced.

B. Image Quality Measurement

Quality of the image are increase by adjusted bar graph equalisation. After pre-processing the quality of the image must be check by image quality measurement. In image quality measurement we are taking 25 feature for each and every bio-metric, they are given in 5 different classes: (i) Difference based measure - Difference measures these features enumerate the perversion between two images on the basis of their pixel wise differences. (ii) Correlation based measure - Correlation based measure the similarity between two digital images can also be quantified in terms of the correlation charge. A alternative of analogue based measures can be obtained by considering the statistics of the angles between the pixel vectors of the authentic and distorted images. (iii) Edge based measure - Edge-based measures the edges and other two-dimensional features such as corners, are some of the most informational parts of an image, which play a key role in the human visual system and in many computer perception algorithms as well as quality assessment applications. Since the structural distortion of an image is tightly linked with its edge degeneracy. (iv) Gradient based measure - Gradients convey important visual information which can be of great use for quality

© 2016, IJCSMC All Rights Reserved

assessment. Many of the misuse that can affect an image are reflected by a change in its gradient. (v) Spectral based measure - Spectral distance measure used for the Fourier transform is another traditional image processing tool which has been applied to the enclosure of image quality assessment.

C. Classification

Based on the classification we recognize the matched and not matched person. Euclidian based classifier is used for classification. Based on the training data we check the test data with train data if our test data and train data is matched means the person is valid person. Else the person is invalid person.

VI. CONCLUSION

The fake detection method that can be used in multiple biometric systems to detect different types of fraudulent approach attack. The objective of the proposed system is to enhance the security of biometric recognition frameworks, by adding liveliness estimate in a fast, user-friendly, and non-intrusive manner, through the use of image quality assessment. The proposed approve presents a very low degree of complexity, which makes it suitable for real-time applications, using twenty five general image quality features derive from one image to distinguish between legitimate and impostor Samples. The proposed approve presents a very low degree of complexity. In this phase the fingerprint detection has been detected by using minute extraction technique and the fingerprint is under processing. In future work liveliness detection of face will be implemented and both fingerprint and liveliness face detection will be matched to check whether the person is certified person to access the valid system.

REFERENCES

[1] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition: Security and privacy concerns," IEEE Security Privacy, vol. 1, no. 2,pp. 33–42, Mar./Apr. 2003.

[2] Jain LC, "Intelligent Biometric Techniques in Fingerprint and Face Recognition", CRC Press, 1999.

[3] S. Adebayo Daramola, Tola Sokunbi and A.U Adoghe "Fingerprint Verification System Using Support Vector Machine" , IJCSE ISSN : 0975-3397 Vol. 5 No. 07 Jul 2013.

[4] Hoi Le, The Duy Bui, "Online fingerprint identification with a fast and distortion tolerant hashing", Journal of Information Assurance and Security 4 page no. 117-123, 2009.

[5] Wei Cui, Guoliang Wu, Rongjin Hua, and Hao Yang, "The Research of Edge Detection Algorithm for Fingerprint Images", IEEE‟ 2008.

[6] Asker M. Bazen, Gerben T.B. Verwaaijen, Sabih H.Gerez, "A Correlation- Based Fingerprint Verification System" ,Workshop on Circuits, Systems and Signal Processing, Veldhoven, The Netherlands, November,2000

© 2016, IJCSMC All Rights Reserved