IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 3, March 2020

Exploring both Major and Minor Knuckle Pattern for Human Identities

Roshini Shaheen[3], Aneesha Fathima[1], Mujaida[2], Anbarasan[4], Vignesh[5]

Student, Computer Science and Engineering, Dhaanish Ahmed Institute of Technology, Tamil Nadu, India[1, 2,3]

Professor, Computer Science and Engineering, Dhaanish Ahmed Institute of Technology, Tamil Nadu, India[4, 5]

Abstract: The biometrics is the challenging task for researcher. Biometrics based authentication is just impossible to help us if we don't know what are the requirements. Biometrics authentication must provide the security level, unattended system, Spoofing and Reliability. Among all the modalities FKP broadly explored which has not yet attracted significant attention of researchers. Finger knuckle is user centric contactless and unrestricted access control. We have proposed a novel person identification system that uses knuckle print features extracted by using Radon transform. The knuckle print image has been viewed as a texture image. The local features from the knuckle print represent the texture information present in the image in better sense .Radon transform computes the line integral along parallel paths in a certain direction.

Keywords: Finger Biometric, Finger Knuckle Methodology, Pattern Recognition, Finger-vein Identification.

I. INTRODUCTION

As with growth of information technology ,the need of the security has became a prime issue in the area of IT. The security can be managed in number of ways . One way to improve security is by identifying or verifying the person with some technique so, the basic idea is the identity of the person which can be improve the security. Secure Computing is information security is applied computing devices such as computers and smartphones. Most computer security measures involve data encryption and passwords. The term " Biometrics " is derived from the Greek words "bio"(life) and "metrics"(to measures). Biometric refers to the automatic identification of a person based on his /her physiological or behavioral characteristics. Existing biometric systems involve various technologies such as face, iris fingerprint and finger vein recognition. Finger vein recognition is one of the promising approaches for human identification because of its advantages on living body identification and high security. However, upon image capture, finger vein identification can suffer from performance degradation caused by illumination variation, finger positional variation shading and misalignment. In this paper finger knuckle also be used, exploring the both major and minor finger knuckle pattern with features extraction, verifying and identification. Finger knuckle is user-centric, contactless and unrestricted access control. We have proposed a novel person identification system that uses knuckle print features extracted by using Radon transform. Advantages of finger knuckle print (FKP) include rich in texture features , easily accessible , contactless image acquistion invariant to emotions and other behavioral aspects such as tiredness, stable features and acceptability in the society.

1.1 SECURE COMPUTING

Secure computing (also known as cyber security or computer security) is information security is applied to computing devices such as computers and smartphones, as well as computer networks such as private and public networks, including the internet. In the computer industry, the term security refers to techniques for ensuring that data stored in a computer cannot be read or compromised by any individuals without authorization . Most computer security measures involve data encryption and passwords. Data encryption is the translation of data into form that is unintelligible without a deciphering mechanism. A password is a secret word or phrase that gives a user access to a particular program or system.

Computer security is important because without it, your computer would by vulnerable to viruses, worms, and other malicious code. Security tool is a rogue antispyware program that uses fake security alerts and system scan results to convince computer user believe that they must purchase the Security Tool program to remove the found threats. Security Tool , through the use of trojans and malicious websites, can be installed onto your computer without notification.

Most of the time, the term " Computer Security" refers to the security of a computer's insides. The data and

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 9, Issue 3, March 2020

compendious information that most users store on their hard drives is often far more valuable than are the machines themselves. Broadly speaking, the importance
of computer security lies in how harmful it can be if that data is lost. Many computer users don not realize that simply accessing the web could be making their computers more vulnerable. The security has to increas-
e rapidly because the attackers are daily increasing. The users are mostly wanted to secure the information on their computer because:

- For ensuring that our information remains confidential and only those who should access that information.
- Knowing that no one has been able to change our information, so we can depend on its accuracy.

Making sure that our information is available when we need it (by making back-up copies and if appropriate storing the back-up copies off-site).

Secure Computing Corporation (SCC) is a public company that developed and sold computer security appliances and hosted services to protect users and data. McAfee acquired the company in 2008.

Taking charge of computer security usually is as simply as installing an antivirus program or purchasing basic computer security software. The importance of computer security also extents to computer skills. Users should educate themselves about the risks of the Internet, particularly with respect to downloads. They also should take care when sharing personal information with untrusted websites and should keep credit card information closely guarded.
The authentication is one the most widely used forms of security and forms the most basic security mechanism. Biometric refers to the automatic identification of a person based on his/her physiological or behavioral characteristics.

