STRATEGY ON FINGER PRINT IDENNTIFICATIO PROCESS USING SHORT TIME FOURIER ANALYSIS METHOD

[1]PRATAP KUMAR DEVARAPALLI, [2]VEERA PUNNAIAH MANDA
[1]Assistant Professor, Dept of ECE, St. Mary's Women's Engineering College, Guntur Dt, AP, INDIA.
[2]Assistant Professor, Dept of ECE, Gudlavalleru Engineering College, Gudlavalleru, Krishna Dt, AP, INDIA

ABSTRACT: Identification and authentication are critical assignments as we keep on moving into an information-oriented age. Authentication is getting to be important for two of the primary gadgets utilized by about everybody today, i.e., workstations/netbooks and Cell telephones. Fingerprint matching and recognition are extremely difficult problems. Several different important factors are to be considered whil attempting to find a fingerprint match. In this paper we propose a finger print identification system using STFT analysis process. This STFT analysis is also known as region mask which will distinguish the map between fingerprint and the background regions. The proposed system will reduce the computational complexity by using Fourier domain enhancement. At last compared to existed system, the proposed system gives efficient results.

KEY WORDS: Fingerprint, biometrics identification, Analysis of fingerprint, Short Time Fourier analysis (STFT), Fourier domain enhancement.

I.INTRODUCTION

Fingerprint matching analysis has been a useful measure of identity and authenticity for over 2,000 years, first in China as a method of authenticating documents. Fingerprint identification and verification is based on the assumption that no two individuals share identical fingerprint patterns. Fingerprint ridge and pore patterns (in whole or in part) can be transferred to solid surfaces by deposition of contact residue comprised of skin cells, oil, salt and moisture, or optically captured to provide a two-dimensional representation. Such representations can be stored indefinitely in photographic or digital form, facilitating comparison against fingerprint archives. The process of determining a fingerprint match entails the evaluation of spatially distributed components of fingerprints that are in alignment as opposed to those those are not. Feature extraction is pivotal to the function and performance of a fingerprint recognition system. The fingerprint ridge-features used by our library are primarily the minutiae. Extraction is performed through the use of the "mindtct" program.

The most common application of a biometric system is identification, although this is changing with the widespread availability of inexpensive scanners for fingerprints and the biometric software required to use them. For the purposes of this thesis "identification" refers to the determination of a person's identity from a database of identity-to-biometric-characteristic pairs. It is obvious that in the case of identification, the whole available database must be compared against the query template. As a result of the "1-to-N" comparisons that must be made, execution time is often a constraint.

The processes involved in the gathering and storage of prints generate distortions, artifacts and noise which need to be managed so as to increase the accuracy and precision of any fingerprint matching system. Very often, only partial representations of the prints are available, further increasing the complexity of the pattern matching process. Although fingerprint recognition is a well-studied problem, matching highly fragmented fingerprints is a very difficult problem, and is widely considered to be unsolved. First, we decided to develop a detailed study of biometric systems, including the design, specification and construction of a complete fingerprint recognition system. Such a system could be viewed as a "pipeline" of data which has a number of

components characterizing its functionality. We had to understand, then collect or design and implement all the necessary components, or modules, of the final system. The modules involved included raw data collection, image processing and enhancement, feature extraction and template construction, and finally minutia matching. In addition to the components and functionality typically included in a fingerprint recognition system, we wished to create a reusable and flexible fingerprint recognition system which could be extended to the users/developer's liking. The construction of a fingerprint recognition system, as well as the task of studying and implementing several different algorithms available in the literature, provided us with insight into the issues related to our next task the implementation of a new approach to fingerprint matching. The raw data collection is handled by the library through the use of the open source fingerprint scanner library "fprint".

