Chapter 3

Biometric Authentication Based on Hand Vein Pattern

Munaga V. N. K. Prasad  
IDRBT, India

Ilaiah Kavati  
IDRBT, India

ABSTRACT

Recently, a new biometric technology based on human hand vein patterns has attracted the attention of many researchers. This chapter discusses vein pattern authentication, which uses the vascular patterns of the back of the hand as personal authentication data. Vein information is hard to duplicate because veins are internal to the human body. Vein authentication is one of the most accurate and reliable biometric technologies, which is widely employed in mission-critical applications such as banking, etc. A dynamic ROI extraction algorithm was presented through which more features can be extracted when compared to the fixed ROI. The extracted ROI was enhanced, and then the noise content was removed. The key features that represent the geometric information of the vein pattern were extracted; they are the bifurcation and ending points. This chapter presents a new vein pattern recognition system by assigning different weights to bifurcation and ending points. The approach is tested on a vein pattern database of 60 different hands. Experimental results show the approach achieves 2.5% of Equal Error Rate (EER) and recognition accuracy of 98.24%.

INTRODUCTION

There are many real-world applications where security is a strong requirement, and reliable personal authentication is critical to that security. Since September 2001, public awareness about the need for security has been increased considerably. This has lead to a massive rise in demand for the personal identification systems (Wang & Leedham, 2005). Biometrics plays a major role in today’s security applications. A biometric system is essentially a pattern recognition system that recognizes a
Biometric Authentication Based on Hand Vein Pattern

person based on a feature vector derived from specific physiological or behavioral characteristic that the person possesses (Prabhakar, Pankanti & Jain, 2003). Biometric authentication is the most important technology of the 21st century. As we move forward and face the challenges of the 21st century, security of personal information will continue to be foremost in our thoughts (Wilson, 2010). Our lives are already heavily dependent on secure information flow since nearly everything we touch has some connection to information processing. Bank accounts, transportation systems, mobile phones, and computers are all connected to networks, allowing them to serve our needs. The first question that any of these systems asks us is: “Who are you?” The ability to determine our true identity is critical to ensure the protection of both our personal information and the networks that underpin the digital fabric of society. Without Personal Identification Numbers (PINs), passwords, tokens, and now biometrics, such systems would not be able to reliably know who we are and act to protect our interests. The tokens may be lost or passwords may be forgotten, but the people’s biology features, such as face, finger mark, iris, palm print and vein, cannot be lost or forgotten.

Biometrics is considered a more natural and reliable solution for personal identification situations. Biometrics offers certain advantages such as negative recognition and non-repudiation that cannot be provided by tokens and passwords (Jain, Flynn, & Ross, 2007). Negative recognition is the process by which a system determines that a certain individual is indeed enrolled in the system although the individual might deny it. This is especially critical in applications such as welfare disbursement where an impostor may attempt to claim multiple benefits under different names. Non-repudiation is a way to guarantee that an individual who accesses a certain facility cannot later deny using it (e.g., a person accesses a certain computer resource and later claims that an imposter must have used it under falsified credentials).

The characteristics that help define a good biometric modality (Jain, Bolle & Pankati, 1999) are:

- **Uniqueness:** How the biometric identifier differentiates the individual from one another.
- **Permanence:** How well does a given biometric attribute resist changes due to aging, injury, disease, and other factors.
- **Universality:** How commonly a biometric is found in an individual and how readily it can be used. A good biometric attribute is one that is found in all human beings, and its usability does not vary significantly.
- **Collectability:** The attribute should be suitable for capture and measurement, and must be convenient for the individual to present to the biometric sensor.
- **Acceptability:** The degree of public acceptance and approval for a given biometric modality. This is a very important criterion because user acceptance is critical to the success of any biometric implementation.
- **Performance:** The accuracy, speed, and general robustness of the biometric in varied environmental circumstances.
- **Resistance to circumvention:** How hard it is to spoof or otherwise defeat a biometric.

Biometrics can be easily deployed to various commercial and government applications like e-commerce, welfare-disbursement, boarder control, criminal investigation, physical access control, etc. As we know, banking system has several leakages such as security threats and transaction frauds in the available system. The use of biometrics is a near perfect solution to such leakages. During the past few decades, many researchers have carried out on utilizing various biometrics for personal recognition. Amongst those biometrics, the most popular ones are Fingerprint, Face, Iris, Palm print, Retina, Hand geometry, Ear for physiological biometrics, as well as Keystroke, Gait, Signature, Voice, DNA, Odor for behavioral one.
Related Content

Identity Management Systems
www.igi-global.com/chapter/identity-management-systems/61538?camid=4v1

Studying the Blood Plasma Flow past a Red Blood Cell with the Mathematical Method of Kelvin's Transformation

Investigation of Human Monitoring Capabilities for Multiple Watch Windows
www.igi-global.com/article/investigation-of-human-monitoring-capabilities-for-multiple-watch-windows/177209?camid=4v1

Multimodal Biometric Hand-Off for Robust Unobtrusive Continuous Biometric Authentication
www.igi-global.com/chapter/multimodal-biometric-hand-off-robust/59667?camid=4v1