Scientific Journal of Impact Factor(SJIF): 3.134
e-ISSN(O): 2348-4470
p-ISSN(P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 2,Issue 6, June -2015

A Proposed Architecture for Biometrics Fingerprint Recognition and Authentication Using NN Command Line

Arun Jain[1], Mukesh Kumar[2], Anil Kumar[3]

[1,3]CSE, HCTM
[2]Research Scholars, CSE, HCTM

Abstract -- *Fingerprints are one of the most mature biometric technologies used in forensic divisions worldwide for criminal investigations and therefore, have a stigma of criminality associated with them. Our proposed algorithm is for personal authentication of an individual fingerprints using Neural Network Pattern Recognition tool. Fingerprint recognition is also known as "image acquisition". We will consider the fingerprint as an image and create the database for all the images. After creation of the database the input fingerprint image will be compared for perfect matching with the database templates to recognize the identity. The experiment result of this research work will achieve a good performance on these databases. Finally Results we will analyzed between input and recognized fingerprint image using MSE, PSNR and CCR.*

Keywords- *NN, Fingerprint, MSE, PSNR, CCR.*

I. INTRODUCTION

Biometrics is the science of recognizing the identity of a person based on the physical or behavioral attributes of the individual such as face, fingerprints, voice and iris as shown in figure 1. Biometrics comes from the Greek words bios (Life) and metricos (Measure). It is basically a pattern-recognition system that is used to identify a user. There are three levels of computer security schemes. Level 1 relies on something a person carries, such as an ID badge with a photograph or a computer cardkey. Level 2 relies on something a person knows, such as a password or a code number. Level 3, the highest level, relies on something that is a part of a person's biological makeup of behavior, such as a fingerprint, a facial image, or a signature.