There are numerous ways to collect fingerprints, and many modern techniques only require that a finger be pressed against a sensor which prevents the need to use the traditional ink-and-paper family of fingerprint collection methods, which are often unpleasant. Many of the fingerprint-based biometric systems in use today are extremely efficient, and can offer results in seconds. Important issue with using fingerprints in security (verification) is that security measures built on fingerprints are relatively easily circumvented. If fingerprints from an individual can be obtained, with the proper "tools", there is nothing stopping a person from accessing a system secured solely through fingerprints. However, by combining fingerprints and some other type of verification, an acceptable level of security can be reached.

II. BACKGROUND

It is widely believed that all humans are unique. This premise underlies the development of methods with the potential to systematically identify each and every human on the planet on the basis of biometrics such as DNA sequences, voice profiles, eye patterning and fingerprints. Collection of these measures can be made with or without our consent and used to provide evidence that we participated or did not participate in some event or that we should be included or excluded from some grouping of people. Increasing populations and global movement of people has increased the need for cheaper, faster and more accurate biometric systems. Such biometric evaluations rely heavily on advances in computer hardware and software.

Biometric Systems can roughly be defined as systems which use biological characteristics of individuals for some specific purpose. The most common purpose of biometric systems is to either establish or authenticate a person's identity based on the relevant biological characteristic. This characteristic is typically one of two types: physiological or behavioural. Many different potential physiological and behavioural characteristics that could be used by a biometric system for identification or authentication purposes have been reported in the literature. Of the two types of biometrics, the most commonly used ones are physiological. Although less common, there are also many different types of behavioural characteristics that could be used for identification or authentication purposes such as signatures, keystrokes, or skill at a particular task.

Another application for biometric systems is authentication/verification. For the purposes of this thesis, verification or authentication refers to the verification of a claimed identity, usually for security applications. In this case, it is sufficient to

achieve a comparison against only the biometric data associated with the claimed identity. Since only a single comparison is required, the corresponding execution time of the task is not usually a constraint. This allows authentication algorithms to be much more discriminating in their analysis, and consequently they can be more accurate in their claims.

Biometric systems designed for identification often have very large databases, with up to 66 million templates in the case of the Integrated Automated Fingerprint Identification System (IAFIS). Since their databases usually must be quite large, their storage requirements and the cost of storage will be correspondingly high. The storage requirements of authentication-based systems are likely to be much smaller and restricted, for example, a company desiring biometric authentication need only store enough images to account for each of their employees, or a computer user who desired biometric authentication need only store enough images to account for each of those people s/he wished to have access to the their personal computer. Two terms are widely used to discriminate between different common configurations of biometric systems, namely the terms "on-line" and "off-line".

• **On-line:** An "on-line" biometric system should be able to provide "immediate" results. It should, essentially be able to act on its own in an unattended/supervised manner. The biometrics are usually collected on site and the enrolment process could potentially be unsupervised. On-line biometric systems are somewhat geared towards personal or commercial use.

• **Off-line:** An "off-line" biometric system is typically used when more accurate results or a higher level of security is needed. "Off-line" systems usually take a longer time to perform matching and enrolment, and often both of these tasks must be supervised due to the nature of the system's use. There may be additional restrictions on their use, e.g., high cost hardware requirements such as those which provide support for massive parallelism and storage, or manual supervision and human intervention at the final stages of identification to ensure the lowest error rate possible. Off-line biometric systems are suited for use in high security and other critical applications like law enforcement.

III. RELATED WORK

Fingerprints are viewed as one of the supreme proof to distinguish a man. The procedure of identifications proof requires examination of addressed and standard fingerprints. The creed embraced by various unique mark analysts considers it a "correct" science, however now some of them think about it as a misinterpretation. Since it isn't "correct" as science, in which results or estimations are communicated in correct numbers. In the meantime the unique mark distinguishing proof science can't be considered as "engaging" science like ornithology, in which a specific types of winged animal recognized, yet not a person inside similar species. Or maybe, unique mark recognizable proof falls into a classification of connected science in which the logical learning and standards can be connected to the issues to touch base at ends. This application gives logical legitimacy to the ends. These ends can be additionally reinforced by utilizing mechanized Software. The Automated Fingerprint Identification System (AFIS) was brought into scientific work after 2000. AFIS depended on biometric ID system which utilizes computerized imaging innovation to get, store, and dissect information identified with unique mark. The

AFIS was initially utilized by the U.S. Federal Bureau of Investigation (FBI) in criminal cases. In this robotized Software framework, optical sensor based perusers are utilized to peruse and procured unique mark pictures in the accompanying three phases:

• Firstly, picture preparing calculations are utilized to acquire dark tone impressions of the unique mark picture.

