Fingerprint Recognistion Using Image Processing

Satyanarayana[1], Tumoju Ramyasree[2], Kumbam Akhila[3]
[1]*Asst. Professor, Dept. of Computer Science and Engineering, SNIST, Hyderabad-501301, India*
[2,3,4]*B. TECH Scholars, Dept. of Computer Science and Engineering Hyderabad-501301, India*

Abstract: Fingerprint based recognition systems have been widely deployed in numerous civilian and government applications. However, fingerprint based biometric systems are vulnerable to spoofing attacks. To protect against spoofing, methods of liveness detection measure physiological signs of life from fingerprints, ensuring that only live fingers are captured for enrolment or authentication. In this project, propose a novel image descriptor for fingerprint live-ness detect -ion using the local coherence of a given image. The key idea of the proposed method is that the difference between live and fake fingerprints is well revealed by the directional coherence in the gradient field. More specifically, the replica fabrication process is highly likely to yield dispersion of gradient distributions in a fake fingerprint image due to loss of information by the acquisition noise and blurring artifacts. Therefore, propose to exploit the local patterns of the directional coherence as our features, the so-called local coherence pattern (LCP). As compared to previous approaches, the proposed method efficiently describes the Under -lying structure of ridges and valleys (i.e., directional structure) in the fingerprint image and thus successfully captures the slight difference of textural characteristics between live and fake fingerprints even under noisy environment The experimental results on various datasets demonstrate that the proposed method efficiently improves the performance of fingerprint live-ness detection.

Key Words: live ness, Real, Fake, Logical Regression, Fingerprint validation.

INTRODUCTION

Biometrics based personal identification is getting wide acceptance within the networked society, replacing passwords and keys thanks to its reliability, uniqueness and therefore the ever increasing demand of security. Common modalities getting used are fingerprint and face except for face authentication people are still working with the matter of pose and illumination in variance whereas fingerprint doesn't have a decent psychological effect on the user thanks to its wide use in crime investigations. If any biometric modality is to reach the longer term it should have the traits like uniqueness, accuracy, richness, simple acquisition, reliability and particularly user acceptance. Fingerprint based personal identification could be a new biometric modality which is getting wide acceptance and has all the required traits to create it part of our lifestyle. This paper investigates the employment of fingerprint for private identification using combination of various wavelets. Fingerprint not only has the unique information available as on the fingerprint but has much more amount of details in terms of principal lines, wrinkles and creases. Moreover, it can easily be combined with hand shaped biometrics and so on form a highly accurate and reliable biometric-based personal identification system. Besides, since fingerprint features are used officially in criminal investigations and commercial transactions, most of the users are unwilling to deliver their fingerprint data to a corporation or system for privacy reason. During this paper, we propose a fingerprint-based technology to spot the individuals within the entry control systems. Extracted hand shape features to verify the non-public identity. captured a picture of finger by employing a CCD camera to come up with the wide line integrated profile (WLIP) of length 472. Introduced an advertisement product of hand geometry-based recognition and applied it to several access control systems. features extracted from the inked paper. it's not suitable for several on-line security systems because two steps are needed to get the finger-print images in their approach. during this paper, we propose a scanner-based personal authentication system by using the fingerprint features. Two stages, enrolment and verification stages, constitute the identification system. within the enrolment stage, M hand images of a personal are collected to be the training samples. These samples should be processed by the prepossessing, feature extraction, and modeling modules to get the matching templates. within the verification stage, a question sample is additionally

processed by the prepossessing and have extraction modules, then be matched with the templates.

LITERATURE SURVERY

Time-series detection of perspiration as a liveness test in fingerprint devices. Author: S. T.VParthasaradhi Year of publishing: 2005 Biometrics can play a vital role in enhancing security systems and is under consideration for dramatically increased use in order to minimize security threats in military organizations, government centers, and public places like airports. Bio-metrics systems use physiological or behavioral characteristics to automatically determine or verify the identity of a person. Examples of biometric technologies include fingerprint, facial, iris, hand geometry, voice, and keystroke recognition. As with all security measures, a biometric system is subject to various threats like attacks at the sensor level, replay attacks on the data communication stream and attacks on the database. This paper will focus on countermeasures to attacks at the sensor level of fingerprint influencing our public movement. Fake news area is a rising investigation district which is getting interest with the resources available.