1.2 BIOMETRIC

This method of identification is preferred over traditional methods involving passwords and PIN numbers for various reasons: the person to be identified is required to be physically present at the point-of-identification; identification is based on biometric techniques obviates the need to remember a password or carry a token. This paper attempts to look at the various advantages offered by this method of user authentication and also looks at the pits falls encountered in its implementation, some of which are specific to biometrics.
Using biometrics for authentication has obvious conceptual advantages when compared to the traditional use of passwords or PINs. In theory, biometric data cannot be guessed, stolen or shared among users, therefore providing increased security to a system. It also relieves the user from the burden of having to remember a password, or worse multiple passwords for different systems within an organization.
In addition to authentication, biometric applications are employed in large-scale identification systems, where they offer two important benefits: fraud detection and fraud deterrance. For example, one person can claim multiple identities, using fraudulent documents, to receive benefits from a public program. Without the use of biometrics, it would be extremely difficult to discover that the person has multiple registrations, considering the large volume of data stored in the system. Biometrics can therefore contribute to fraud detection. On the other hand, the presence of such a feature in a system introduces a physiological effect on people, as it dissuades individuals from attempting to register more than once, as they become aware of the fact the their unique physiological/behavioral characteristics are used to identify them. For this effect, biometrics provides the benefit of fraud deterrance.

There are 3 basic function in any biometric system:

1.2.1 ENROLLMENT

A person's reference data is produced in the enrolment process. The reference data contains the most basic information about a person's biometric features. In the case of the ID Module these are the fingerprint features or reference data that can be produced from this. During the subsequent identification and verification processes in the biometric system, this reference data is used for comparison with the current features. The enrolment can be performed by loading biodata or by feeding in the biodata on the module itself.

1.2.2 VERIFICATION

Verification is checking a person against a predefined identity. This means that the identity of the expected person must be known before the start of the verification process. This can be done for example by entering a person's name or data, via a keyboard , keypad or card.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 9, Issue 3, March 2020

1.2.3 IDENTIFICATION

Identification means that the biometric system checks the identity of the finger specific features that a person enters through comparison with the archived fingerprint features of multiple people. The identity of the person being checked is therefore returned as a result of a successful identification.

II. PROBLEM DEFINITION

Automated identification of humans using their unique anatomical characteristics has been increasingly investigated for their applications in human surveillance and image forensics . Many traits like fingerprint face iris, palm vein, DNA and many others have been used for personal identification. One new biometric trait that has attracted researchers in the recent years is the finger knuckle print. Accurate identification of finger knuckle patterns can be beneficial for several applications involving forensic and covert identification of suspects. To build a secure and authenticated system for finger knuckle.

III. NEED OF FINGER KNUCKLE PRINT

There are many different types of Biometrics, these are, IRIS Identification, Retinal Identification, Face Recognition, Voice Recognition, Fingerprint, Hand/Finger Geometry, Signature verification, Keystroke Dynamics, and other esoteric biometrics. Hand-based biometrics, such as fingerprint and hand geometry, is the most prevalent biometric system in the marketplace.
However, fingerprint suffers from a major drawback, which is its proneness to anti-security threats, such as
the reproduction of fingerprints left on surfaces to deceive the system. On the other hand, the hand geometry features are not descriptive enough for identification when the number of users grows larger. Problem related to other identifiers are as human voice and signature can be copied, duplicates are available so face recognition will not be foolproof identifier.
Palm print and finger print can be simultaneous extracted from the palm side which can give better performance improvement, but size of finger knuckle is very small as compared to palm print and offers more attractive alternative as it requires less processing as compared to palm print. These biometric identifier systems can cause problem in children and adults.
Many concepts are proposed to explore an alternative way to utilize the major knuckle print for human identification. This biometric system implementation is contactless and peg-free and free from factors like tiredness etc. which causes problem in other biometric identifiers. But in some humans the major knuckle pattern of finger can be occluded by hair and there are some cases where only the minor knuckle portions are visible in forensic images. By considering this problem, now need to utilize the major and minor portions simultaneously.

IV.PROPOSED SYSTEM

We have proposed a novel person identification system that uses knuckle print features extracted by using Radon transform. The knuckle print image has been viewed as a texture image. The local features from the knuckle print represent the texture information present in the image in the better sense. Radon transform computes the line integral along parallel paths in a certain direction.

