ISSN No. 0976-5697

Volume 7, No. 3, May-June 2016

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Novel Approach For Precise Fingerprint Detection

Meenakshi
Research Scholar (M. Tech)
Department of Computer Science and Applications
Kurukshetra University, Kurukshetra, INDIA

Dr. Chander Kant
Assistant Professor
Department of Computer Science and Applications
Kurukshetra University, Kurukshetra, INDIA

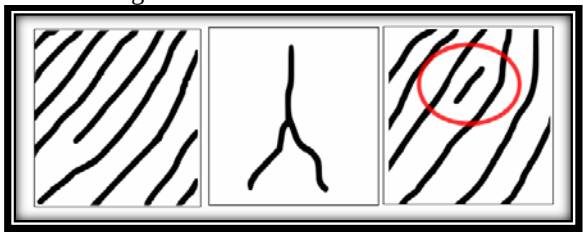
Abstract: Fingerprint recognition is very stable, reliable, and oldest biometric authentication technology that has been widely used in various civilian and government applications. Like other authentication technologies, fingerprint recognition is not totally free from spoofing. A fingerprint recognition system can be spoofed by placing artificially generated fingerprints of enrolled user at the sensor that are made up of materials like gelatine, silicon, wax or play-doh etc. Liveness detection is a technique to enhance the security of such systems by detecting physiological life signs in fingerprint samples to differentiate a real fingerprint from an artificial one. A live fingerprint image has the property to produce gray level variations along ridges due to presence of sweat pores, perspiration and skin quality (dry, wet) whereas a fake fingerprint has uniform gray levels that can give a fair idea about the liveness in input sample. In the proposed work, two fingerprints are captured by scanner at different time points (0 sec and 2 sec). In order to find their gray level variations, a gray level co-occurrence matrix of each fingerprint image is determined. After that, contrast value is computed from each matrix. If the difference in their contrast value is greater than threshold, then the input fingerprint sample is considered as live otherwise it is considered as fake. Liveness detection solution presented in this work helps to avoid direct attacks at fingerprint sensor that result in very secure and precise fingerprint detection.

Keywords: Biometrics, Fingerprint detection, Liveness Detection, Spoofing

I. INTRODUCTION

Biometrics is a modern authentication technology that identifies or verifies a person on the basis of his physiological (fingerprint, face, iris etc) or behavioral traits (voice, signature, gait etc). These traits are also known as biometric modalities, biometric technologies or biometric characteristics. Biometrics is most secure form of authentication because unlike traditional methods of security (token based: ID cards and knowledge based methods: passwords) it can't be lost, forgotten or shared. [1]

Fingerprint recognition is very stable, reliable and oldest biometric authentication technology that has been widely used in various civilian and government applications. Fingerprint recognition is an automated method of verifying a match between two human fingerprints. Fingerprints are unique and absolute for each individual; even the fingerprints of identical twins are different from each other. The basic characteristic of fingerprint is that they do not change over time. The matching accuracy of fingerprint is very high. In the Fingerprint Recognition process, [2] firstly an image of person's fingertip is taken and then its unique biometric characteristics like whorls, arches, and loops along with the patterns of ridges, furrows, and minutiae points are recorded. The most common method involves recording and comparing fingerprint's "minutiae points" i.e. minutiae based matching. The major Minutia points in fingerprint are: ridge ending, bifurcation, and short ridge or dot as shown in Fig. 1 below:



(a)Ridges Ending (b) Ridges Bifurcation (c) Dot

Figure 1. Minutiae Points in Fingerprints [3]

A fingerprint recognition system works in two phases:

- Enrollment Phase
- Recognition Phase

In the Enrollment phase, first of all sensor scans the fingerprint of user and then the minutiae point extractor extracts the minutiae points from image and finally, minutiae information along with the user demographic information is stored as a template in database.