In this paper we have displayed an acknowledgement model for fake news using logical regression methodologies. In the last decade, Fake News phenomenon has experienced a very significant spread, favored by social networks. This fake news can be broad casted for different purposes. Hence there is a requirement of a technology where the human being can understand and react to such fake news. Hence the fake news biometric systems or spoofing, the process of defeating a biometric system through an introduction of a fake biometric sample or, worst case, a dismembered finger. Liveness detection, i.e. to determine whether the introduced biometric is coming from a live source, has been suggested as a means to circumvent attacks that use spoof fingers. 2. A computational approach to edge detection Author: J.Canny Year of publishing: 2009 This paper describes a computational approach to edge detection. The success of the approach depends on the definition of a comprehensive set of goals for the computation of edge points. These goals must be precise enough to delimit the desired behavior of the detector while making minimal assumptions about the form of the solution. We define detection and localization criteria for a class of edges, and present mathematical forms for these criteria as functional s on the operator impulse response. A third criterion is then added to ensure that the detector has only one response to a single edge. We use the criteria in numerical optimization to derive detectors for several common image features, including step edges. On specializing the analysis to step edges, we find that there is a natural uncertainty principle between detection and localization performance, which are the two main goals. With this principle we derive a single operator shape which is optimal at any scale. The optimal detector has a simple approximate implementation in which edges are marked at maxima in gradient magnitude of a Gaussian-smoothed image. We extend this simple detector using operators of several widths to cope with different signal to noise ratios in the image. We present a general method, called feature synthesis, for the fine to coarse integration of information from operators at different scales. Finally, we show that step edge detector performance improves considerably as the operator point spread function is extended along the edge.

PROPOSED METHOD

In this project, propose a novel image descriptor for detecting the fingerprint liveness. The key idea of the proposed method is that the difference between live and fake fingerprints is well revealed by the directional coherence in the gradient field. More specifically, the replica fabrication process is highly likely to yield dispersion of gradient distributions in a fake fingerprint image due to loss of information by the acquisition noise and blurring artifacts. Therefore, propose to exploit the local patterns of the directional coherence as our features, the so-called local coherence pattern intensity-gradient distribution which brings a significant increase of the discriminate power to determine whether a given fingerprint is fake or not. In the following, need to find the dominant orientation and its coherence based on the intensity-gradient distribution defined. To this end, propose to adopt the singular value decomposition (SVD) since it decomposes the given distribution into independent axes with the corresponding energy. Therefore, the dominant orientation and its energy in the intensity-gradient distribution can be efficiently estimated by computing SVD of coherence and then construct local patterns. Feature of LCP is the feature vector for the given fingerprint image, which is fed into the linear SVM classifier for training and test to

determine whether a given fingerprint is fake or not. The experimental results on various datasets demonstrate that the proposed method efficiently improves the performance of fingerprint liveness detection.

ANALYSIS

The current and arranged the technology calculated model and methods for creating the frameworks for the investigators to a data framework that accompany in the exercises such as:

1 plan
2 Execution
3 Testing
4 Sending
5 Activities 6 Result

Levels of emotionalintensity (normal, strong), with an additional neutral expression. the above is used for life cycle of development of system that brings an excellent framework that meets client assumptions and inside time and cost assessments and works very productively in the system.