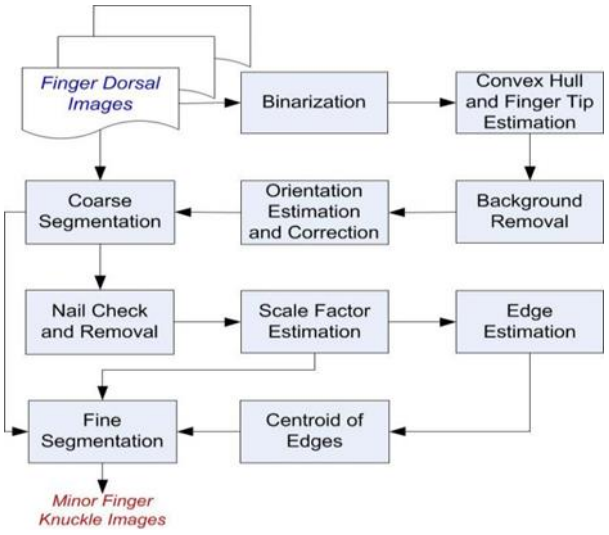
The personal identification system using knuckle prints operates in two modes namely enrolment phase and identification phase. During the enrolment phase, several knuckle prints of the persons obtained from the FKP scanner are passed to the system. The samples captured by knuckle print scanner are passed through pre-processing and feature extraction to produce the templates which are then stored in the database.

In the identification/recognition mode, the query knuckle print image is passed to the system. These query knuckle prints are passed through pre-processing and feature extraction block. The extracted features from the query knuckle print are then compared with templates stored in the database in order to find the correct match. A distance measure is used to find the close match between the query knuckle print and the template imprints stored in the database.

4.1 OVERVIEW OF THE PROJECT

Automated biometric identification using finger knuckle images has increasingly generated interest among researchers with emerging applications in human forensics and biometrics. Prior efforts in the biometrics literature have only investigated the " major" finger knuckle patterns that are formed on the finger surface joining proximal phalanx and middle phalanx bones.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 9, Issue 3, March 2020



The biometrics is the challenging task for researcher. Biometrics based authentication is just impossible to help us if we don't know what are the requirements. Biometrics authentication must provide the security level, unattended system , Spoofing and Reliability. Among all the modalities FKP broadly explored which has not yet attracted significant attention of researchers. Finger knuckle is user-centric, contactless and unrestricted access control. We have proposed a novel person identification system that uses knuckle print features extracted by using Radon transform. The knuckle print image has been viewed as a texture image. The local features from the knuckle print represent the texture information present in the image in better sense. Radon transform computes the line integral along parallel paths in a certain direction.

The possible use of major finger knuckle patterns which are formed on the finger surface joining distal phalanx and middle phalanx bones. The major finger knuckle patterns can either be used as independent biometric patterns or employed to improve the performance from the major finger knuckle patterns. A completely automated approach for the minor finger knuckle identification is developed with key steps for region of interest segmentation, image normalization, enchancement and robust matching to accommodate image variations.

The personal identification system using knuckle prints operates in two modes namely enrolment phase and identification phase. During the enrolment phase, several knuckle prints of the persons obtained from the FKP scanner are passed to the system. The samples captured by knuckle print scanner are passed through pre-processing and feature extraction to produce the templates which are then stored in the database. In the identification/recognition mode , the query knuckle print image is passed to the system . The query knuckle prints are passed through pre-processing and feature extraction block. The extracted features from the query knuckle print are then compared with templates stored in the database. A distance measure is used to find the close match between the query knuckle print and the template imprints stored in the database.

4.2 FINGER IMAGE ACQUISITION

The backside of finger is to be acquired using web cam or smartphone or digital camera. An acquisition system has been developed for the collection of finger -back images. A very user-friendly imaging system is constructed. This imaging system uses a web camera focused against a white background under uniform illumination. The camera has been set and fixed at a suitable distance from the imaging surface.

4.3 PRE-PROCESSING FOR FEATURE EXTRACTION

Each of these images requires localization of region of interest for the feature extraction. The region of interest is the region having maximum knuckle creases. An ROI can be cropped from the original image for reliable feature extraction and matching. This gives segmentated finger knuckle image.

The image is captured; it is pre-processed to obtain only the area information of the FKP.
The detailed steps for pre-processing process are as follows first; apply a Gaussian smoothing operation to the original

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 9, Issue 3, March 2020

image. Second, determine the X axis of the coordinate system fitted from the bottom boundary of the finger can be easily extracted by a Canny edge detector. Third , determine the Y-axis of the coordinate system by applying a Canny edge detector on the cropped sub-image original base on X-axis , then find the convex direction coding scheme.

4.4 KNUCKLE FEATURE EXTRACTION

The knuckle image mainly consists of curved lines and creases. Knuckle curved lines and creases are to be detected. Knuckle features are then extracted. In feature extraction, first the target vector is created. Target vector is n x n matrix with are zeros. The purpose of feature extraction is to extract the significant features of images.

4.5 IDENTIFICATION

Identification is the final application portion of the system it is used to identify the name of the user. The input feature vector is extracted from the user input image file. The binarized templates generated from every finger knuckle image is subjected to template matching to ascertain the similarity between claimed user identity and the input template(s) stored in the enrollment database. The degree of the similarity or the dissimilarity between two templates is determined using the Hamming distance.