• Secondly, the prepared picture is hence used to separate the particulars.

• Third step is examining the position of various details on fingerprints, with the assistance of situation coordinated calculations.

The extricated pictures are contrasted and the databases present in the framework and results are gotten. In any case, as opposed to the abovementioned, in the present investigation a semi-self-governing the system has been utilized. In this manner, in the present examination, a thorough endeavour has been made to separate physically all the details present in the unique finger impression with the assistance of Adobe Photoshop Software and to build up an altered matrix which can be utilized to deliberately discover the situation of the particulars alongside estimating certain extra element like Angle. The strategy can possibly complete correlation with framework technique and is required to add objectivity to the present day fingerprints examination situation.

IV. FINGER PRINT IDENTIFICATION PROCESS

All biometric systems follow a similar pattern in their construction and organization. This is true for the phases up to and including the process by which they identify or authenticate individuals. The process begins with the data collection of raw biological data from the subjects). This includes pre-processing of the raw data (if necessary). This is followed by the extraction of the useful features and the construction of the template. Matching based on the templates obtained from feature extraction is then involved.

1) Raw Data Collection

Collection of raw fingerprint data has changed significantly over time, starting from simpler ink-based collection techniques to the use of much more convenient and less error-prone fingerprint scanners. Although the standard techniques for fingerprint collection have changed greatly, the use of older fingerprints in newer systems is a necessity for several applied biometric systems. This is because fingerprints that were collected using older techniques must still be used in some systems, and thus it is important that the issues that are present in these collection techniques be taken into consideration.

2) Data Enhancement

Fingerprint identification, both manual and automated, depends on the quality of the image when it concerns performance5. There are many different kinds of noise that can cause issues when performing fingerprint matching. These include: rotation, displacement, distortion due to skin plasticity, variance in pressure when the print is taken, use of older fingerprint images, and differences in fingerprint collection techniques.

3) Feature Extraction

Feature extraction is the process of extracting useful features for identification and/or authentication from the biometric. This phase is tied to the process of image enhancement, and it is difficult determine where the image enhancement process ceases and the feature extraction begins. Frequency estimation deals with the task of determining the approximate frequency of the ridges in a certain region.

V. EXISTED SYSTEM

The below figure (1) shows the architecture of existed system which means fingerprint recognition system. The fingerprint recognition system can be procured either by utilizing disconnected strategies, for example, making an inked impact on paper or through a live catch gadget comprising of an optical, capacitive, ultrasound or warm sensor.

Here the unique mark picture speaks to an arrangement of situated surface and it includes basic data inside the picture. Moreover, the meaning of noise is likewise particular to fingerprints. Generally fingerprints were obtained by exchanging the inked impression onto the paper. This procedure is named as disconnected procurement. Existing verification frameworks depend on gadgets that catch the unique finger impression picture continuously. The live-scan devices can be based on one of the following sensing schemes:

(a) Optical sensors
(b) Capacitive sensors
(c) Ultra-sound sensors
(d) Thermal sensors