In the Recognition phase, sensor generates the fingerprint image of user called as a query image. Minutiae extractor extracts the minutiae points from query image and then matcher module compares the minutiae points of query image with the stored minutiae template(s) in database. After that, a match score is generated by the system and system determines the person's identity by comparing the obtained match score with the threshold value. The basic block diagram of the fingerprint recognition system is shown in Fig. 2 below:

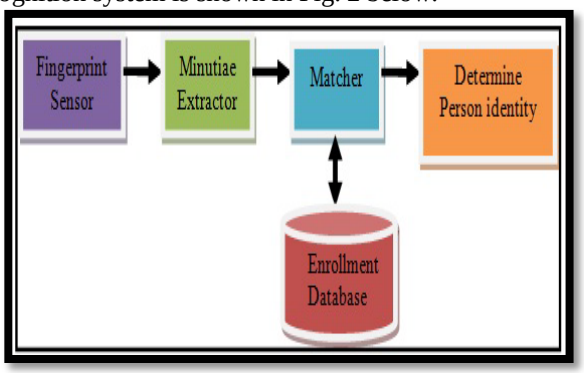


Figure 2. Block Diagram of Fingerprint Recognition System

Fingerprint recognition is also prone to the spoofing attacks. Most common attacks are the direct attacks or sensor attacks. These attacks consist of presenting [4] an artificially generated fingerprint to the sensor and hence system can be

accessed. Some of the possible sensor attacks are as given below:

A. The Registered Finger (Legitimate Finger)

In this attack, fingerprint of a registered user is stolen that can be used by casting into moulds. Registered user can also be forced to present his finger directly or indirectly at the sensor.

B. The Unregistered Finger(Imposter Finger)

In this attack, the intruder uses his own finger to try to log in as a valid user.

C. By Using Genetic Clone Of Finger

In this attack, the genetic clone of the registered or legitimate user is presented in front of the sensor to fool the system because fingerprint of identical twins are quite similar with each other.

D. Artificial fingerprints

In this attack, artificial fingerprints of the user can be generated by using materials like silicon, gelatin, clay etc. The attacker make fake fingerprints either by direct methods i.e. moulds or by collecting the latent fingerprints of the legitimate user.

To minimize such spoofing attacks, liveness detection technique is integrated within the system. It is used to prevent the sensor attacks. [3] The proposed approach makes use of gray level variations along ridges that are caused by sweat pores, perspiration and skin quality (dry, wet) to detect liveness. The gray level values and their variations are computed by generating gray level co occurrence matrix and then computing contrast.

This paper is organized as follows, section II introduces the fingerprint liveness detection, section III gives related work regarding fingerprint liveness detection, section IV describes the proposed work and the and the corresponding results are shown in the section V, Interpretation of results is done in section VI and then Comparison of proposed work with existing techniques is done in section VII and finally in the section VIII, conclusion and future scope of work is explained.

II. FINGERPRINT LIVENESS DETECTION

Fingerprint liveness detection ensures that the input fingerprint is provided by a live user and is not generated by artificial means. There are two types of liveness detection methods: hardware based methods and software based methods. [5]

A. Hardware Based Methods

These methods detect liveness signs in fingerprint by using an extra hardware at the sensor. Liveness signs such as temperature of fingerprint, pulse oximetry, blood pressure, resistance and skin odor can be detected by hardware means.

B. Software Based Methods

Software based methods are frequently used methods for liveness detection because they are cheaper solution than hardware methods and also very flexible.

Various software based liveness detection methods are as given below:

- Perspiration Based Methods that are based on change in fingerprint patterns due to the presence of sweat pores. Fake fingerprint cannot possess such properties.
- Skin Deformation Based Methods that are based on the skin elasticity property of a live finger. The deformation produced by live finger is higher than the fake fingers.
- Image Quality Based Methods that are based on image quality difference between live and fake images. Different quality measures are extracted from fingerprint image such as ridge strength, ridge continuity, ridge clarity etc
- Pore Based Methods that detect the active sweat [5] pores in the input fingerprint image to check liveness.

III. RELATED WORK

P. Reddy, Ajay Kumar et al. [6] proposed a method that was based on pulse oximetry principle to detect liveness in fingerprint. It monitors the oxygenation of human hemoglobin. They also used heart pulse as another sign of fingerprint liveness. This was a cost effective hardware solution.

R. Notzel, W. Funk and M. Drahansky [7] proposed a method that was based on the fine movements of fingerprint surface by analyzing the changes in volume of finger (expansion and contraction of fingerprint papillary lines) but this method required an extra hardware.