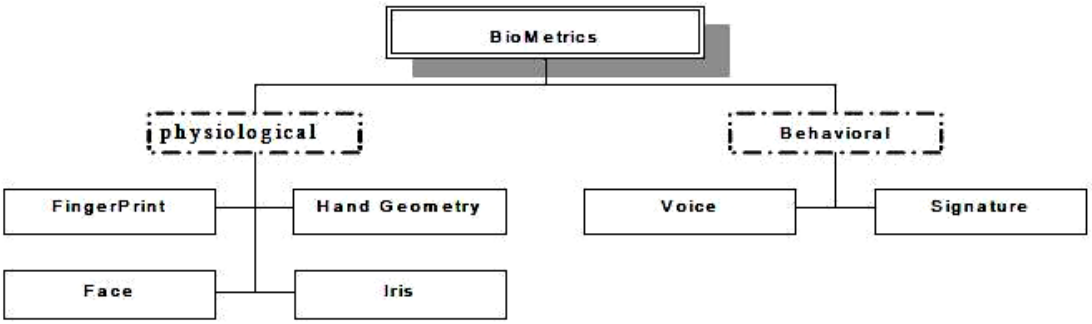

Figure 1: *Factors of a Biometric Authentication System. [1]*

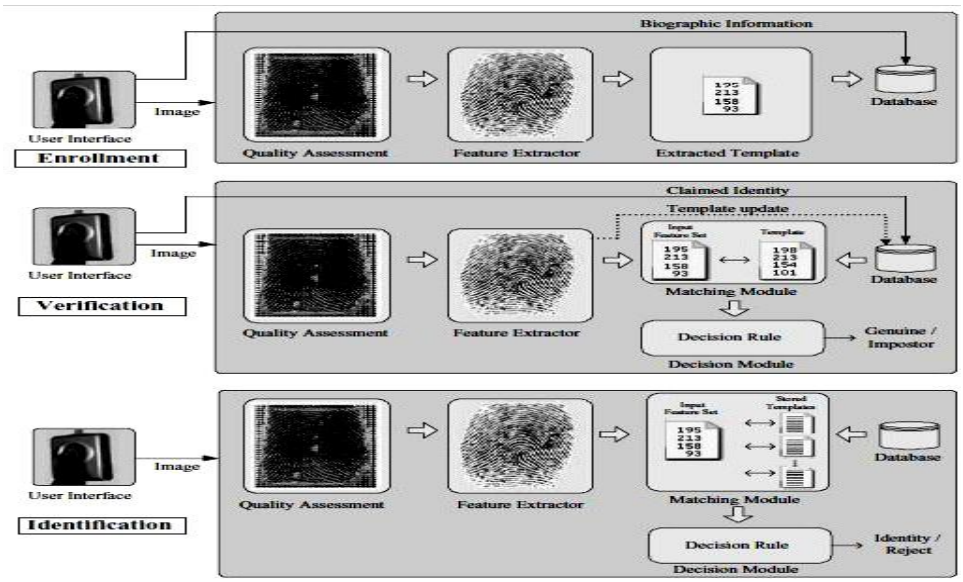

Figure 2: *Verification and Identification stages of a biometric system. [2]*

The problem of resolving the identity of a person can be categorized into two fundamentally distinct types of problems with different inherent complexities shown in figure 2.

Verification (authentication) refers to the problem of confirming or denying a person's claimed identity (Am I who I claim I am?). **Identification** (Who am I?) refers to the problem of establishing a subject's identity - either from a set of already known identities (closed identification problem) or otherwise (open identification problem).

II. FINGERPRINT RECOGNITION

Fingerprint recognition is also known as "image acquisition". In this part of the process, a user places his or her finger on a scanner. Numerous images of the fingerprint are then captured. It should be noted that during this stage, the goal is to capture images of the center of the fingerprint, which contains many of the unique features. All of the captured images are then converted into black and white images.

III. REVIEW OF LITERATURE

Ling Hong et al (2000) [3] developed an improved minutiae extraction algorithm which is faster and more accurate than our earlier algorithm. An alignment-based minutiae matching algorithm has been proposed. This algorithm is capable of finding the correspondences between input minutiae and the stored template without resorting to exhaustive search and has the ability to adaptively compensate for the nonlinear deformations and inexact transformations between an input and a template.

T. Sutomu Matsumoto et al (2002) [4] This paper reports that gummy fingers, namely artificial fingers that are easily made of cheap and readily available gelatin, were accepted by extremely high rates by 11 particular fingerprint devices with optical or capacitive sensors. We have used the molds, which we made by pressing our live fingers against them or by processing fingerprint images from prints on glass surfaces, etc.

R. Snelick et al (2003) [5] presents a multimodal biometrics system analysis that explores various normalization and fusion techniques for face and fingerprint classifiers. This multimodal analysis uses a population of about 1000 subjects, a number ten-times larger than seen in any previously reported study. Experimental results combining face and fingerprint biometric classifiers reveal significant performance improvement over single-mode biometric systems.

Woodard et al (2005) [6] in this paper we present a novel approach for personal identification, which utilizes finger surface features as a biometric identifier. Using dense range data images of the hand, we calculate the curvature-based surface representation, shape index, for the index, middle, and ring fingers.

A. Arakala et al (2007) [7] we propose an authentication scheme using fingerprint biometrics, protected by a construct called a Fuzzy Extractor. We look at a new way of quantizing and digitally representing the minutiae measurements so that a construct called Pin Sketch can be applied to the minutiae. This is converted to a Fuzzy Extractor by tying some random information to the minutiae measurements. We run a matching algorithm at chosen quantization parameters and show that the authentication accuracy is within acceptable limits.

Mr. Ratnakar Anandrao Kharade et al (2012) [8] in this paper, we describe the design and implementation of a prototype automatic identity-authentication system that uses fingerprints to authenticate the identity of an individual. We have developed an improved minutiae-extraction algorithm that is faster and more accurate than our earlier algorithm. This algorithm is capable of finding the correspondences between input minutiae and the stored template without resorting to exhaustive search and has the ability to compensate adaptively for the nonlinear deformations and inexact transformations between an input and a template.