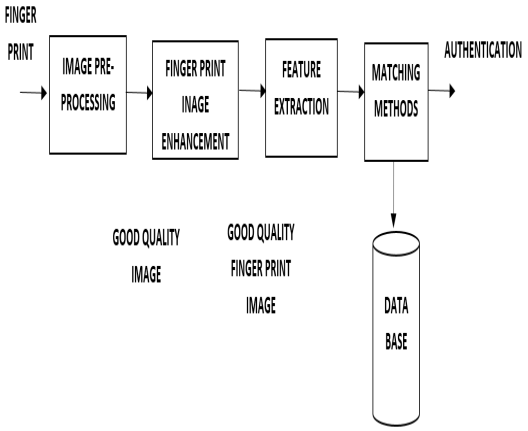

Fig.1: EXISTED SYSTEM

Optical sensors are the most seasoned and most broadly utilized in unique mark procurement innovation. In many gadgets, picture of the unique mark with dull edges and light valleys is changed over by a charged coupled gadget (CCD) into a computerized flag. Optical sensors additionally confronted another issue which is the remaining examples left by the past fingers. It has likewise been demonstrated that phony fingers can trick most poor quality business sensors. In capacitive sensors, the silicon sensor goes about as one plate of a capacitor while the finger goes about as another other plate. The capacitance between the plate and the finger depends contrarily with the separation between them. Since the edges are nearer, they identify with expanded capacitance and the valleys identify with littler capacitance. This variety is changed into an 8-bit greyscale digital picture. Because of its little size, the greater part of the electronic gadgets highlighting unique mark validation uses this type of strong state sensors.

Ultrasound innovation is conceivably the most precise unique mark detecting advancements where it uses ultrasound waves and measures the separation dependent on the impedance of the finger, the plate, and air. The sensors are prepared to do high goals of 1000 dpi or more. In any case, these sensors will in general be exceptionally enormous and contain moving parts. Warm sensors are comprised of pyro-electric materials whose properties change with temperature. These are normally made as strips. As the fingerprints are swiped over the sensor, there is differential conduction of warmth between the edges and valleys (since skin conducts warm superior to the air in the valleys) that is estimated by the sensor. Full size thermal sensors are not practical and this sensor leading to loss of signal. To overcome this issue a new system is proposed which is discussed in below section.

VI. PROPOSED SYSTEM

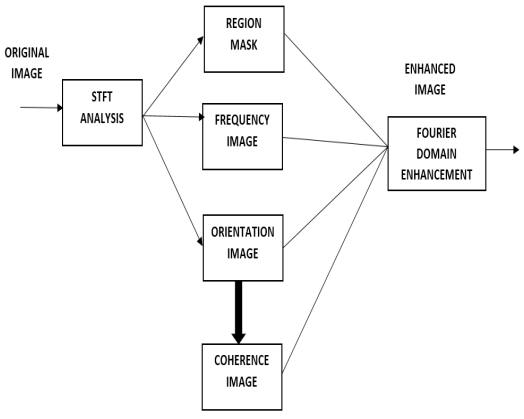

Fig.2: PROPOSED SYSTEM

The above figure (2) shows the architecture of proposed system, in this system we use STFT analysis, region mask, frequency image, coherence image and Fourier domain enhancement. The entire process depends upon the conceptual filtering in Fourier domain. The proposed system estimates the frequency information using Short Time Fourier Analysis. STFT analysis will divide an image into overlapping windows. Ridge frequency and ridge orientation will be obtained because of Fourier spectrum. This STFT analysis is also known as regions ask and it distinguishes the map between fingerprint and the background regions. So the STFT analysis will compute by ridge orientation image, ridge frequency image and also the region mask. Basically, the finger print image consists of oriented texture with non-stationary properties. This property can be resolved in both space and frequency. STFT analysis process will be performed by extending the one dimensional time-frequency analysis to two dimensional image signals.

The suitable process is obtained by utilizing the cosine window at the starting point. From figure (2) we can observe that the orientation message is computed by the coherence image. This coherence image produces angular bandwidth. Now the conceptual information will filter the each window in Fourier domain. This Fourier domain consists of two impulses. This impulse will indicate the frequency and location of the orientation wave. At last the enhancement image is obtained from the analysis of Fourier domain enhancement. So compared to existed system, the proposed system gives effective results in terms of delay and loss of signals.