4.6 ARCHITECTURE DIAGRAM

An architectural diagram is a rich and rigorous diagram, created using available standards, in which the primary concern is to illustrate a specific set of tradeoffs inherent in the structure and design of a system or ecosystem. The architectural of feature image extraction is described in figure 1.

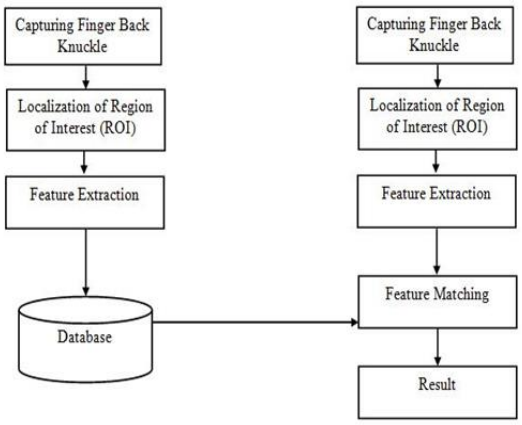


Fig 1. Architecture Diagram

V. SOFTWARE OVERVIEW

5.1 FRONT END

The front end is an interface between the user and the back end. The front ends may be distributed amongst one or more systems. The front is an abstraction, simplyfying the underlying component by providing a user-friendly interface. Front end development is the development of those elements of a website that the customer sees and interacts with directly.

5.2 MATLAB

MATLAB (matrix laboratory) is a multi-paradigm numerical computing environment and fourth -generation programming language. Developed by Math- works, MATLAB allows matrix manipulations, plotting of functions and data, implementation of algorithms, creation of user interfaces, and interfacing with programs written in other languages, including C, C++, Java, Fortran and Python.

Although MATLAB is intended primarily for numerical computing, an optional toolbox uses the MuPAD symbolic

engine, allowing access to symbolic computing capabilities. An additional package, Simulink, adds graphical multi-domain simulation and Model-Based Design for dynamic and embedded systems.

In 2004, MATLAB had around one million users across industry and academia. MATLAB users come from various backgrounds of engineering, science, and economics. MATLAB is widely used in academic and research institutions as well as industrial enterprises.

VI. FUTURE ENHANCEMENT

This paper has successfully investigated the possibility of employing minor finger knuckle images for the biometric identification. The coarse-to-fine segmentation strategy developed in this paper has been quite successful as it has been able to achieve higher matching accuracy. In future, both major and minor knuckle images are retrieved for better performance and security. The new matching method is created for higher matching accuracy.

VII. CONCLUSION

The possibility of employing minor finger knuckle images for the biometric identification. The coarse-to-fine segmentation strategy developed in this paper has been quite successful as it has been able to achieve higher matching accuracy. The use of only major knuckle patterns, small number of subjects, and lack of systematic evaluation in various age groups reflects narrow focus on this topic in this paper. Availablility of such images acquired after an interval of years in public domain will serve as useful evidence to favourly argue on suspects/offenders for forensic The finger dorsal images employed this paper were acquired in single session and therefore conclusions on the accuracy points towards the uniqueness of major/minor finger knuckle patterns in the given database rather than on the stability of such patterns with time.
and law-enforcement applications.

ACKNOWLEDGEMENT

The authors are grateful to reviewers for thorough reports with comments and corrections that have helped to improve this article. I would like to thanks to **Prof. Anbarasan** who guided and supported me for this work.

REFERENCES

[1]. Aoyama. S, Ito .K, and Aoki .T (2011), “Finger-knuckle-print recognition using BLPOC-based local block matching,” in Proc. ACPR,pp. 625–529.
[2]. Deepak Gautam, Usha Mittal (2014), “An Efficient and Improved Technique For Human Identification Using Finger Vein” International Journal of Latest Scientific Research and Technology 1(2), pp. 72-77 ISSN: 2348-9464.
[3]. Kam Yuen, Ajay Kumar, “Contactless Finger Knuckle Identification Using Smartphone‟s” Department of Computing, The Hong Kong Polytechnic University.
[4]. Lin Zhang, Lei Zhang, And David Zhang, “Finger-Knuckle-Print Verification Based On Band-Limited Phase-Only Correlation” Biometrics Research Center,
[5]. Department of Computing, The Hong Kong Polytechnic University.
[6]. Mathivanan B, Palanisamy V and Selvarajan S (2012), “A Hybrid Model For Human Recognition System Using Hand Dorsum Geometry And Finger-Knuckle-Print” Journal of Computer Science, 8 (11), 1814-1821, ISSN 1549-3636.
[7]. 6. Shubhangi Neware1, Dr. Kamal Mehta, Dr. A.S. Zadgaonkar (2012), “Finger Knuckle Surface Biometrics” International Journal of Emerging Technology and Advanced Engineering Website, ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 2, Issue.