Parthasaradhi, Derakhshani et al. [8] proposed a method that was based on change in fingerprint pattern of images due to perspiration. Fingerprints were captured at 0 second and 5 second. Ridge signal was extracted using a ridge signal algorithm.

A. Antonelli, R. Cappelli et al. [9] proposed a fingerprint liveness detection method that was based on skin elasticity. This method was based on the fact that deformation caused by the live finger is higher than the fake finger. EER of this method was 4.9%.

A. Abhyankar and S. Schuckers [10] developed a liveness detection method that was based on the texture pattern in the fingerprint image. Various first order and second order statistic features such as energy, entropy, median, variance etc were extracted to determine the nature of finger.

M. Espinoza and C. Champod [11] proposed a method that was based on pore detection in fingerprint images as a liveness clue because live fingers produce pores in a different manner than the fake fingers. The pore quantity of the query images was compared with the recorded ones.

B. Tan and S. Schuckers [12] combined ridge signal algorithm and valley noise analysis to detect the perspiration pattern in the fingerprint image. A real finger produces less noise and more gray level variations than a fake finger that was used as a liveness clue.

IV. PROPOSED WORK

A. Liveness Detection In Proposed Approach

To detect liveness in fingerprint images, the proposed approach takes advantages of the following properties of a live finger:

- When a live finger is placed on the sensor, then there will be a slight change in the obtained fingerprints that are taken in a short time span. The reason for this change is the moisture produced by our sweat glands of finger.
- Due to the presence of sweat pores, perspiration and skin quality (dry, wet), live fingerprints produce non uniform gray levels along the ridges. Hence there will be a gray level change in the two sequential images of live finger. The surface of spoof fingers (made up of

gelatin or silicon) cannot produce such characteristics due to the absence of perspiration phenomenon. They have uniform grey levels along the ridges.

B. Gray Level Co-Occurrence Matrix

The proposed approach makes use of Gray level Co occurrence Matrix (GLCM) to compute the gray level variations in the input fingerprints. GLCM is a matrix that calculates how often a pixel with gray level value i occurs horizontally adjacent to a pixel with value j. The gray level co-occurrence matrix can reveal various properties regarding spatial distribution of gray levels in texture image.

To create a GLCM matrix, MATLAB function graycomatrix ( ) is used. After creating GLCM, various statistical measures can be derived such as contrast, correlation, energy and homogeneity. For this purpose, MATLAB function graycoprops ( ) is used. Here in the proposed approach, we will compute contrast value from the GLCM matrix to check the gray level variations in the sequential images of input finger. Live finger images will produce a high contrast difference while fake finger images will produce very small contrast difference or sometimes even zero. Hence liveness of the input finger can be determined by comparing the contrast difference with threshold value. Histogram of fingerprint images are also plotted to show the grey level variations graphically. Live finger images will produce large difference in their histogram distributions as compared to the fake ones.

C. Proposed System Architecture

Proposed system works in two phases: Enrollment Phase and Recognition Phase

1) Enrollment Phase

It is the process of registering a new user in the database by collecting and processing his biometric samples and then storing them along with user demographic information as a biometric template. Proposed approach makes sure that only live fingerprint samples will be enrolled in the database and the fake samples are automatically rejected. If the proposed liveness test is passed, only then the user will be enrolled otherwise it is rejected as shown in Fig. 3 below:

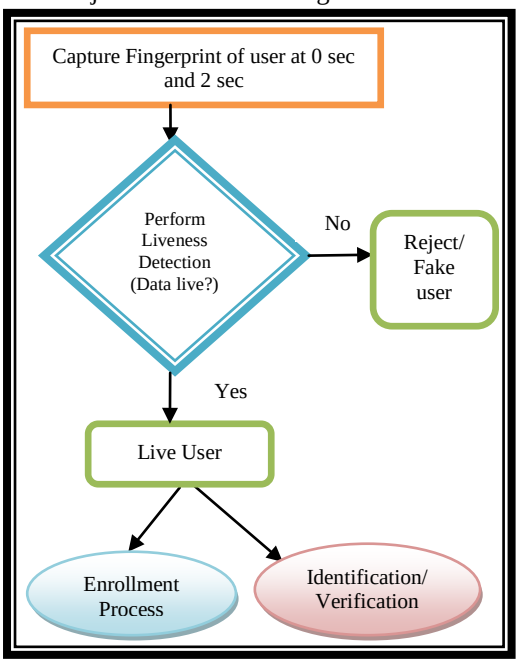


Figure 3. Basic Architecture of Liveness Detection in Enrollment and Recognition Phase

