IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 7, July 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.542

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907177 |

Contactless Major and Minor Knuckle Patterns Identification

Greeshma.K, Reshma.P

M. E Student, Dept. of Computer Science and Engineering, CMS College of Engineering and Technology, Coimbatore, India

Assistant Professor, Dept. of Computer Science and Engineering, CMS College of Engineering and Technology, Coimbatore, India

ABSTRACT: Contactless biometric identification using finger knuckle images has shown significant potential for the e-business and forensic applications.one of the key challenges in accurately matching the real-world contactless finger knuckle images is related to the knuckle pattern deformations that are involuntarily generated due to finger pose-changes. 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.

KEY WORDS: Finger Biometric, Finger Pattern Recognition, Finger-vein Identification.

I. INTRODUCTION

The Authentication is one of 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. 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 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 pit falls.

Fingerprint recognition can also be categorized into minutiae extraction based and spectral features of the image based. All technologies of fingerprint recognition, identification and verification, minutiae extraction based and spectral features based, each has its own advantages and disadvantages and it may requires different treatments and techniques. The choice of which technologies to use is application specific. Several biometrics technologies are susceptible to spoof attacks in which fake fingerprints, static palm prints, static face images can be successfully employed as biometric samples to impersonate the identification. At the highest level, all fingerprint recognition systems contain two main modules feature extraction and feature matching.

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 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 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

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907177 |

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 increaserapidly because the attackers are daily increasing. The users are mostly wanted to secure the information on their computer.

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-ofidentification; 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 program. Without the use of biometrics, it would be extremely difficult to discoverthat 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 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 deterrence

For example, one person can claim multiple identities, using fraudulent documents, to receive benefits from a public more than once, as they become aware of the fact their unique physiological/behavioral characteristics are used to identify them.

There are 3 basic functions 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 bio-data or byfeeding in the bio-data 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.

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. NEED OF FINGER KNUCKLE PRINT

There are many different types of Biometrics, these are, IRIS Identification, Retinal IdentificationFace 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

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907177 |

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.

III. PROPOSED SYSTEM

We have proposed a novel person identification systemthat 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 preprocessing 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.

3.1FINGER 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.

3.2 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 segmented 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 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

3.3KNUCKLE 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. Targetcreation 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

3.4 IDENTIFICATION

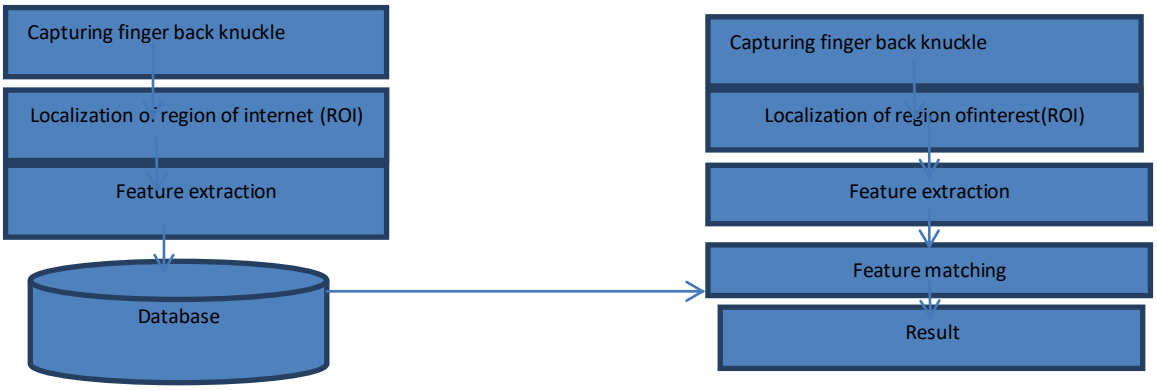
identification is the final application portion of the system it is used to identify the name of the user. The input feature vector is extracted from the user input image file. The binarized templates generated from every finger knuckle image is subjected to template matching to ascertain the similarity 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.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907177 |

3.5 ARCHITECTURE DIAGRAM



Finger image acquisition : The backside of finger is to be acquired using digital camera.

Localization of Region of Interest (ROI): 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. It is necessary to construct a local coordinate system for each FKP image. With such a coordinate system, an ROI can be cropped from the original image for reliable feature extraction and matching.

Extracting Segmented Finger Knuckle Image: The Region of Interest is to be automatically extracted using the edge detection based approach. This gives segmented finger knuckle image.

Knuckle Image Enhancement: The finger surface is highly curved and results in uneven reflection which also generates shadow. The knuckle images therefore have low contrast and uneven illuminations. These undesirable effects are to be reduced using image enhancement techniques.

Knuckle Feature Extraction: The enhanced knuckle image mainly consists of curved lines and creases. Knuckle curved lines and creases are to be detected. Knuckle features are then extracted.

Database Establishment

IV. CONCLUSION

This paper proposes contactless, cost effective and user friendly finger knuckle surface based biometric identifier for personal identification. Unlike most previous work, this approach uses single knuckle print image and it need not require collecting large amount of knuckle images. It is efficient approach as it requires less computation and processing time. The proposed method improves security and improved efficiency in comparison traditionally used biometric identification.

REFERENCES

1. A.Kumar, “Contactless Palmprint Identification using Deeply Learned Residual Features,”April 2020.
2. A.Kumar, Toward pose invariant and completely contactless finger knuckle recognition,”,jul.2019.
3. A.Kumar, Towards more accurate matching for contactless palmprint images, IEEE Trans.info.Forensics&Security,jan 2019.
4. The Hong Kong Polytecnic University Contactless Finger Knuckle Images Database(version 3.0),2019.
5. J.Kim,K.Oh,B.S.Oh,Z,Linand K.A.Toh,”A line feature extraction method for finger-knuckle-print verification,.”Cogn.Comput.,2018.
6. A.Kumar and Z. Xu,”Personal identification using minor knuckle patterns from palm dorsal surface,”IEEETrans.Info.Forensicand Security,Oct.2016.
7. Q,Zheng,A.Kumar,andG.Pan”A 3D Feature Descriptor Recovered from a Single 2D PalamprintImage,”IEEE Trans. Pattern Analysis & Machine Intell.,jun 2016.
8. Deepak Gautam, Usha Mittal (2014), “An Efficient and Improved Technique For Human Identification Using Finger Vein” International Journal of Latest Scientific Research and Technology .

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907177 |

9. 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.
10. Shubhangi Neware1, Dr. Kamal Mehta, Dr. A.S. Zadgaonkar (2012), "Finger Knuckle Surface Biometrics" International Journal of Emerging Technology and Advanced Engineering Website.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 7.542

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details