Ravi Bhusan et al (2013) [9] this study describes a fingerprint identification system and its implementation to establish the identity of a person. The approach presented herein matches the fingerprint on two parameter minutia and furrows.

IV. PROPOSED ARCHITECTURE

Matching algorithms are used to compare previously stored templates of fingerprints against candidate fingerprints for authentication purposes. In order to do this either the original image must be directly compared with the candidate image or certain features must be compared [10]. Pattern based algorithms compare the basic fingerprint patterns between a previously stored template and a candidate fingerprint. This requires that the images can be aligned in the same orientation.

Neural networks are composed of simple elements operating in parallel. These elements are inspired by biological nervous systems. As in nature, the connections between elements largely determine the network function. You can train a neural network to perform a particular function by adjusting the values of the connections (weights) between elements.

In addition to function fitting, neural networks are also good at recognizing patterns. ***nprtool*** leads you through solving a pattern-recognition classification problem using a two-layer feed-forward patternnet network with sigmoid output neurons. Finally we will analyze the results between input and recognized character image using MSE and PSNR and CCR.

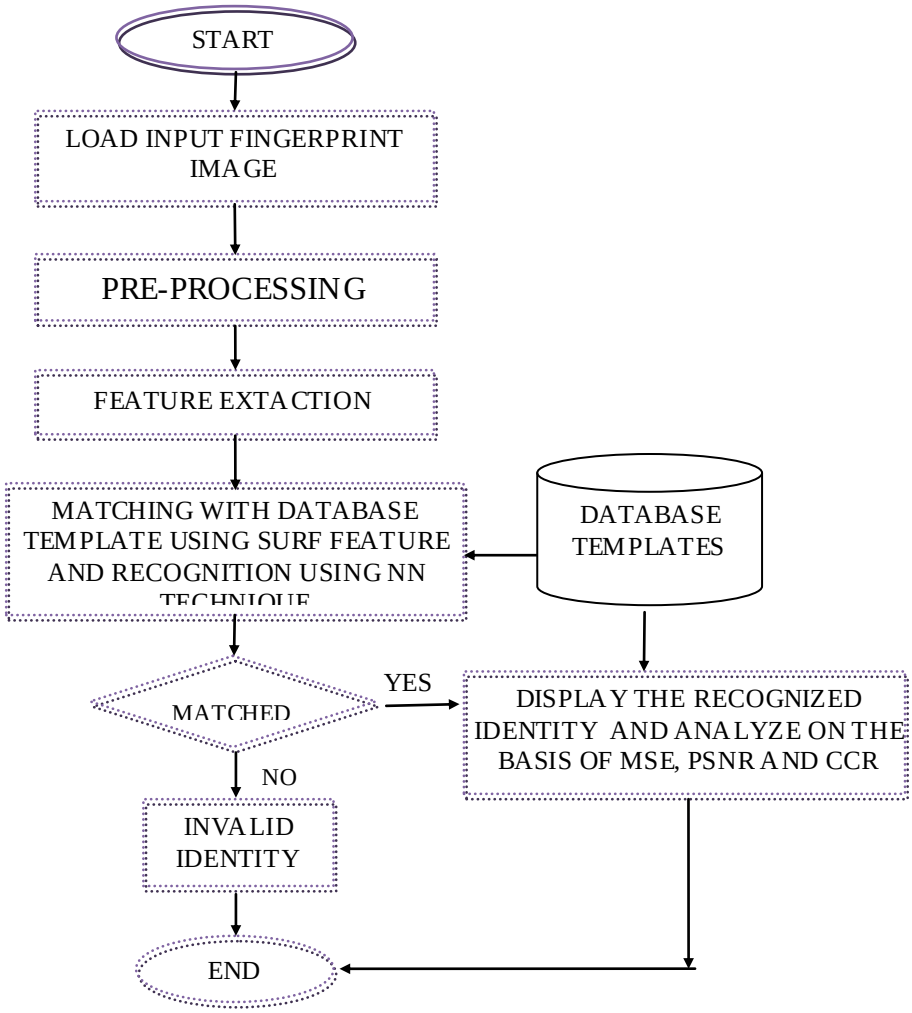

Figure 3: *Flowchart of proposed algorithm*

To do this, the algorithm finds a central point in the fingerprint image and centers on that. In a pattern-based algorithm, the template contains the type, size, and orientation of patterns within the aligned fingerprint image. The candidate fingerprint image is graphically compared with the template to determine the degree to which they match [11]. Here we have developed a flowchart for our proposed algorithm which will use Neural Network Pattern recognition tool for matching input image with the database image. When the input image is matched then it will display the results shown in figure 3.

V. CONCLUSION

Biometric technology provides a strong method of linking persons to identify records. In conclusion, although it is true that in many applications, biometric data is not secret. In many other applications for privacy and trust reasons biometric data is sensitive and we may need to protect it. As biometric technology matures, there will be an increasing interaction among the (biometric) market, (biometric) technology, and the (identification) applications. It is certain that biometrics based identification will have a profound influence on the way we conduct our daily business. It is also certain that, as the most mature and well understood biometric, fingerprints will remain an integral part of the preferred biometric-based identification solutions in the years to come. The proposed work, furthermore, will allow a user to