2) Recognition Phase

Fingerprint recognition refers to identification or verification of an individual by comparing their unique fingerprint characteristics. First of all, input finger images are tested for liveness by the liveness module. If the liveness test is passed, only then fingerprint recognition (feature extraction, matching) process is carried out, otherwise user is declared as "Fake" and recognition steps are not performed for such user as shown in Fig. 3. Hence performance of the system is improved. Basic Flow chart of proposed approach is given in the Fig. 4 of the next subsection below:

D. Basic Flow Chart Of Proposed Approach

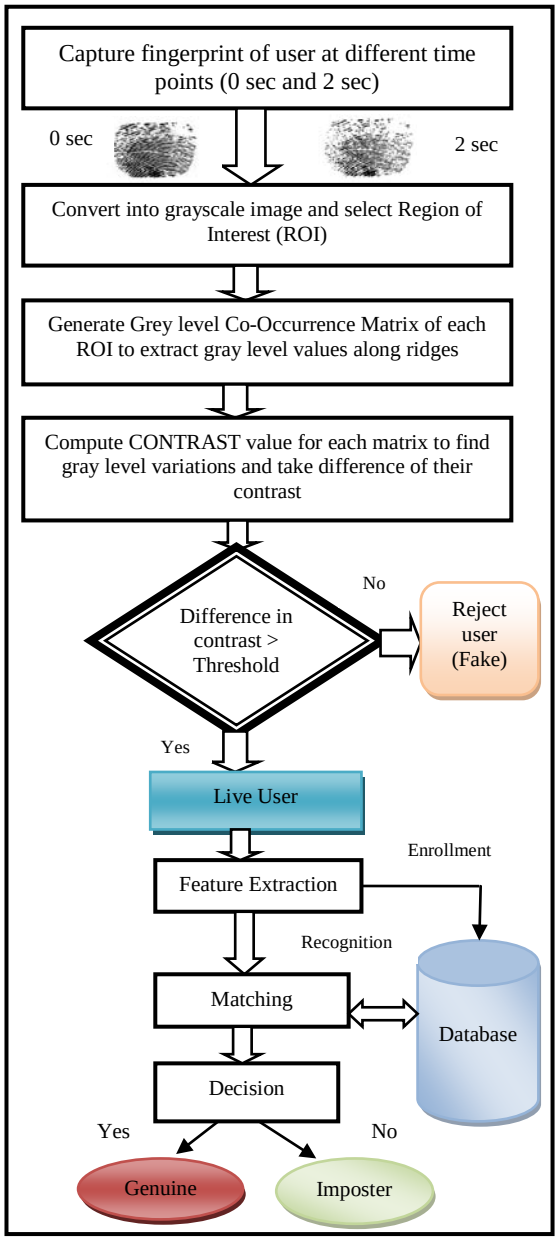


Figure 4. Flow Chart of Proposed Approach

E. Proposed Algorithm

1. Capture two fingerprints at different time points (0 sec and 2 sec) by scanner.
2. Now convert each fingerprint image into grayscale image and select Region of Interest (ROI) from each image.
3. Now Generate Gray Level Co-Occurrence Matrix (GLCM) from the selected region (ROI) of each image.

4. Compute CONTRAST from each matrix to find the gray level variations by Using MATLAB function graycoprops (). CONTRAST is a feature that Measures the local variations in the gray levels of co-occurrence matrix and is computed mathematically as given in equation 1:

$$\text{Contrast}=\sum_{i,j}|i-j|^2 P(i,j) \quad \ldots\ldots\ldots\ldots (1)$$

5. **IF (DIFFERENCE IN CONTRAST>TH1 {THERSHOLD1}) THEN**
6. User is 'LIVE".
7. **IF (User == "NEW USER") THEN** // GO TO ENROLLMENT PHASE
8. Perform feature extraction i.e. extract minutiae points.
9. Generate Template.
10. Store template in Database.
11. **ELSE** // GO TO RECOGNITION PHASE
12. Perform feature extraction i.e. extract minutiae points.
13. Match the extracted minutiae points with the corresponding template in database.
14. **IF (Match Score>TH2 {threshold2}) THEN**
15. User is "Genuine".
16. **ELSE**
17 User is "Not Genuine"
18 END IF

