Real Time Authentication System using Advanced Finger Vein Recognition Technique

N.Sugandhi, M.Mathankumar, V.Priya

Abstract — **In this modern world, achieving high level security is a critical task. There are many authentication techniques have been improved and comparatively forging techniques also developed. So we are in the need of promising authentication methods by considering more security, reliability, cost effectiveness, easier implementation etc. Authentication includes identification, verification and recognition. It can be achieved using a biometric system which uses human physiological features such as fingerprint, palm print, iris, voice and facial recognitions. All such systems having the chances of threaten easily. To overcome this, advanced finger vein recognition technique is proposed and implemented in real time which is unique, does not need any physical contact, invisible feature, non-invasive, hard to be cloned, provide high accuracy and security using NIR (Near Infra-Red) scanning and advanced image processing technology embedded with PIC16F877A microcontroller. The proposed system can be used anywhere to prevent the unauthorized access and protects the privacy information. It can be extensively implemented in ATM's (Automatic Teller Machines), banking sectors, money transfer systems, military areas, hospitals, entry control etc.**

Index Terms—Authentication, Finger vein, Histogram, Image processing, PIC microcontroller

I. INTRODUCTION

To offer security, generally passwords and pin numbers are used but it does not provide cent reliability and may have the chances of being forgotten by the users. So the researcher's concentration moves into biometric authentication systems [1]. By comparing the available authentication systems, it can be understood that every system has both benefits and drawbacks. For example, Fingerprints and palm prints can be easily left everywhere, whenever touching things. Therefore it does not provide much security. Iris scanning is less comfort and may be injurious due to the lightings while scanning. Voice and facial recognition methods can be easily cloned.

N.Sugandhi is with the Electronics and Communication Department, Muthayammal Engineering College, Namakkal, Tamilnadu, India (corresponding author to provide phone: 9443739800; e-mail: sugandhinatarajan@gmail.com).
M.Mathankumar is with the Electronics and Communication Department, K.Ramakrishnan College of Technology, Trichy, Tamilnadu, India (e-mail: mathankumarbit@gmail.com).
V.Priya is with the Electronics and Communication Department, Muthayammal Engineering College, Namakkal, Tamilnadu, India (e-mail: priyaecemec2011@gmail.com).

Before some years, the identification of an individual depends on the finger vein pattern. Veins are completely matchless even for twins. It is not comparable even in left hand and right hand of a person. Their shapes also vary little as the person growing up. A finger vein authentication technique is comparatively simpler and efficient than fingerprint techniques [2] but it should be designed according to the biometric challenges such as accuracy, security, scalability, privacy etc. The accuracy parameter includes image quality, contrast, brightness etc. To overcome this high quality camera should be used. The designed biometric system must not be compromised at any cost for providing security. In scalability aspect, the count of database images should not affect the speed of the process. The individual identity should not be revealed to others for achieving privacy.

The complete process of the proposed system includes vein capturing, extracting, and pattern matching. If we shine near-infrared (NIR) light through fingers, human tissues pass through most of them whereas haemoglobin in our blood blocks it. Thus veins become visible darker in the image. The vein image of each finger has different properties such as brightness and contrast [3]. Accordingly some image enhancement techniques should be needed for improving the quality of the image. Then the veins are extracting out by detecting centre line of the vein by means of maximum curvature points [4]. The width of the vein may differ when blood pressure or temperature changes but the centre line of the vein always stable. Then the extracted lines will be stored in a database for future purpose. In testing phase, the current extracted pattern will be compared with available database by using two dimensional filters for deciding whether the pattern is matched with the original image or not. In this, Section II describes some of the relevant techniques introduced so far based on the authentication and finger vein analysis. Section III gives the overall system overview. Section IV provides with detailed description of individual units and Section V deals with the implementation on LABVIEW.

II. RELATED WORK

D. Wang et al. [5] describes about the finger vein pattern identification for electronics devices. In this, old biometric techniques are vulnerable for spoofing attacks was proved.

X. Sun et al. [6] developed DSP-based Authentication system using vein images. It made use of LED illuminator for NIR light source. But the drawback is that the shadow will also appear in the scanned images. To overcome the issue, an