verify that he or she is using a good biometric system. Compared with other existing systems, the proposed method of personal authentication using NNPRT has merits of high accuracy, high speed, small size and cost-effective.

VI. ACKNOWLEDGE

Thanks to my research supervisor and family member who always support, help and guide me during my dissertation. Special thanks to my father who always support my innovative ideas.

REFERENCES

[1] Kumar, A., Ravikanth, C.: Personal authentication using finger knuckle surface. IEEE Trans. Information Forensics and Security 4(1), 98–109 (2009).

[2] Ravikanth, C., Kumar, A.: Biometric authentication using finger-back surface. In: Proc. CVPR, pp. 1–6 (2007).

[3] Anil Jain and Ling Hong “Identity authentication using Fingerprints” 2002.

[4] T. sutomu Matsumoto” Impact of Artificial "Gummy" Fingers on Fingerprint Systems Proceedings of SPIE Vol. 4677 (2002).

[5] R. Snelick, M. Indovina, J. Yen, and A. Mink. Multimodal Biometrics: Issues in Design and Testing. In Proceedings of Fifth International Conference on Multimodal Interfaces, pages 68–72, Vancouver, Canada, November 2003.

[6] Woodard, D.L., Flynn, P.J.: Finger surface as a biometric identifier. Computer Vision and Image Understanding 100(3), 357–384 (2005).

[7] A. Arakala, J. Jeffers, and K. J. Horadam. Fuzzy Extractors for Minutiae-Based Fingerprint Authentication. In Proceedings of Second International Conference on Biometrics, pages 760-769, Seoul, South Korea, August 2007.

[8] Mr. Ratnakar anandrao kharade, Mr. M.S. Kumbhar / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 6, November- December 2012.

[9] Ravi Bhusan tiwari and Sanjay Sharma, “Biometric authentication using fingerprint “ in Youth Education and Research Trust (YERT), Vol. 1(8) January 2013

[10] J. Hayashi, M. Yasumoto, H. Ito, and H. Koshimizu. Age and Gender Estimation based on Wrinkle Texture and Color of Facial Images. In Proceedings of the Sixteenth International Conference on Pattern Recognition, pages 405–408, Quebec City, Canada, August 2002.

[11] Mazumdar, Subhra; Dhulipala, Venkata (2008). "Biometric Security Using Finger Print Recognition" (PDF). University of California, San Diego. p. 3. Retrieved 30 August 2010.