SOFTWARE REQUIREMENTS

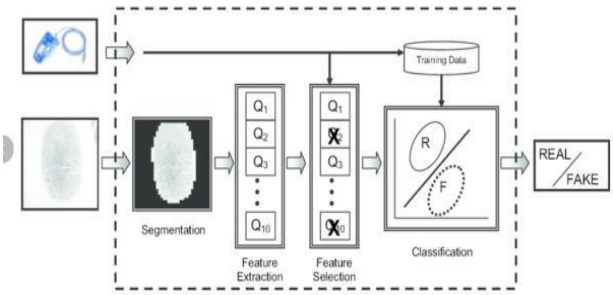
The equipment's will work on the laptop or the system, the working system will be the basic and straightforward and the controls which permit the client and the application will be clear and it will infer the usefulness inside the application and the connection point is that it will take inputs just as two illustrations and gives the output. The software requirements are:

Operating System: Windows XP Simulation Tool: MatlabR2010

HARDWARE REQUIREMENTS

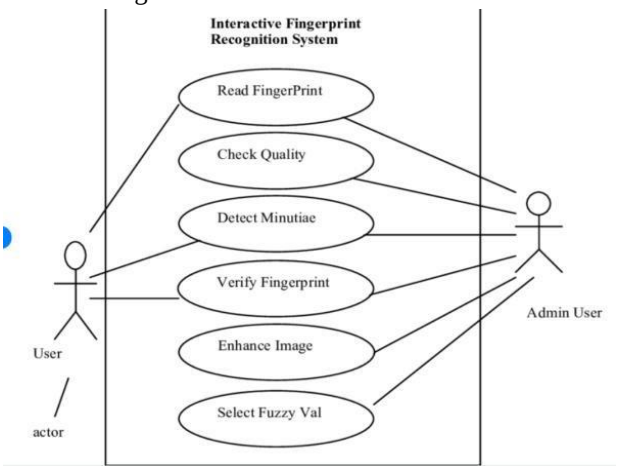
Processor: Intel Pentium D
Mother Board: Intel 945G Express Chipset
Bus Speed: 2.80 GHZ
RAM: 2 GB
Hard disk: 20 GB or more
Monitor: 17 “inch CRT (IBM)
Keyboard: 104 Keys
Mouse: Lenovo PS/2 3 buttons CD-ROM: LITE-ON CD-ROM

SYSTEM DESIGN

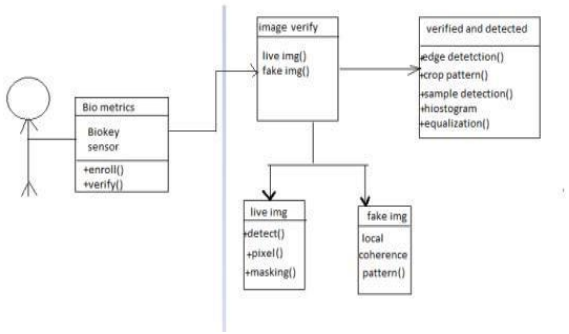


UML DIAGRAMS

Use case diagram:



Class diagram:



ALGORITHM

Input: Training data set T, F= (f1, f2, f3,..., fn) // value of the predictor variable in testing data set
Output: A class of testing data set.

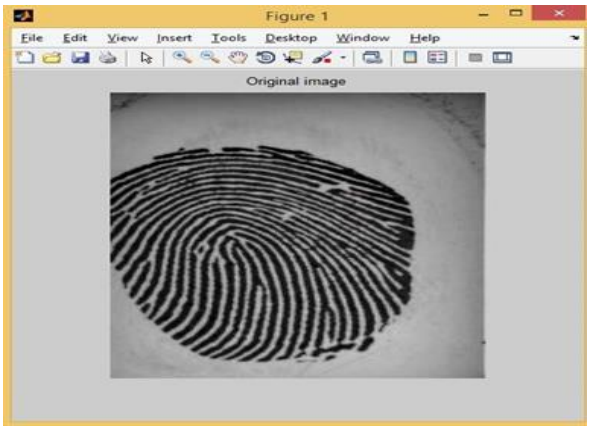
1. Import the data set
2.Explore the data to figure out what they look like
3.Preprocess the data