END IF

19. **ELSE**
20. User is "NOT LIVE"
21. Reject.
22. END IF
23. **EXIT**

F. Matlab code to Find Gray Level Variations

```
%Program Description
%This program finds the gray level variations
from fingerprints captured at 0 sec and 2 sec
% capture fingerprint samples at 0 sec and 2 sec
I1=input ('Capture fingerprint image at 0 sec');
q1 = imread (I1);
I2=input ('Capture fingerprint image at 2 sec');
q2= imread (I2);
% convert into grayscale images
w1 = rgb2gray (q1);
w2 = rgb2gray (q2);
% set a predefined threshold value
Threshold=input ('Enter threshold Value');
%Select an interesting square area or
% REGION OF INTEREST
i1=imcrop (w1,[11.5 7.5 288 184]);
i2=imcrop (w2,[11.5 7.5 288 184]);
figure; imshow(i1);title(' fingerprint at 0 sec')
figure; imshow(i2);title(' fingerprint at 2 sec')
%Generate gray level co occurrence matrix1
l1 = graycomatrix (i1);
disp ('image 1 co occurrence matrix')
disp (l1)
% finds gray level variations by finding contrast value from matrix1
Contrast1=graycoprops (l1, {'contrast'})
%Generate gray level co occurrence matrix2
l2 = graycomatrix (i2);
disp(' image 2 co occurrence matrix')
disp(l2)
%find gray level variations by finding contrast value from matrix2
Contrast2=graycoprops (l2,{'contrast'})
%finding gray level variations
Difference=Contrast2.Contrast- Contrast1.Contrast;
% checking the liveness of user
if(Difference >Threshold)
   disp ('Live User');
else
   disp ('Fake user');
end
 % generate histogram of each image
figure; imhist (i1); title('histogram of fingerprint sample at 0 sec' );
figure; imhist (i2);title('histogram of fingerprint sample at  2 sec');
```

V. EXPERIMENTAL RESULTS

Table 1 shows the contrast values that are obtained for both live samples and fake samples taken at different time points. These values are computed mathematically (with the help of MATLAB) from gray level co occurrence matrix and then compared with the threshold value and finally the result is obtained as live or fake as given in Table 1 below:

Table I: Computation of contrast values for both live images and fake images (0 sec and 2 sec) and the obtained result

Input image	*Contrast1*	*Contrast2*	*Difference in contrast >threshold*	*Result*
	For 0 sec image	*For 2 sec image*		
Real	0.5911	0.7279	Yes	Live
Spoof	1.074	1.074	No	Fake

The gray level variations can also be seen graphically by drawing the histograms of both live samples and fake samples (at 0 sec and 2 sec).

Fig 5 and Fig. 7 shows the ROI regions of live and fake fingerprints taken at 0 sec and 2 sec respectively and their corresponding histograms are shown in Fig 6 and Fig 8 respectively.