VII. RESULTS

Table.1: Time executing for each stage

STAGE	ELAPSED TIME IN SECONDS
INPUT STAGE	3.69
FEATURE EXTRACTION STAGE	0.66
IDENTIFICATION	4.19
VERIFICATION	0.13
RECOGNITION	14.88
TOTAL	23.55

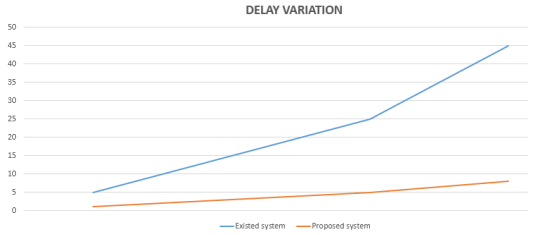

Fig.3: VARIATION OF DELAY

VIII. CONCLUSION

In this paper, proposed finger print identification system is implemented by using STFT analysis. It was capable of handling several different image types and was capable of matching fingerprints in a hierarchical manner. The storage requirements of proposed systems are likely to be much smaller and restricted. The operating speed and accuracy requirements of proposed finger print identification system are usually quite different. But compared to existed system, it produces very effective results.

IX. REFERENCES

[1] Henry C. Lee., "Advances in Fingerprint Technology," 2nd Edition. Florida: CRC Press. 2001.

[2] John Chirillo, Scott Blaul, "Implementing Biometric Security," 1st Edition, Indiana: Wiley, 2003.

[3] Davide Maltoni, Dario Maio, Anil K. Jain, Salil Prabhakar, "Handbook of

Fingerprint Recognition," 2nd Edition. New York: Springer. 2003.
[4] John D. Woodward Jr., Nicholas M. Orlans, Peter T. Higgins, "Biometrics," McGraw-Hill. 2002.
[5] Sharat S. Chikkerur, "Online Fingerprint Verification System," Thesis, State University of New York at Buffalo, June 2005.
[6] Ruud Bolle, Jonathan Connell, Sharanthchandra Pankanti, Nalini Ratha, Andrew Senior, "Guide to Biometrics," 1st Edition, New York: Springer, 2003.
[7] Gary W. Jones, "Introduction to Fingerprint Comparison," Staggs Pub, 2000.
[8] James Wayman, Anil Jain, Davide Maltoni, Dario Maio, "Biometric Systems: Technology, Design and Performance Evaluation," 1st Edition, New York: Springer, 2004.
[9] T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino, "Impact of artificial gummy fingers on fingerprint systems," Proceedings of SPIE, Optical Security and Counterfeit Deterrence Techniques IV, Vol. 8577, 2002.
[10] M.Tartagni and R. Guerrieri, "A Fingerprint Sensor Based on the Feedback Capacitive Sensing Scheme," IEEE Journal of Solid-State Circuits, Vol. 33, No. 1, January 1998.
[11] S. Pankanti, S. Prabhakar, and A. K. Jain, "On the individuality of fingerprints," Transactions on PAMI, 24(8):1010–1025, 2002.
[12] John K. Schneider, "Ultrasonic Fingerprint Sensors," Advances in Biometrics, Springer London, pp 63-74, 2008.
[13] H. Han and Y. Koshimoto, "Characteristics of thermal-type fingerprint sensor," Proceedings of SPIE, Vol. 6944, 2008.
[14] Samir Nanavati, Michael Thieme, Raj Nanavati, "Biometrics: Identity Verification in a Networked World," Indiana: Wiley, 2002.
[15] Bir Bhanu, Xuejun Tan, "Computational Algorithms for Fingerprint Recognition," 1st Edition. New York: Springer, 2001.

PRATAP KUMAR DEVARAPALLI completed his B.Tech in Chirala Engineering College and M.Tech in Bapatla Engineering College. At present he is working as Assistant Professor, in St. Mary's Women's Engineering College, Guntur Dt, AP,INDIA.

VEERA PUNNAIAH MANDA completed his B.Tech in D.M.S.S.V.H college of Engineering in 2011 and M.Tech Gudlavalleru Engineering College in 2013. At present he is working as Assistant Professor, in Gudlavalleru Engineering College, Gudlavalleru, Krishna Dt, AP, INDIA.