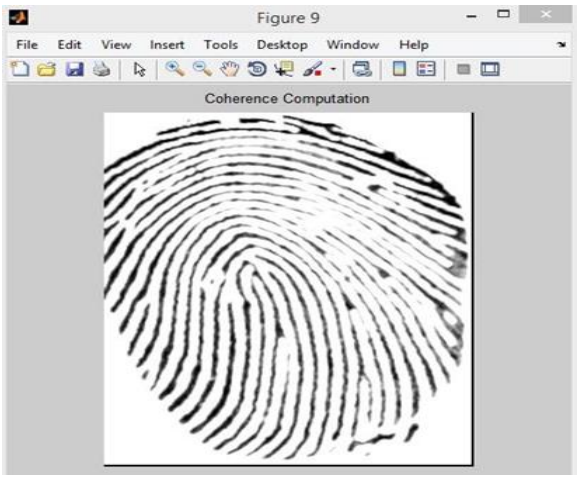
4.Split the data into attributes and labels
5.Divide the data into training and testing sets
6.Train the logistic regression
7.Make some predictions
8.Evaluate the results of the algorithm

Data prepossessing: It is technique in machine learning which is used to clean the data. The aim of prepossessing is to remove noise from the data set. By removing unnecessary features from our text, we can reduce complexity and increase predictability. Removing punctuation, special characters, and 'filler' words (the, a, etc.) does not drastically change the meaning of a text. A real-world data cannot be directly used for machine models because it may be contain noise, missing values, redound and consistent. Data prepossessing increases the accuracy and efficiency of a machine learning which required tasks for cleaning the data and making it suitable for a machine learning model.

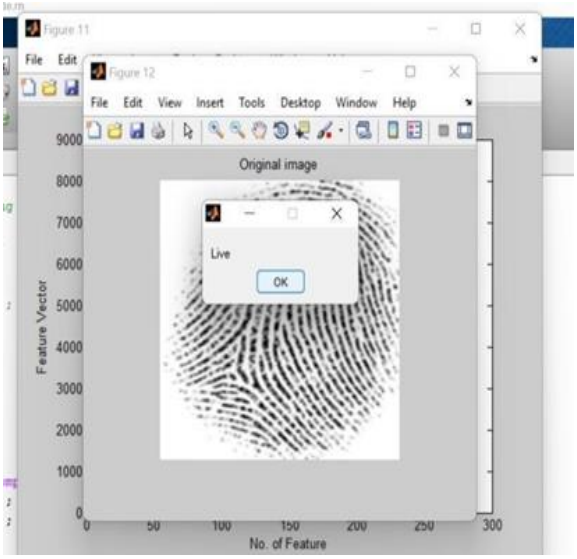
RESULT

The evaluation experimental protocol has been designed with a two-fold objective: First, evaluate the "multi-biometric" dimension of the protection method. That is, its ability to achieve a good performance, compared to other trait specific approaches, under different biometric modalities. For this purpose three of the most extended image based biometric modalities have been considered in the experiments: fingerprint and 2D face. Second, evaluate the "multiattack" dimension of the protection method. That is, its ability to detect not only spoofing attacks (such as other liveness detection specific approaches) but also fraudulent access attempts carried out with synthetic or reconstructed samples input image:
Contrast Enhancement:

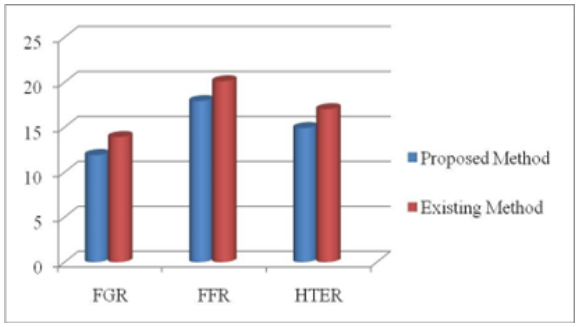




OUTPUT



PREDICTIVE SYSTEM



If the predictive output is 0 then it is real else it is fake

CONCLUSION

A simple and novel local descriptor for fingerprint liveness detection has been proposed in this project.

Our key observation is that the fabrication process mostly makes the dispersion of the directional structures in the fingerprint image (i.e., ridge and valley). Therefore, we propose to exploit the local patterns of the coherence along the dominant orientation in the intensity-gradient distribution of the given fingerprint image. Based on various experiments, we can confirm that the proposed method has an ability to provide a reliable performance for fingerprint liveness detection