A. For Live User

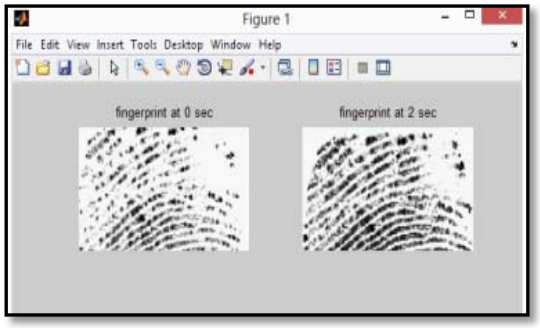
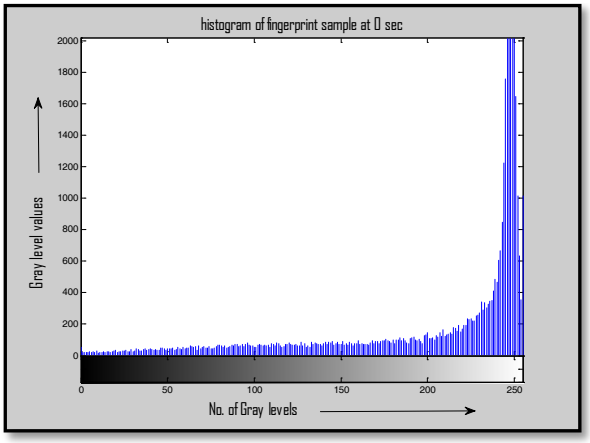
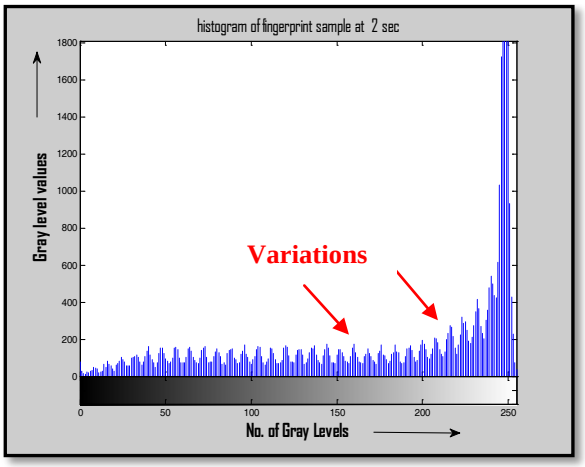


Figure 5: Live fingerprint image at i) 0 sec ii) 2 sec



(a)



(b)

Figure 6. Histogram distribution of live finger (a) at 0 sec and (b) 2 sec

B. For Fake User

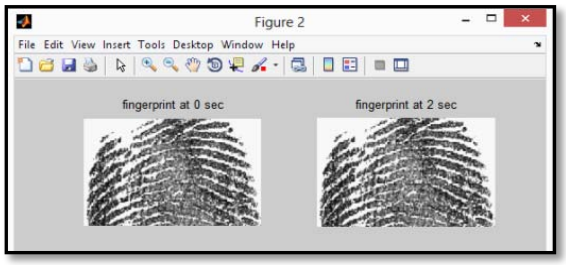
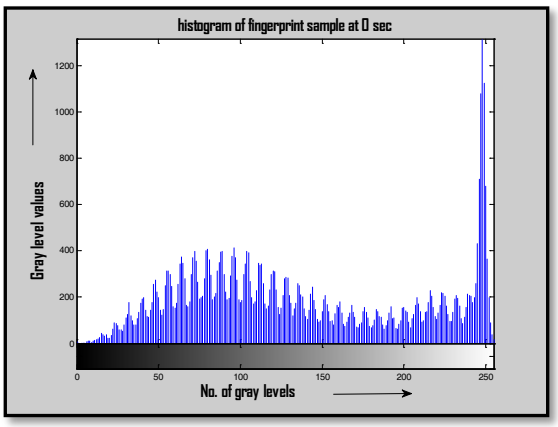
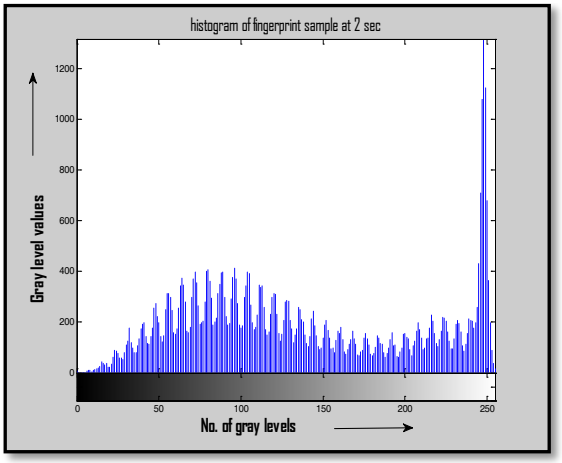


Figure 7. Fake fingerprint image at i) 0 sec and ii) 2 sec



(a)



(b)

Figure 8. Histogram distribution of fake finger (a) at 0 sec and (b) 2 sec

VI. INTERPRETATION OF RESULTS

As illustrated in the histograms of live and fake user shown above in Fig 6 and Fig. 8 respectively, there is a considerable difference in histograms for live user due to the presence of gray level variations whereas there is no visible difference in the histograms for fake user. Also, the contrast values computed for live sequential images have shown higher contrast difference than the fake sequential images. (See Table I). This difference so obtained mathematically (in terms of contrast) and graphically (in terms of histograms) is very useful for differentiating between a live user and fake user and finally helps in attaining a very secure and precise fingerprint detection.

VII. COMPARISON OF PROPOSED APPROACH WITH EXISTING TECHNIQUES

Proposed scheme has many advantages than the existing techniques as given below:

- A live image has different texture features than a fake image. The proposed scheme detects the gray level variations by extracting textural features of image with the help of co-occurrence matrix which is a simple but powerful scheme for Liveness detection.
- The proposed approach uses software method to detect liveness. We don't need to add an extra hardware at sensor hence the overall cost of system is not increased i.e. a cost effective solution. Also, there is no need of large computations i.e. fast method.
- Liveness detection in the proposed scheme is used to avoid direct attacks (at the sensor) thereby enhancing the level of security in fingerprint biometric systems and also improves the performance by integrating itself just before the recognition module.
- In the proposed scheme, Fingerprints are captured at time point (0 sec and 2 sec) instead of (0 sec and 5 sec) which is more convenient to the user because he does not need to press his finger for a longer duration on the sensor.

VIII. CONCLUSION & FUTURE SCOPE

Fingerprint detection is a reliable biometric technology but it is not totally free from spoofing attacks. A novel software based Liveness detection approach is proposed to avoid direct

attacks at fingerprint sensor that results in very secure and precise fingerprint detection. Proposed Scheme detects liveness by checking the gray level variations in the sequential images of input finger, which is a simple but very powerful technique. The proposed method is also cost effective because it does not need extra hardware and large computational resources. In future, this method can be tested on larger datasets with different image quality.

IX. REFERENCES

[1] Anil Jain, Lin Hong, and Sharath Pankanti, "Biometric Identification," in *Communications of ACM*, vol. 43, 2000.

[2] Anil K. Jain, Jianjiang Feng, and Karthik Nandakumar, "Fingerprint Matching," *Computer journal,IEEE Computer Society Press*, vol. 43, no. 2, pp. 36-44, February 2010.

[3] Chander Kant Verma, "Efficiency and Security Optimization for Fingerprint Biometric System," 2009.

[4] Sonal Girdhar and Dr. Chander Kant, "A Novel Approach for Detecting Fingerprint Liveness," *IJIACS*, vol. 4, no. 6, pp. 10-16, June 2015.

[5] Al-Ajlan and Amani, "Survey on fingerprint liveness detection," in *International Workshop on Biometrics and Forensics (IWBF)*, 2013, pp. 1-5.

[6] P. Reddy, Ajay Kumar, S. M. K. Rahman, and Tanvir Singh Mundra, "A New Antispoofing Approach for Biometric Devices," in *IEEE Transactions on Biomedical Circuits and Systems*, vol. 2 Issue 4, 2008, pp. 328-337.

[7] R. Notzel, W. Funk M. Drahansky, "Liveness Detection based on Fine Movements of the Fingertip Surface," in *IEEE Information Assurance Workshop*, Newyork, 2006, pp. 42-47.

[8] Parthasaradhi, Sujan TV, Derakhshani, and Lawrence, "Time-series detection of perspiration as a liveness test in fingerprint devices," in *Systems, Man, and Cybernetics, Part C: Applications and Reviews*, vol. 3, 2005, pp. 335-343.

[9] A. Antonelli, R. Cappelli, Dario Maio, and Davide Maltoni, *A New Approach to Fake Finger Detection Based on Skin Distortion*.: Springer Berlin Heidelberg, vol. 3832.

[10] A. Abhyankar and S. Schuckers, "Fingerprint Liveness Detection using Local Ridge frequencies and multiresolution texture analysis techniques," in *IEEE international conference on image processing*, 2006, pp. 321-324.

[11] M. Espinoza and C. Champod, "Using the number of pores on fingerprint images to detect spoofing attacks," in *International conference on Hand based biometrics*, 2011, pp. 1-5.

[12] B. Tan and S. Schuckers, "Spoofing Protection for Fingerprint Scanner by Fusing Ridge Signal and Valley Noise," *Pattern Recognition*, vol. 43, no. 8, pp. 2845-2857, august 2010.