Biometric Fingerprint Spoof Identification Using Neural Networks

Ajimol C
M.phil Scholar, Nanjil Catholic College of Arts and Science, Kaliakkavilai, Tamil Nadu, India.

Dr.R.Kavitha Jaba Malar
Assistant Professor, Department of Computer Science, Nanjil Catholic College of Arts and Science, Kaliakkavilai, Tamil Nadu, India.

Abstract – Biometrics is a recognition of individuals based on their behavioral and physical appearances. It have become popular in this era since it gives effective and a secured confirmation to a particular person. Biometric identification is gaining more and more recognition as a leading technology for identity management and security systems. Biometrics includes face, iris, fingerprints, voice, palms, hand geometry, retina, handwriting, gait etc. The fingerprints are considered to be the most determined because of its uniqueness and it can never be identical to another .Also they retain the same without any change throughout the time period. In biometrics, there are vulnerable shortcomings such as they are fragile to some attacks namely spoofing which refers to the fraudulent action by an unauthorized person to biometric system with fake inputs that generate authorized person's input. Henceforth it is important to detect the spoof, to this the proposed paper describes an easy to integrate and inexpensive technique or methodology to improvise the security through finger prints using Support Vector Machine (SVM). We achieved a better accuracy of 95.37.

Index Terms – Biometric, Fingerprint, Pattern, Spoof, Gelatin.

1. INTRODUCTION

In the recent years, biometrics takes effective steps for person recognition. Biometrics is a field of science and technology which is used to be measure life features. Fingerprint is still active topic for research in person identification. Normally, we used physiological feature for person identification because it is unique and remain unchanged throughout the life time of a person. Fingerprint is a combination of ridge and valleys found on the upper surface of the finger. Ridges are the dark area of the fingerprint and valleys are the light area exit between the ridges. Mostly we use fingerprint for person recognition because of small and inexpensive fingerprint capture devices, fast computation, and especially for its scalability, reliability and accuracy. Yet these systems are vulnerable to spoof attack. Here, the fake finger prints are generated with cheap materials such as gelatin, silicon etc. which replicate the users fingerprint to make a spoof for illegal authorization. In the other case it may be generated by the user itself to make a spoof for himself to cheat the attendance system. Hence, it is important to evaluate this secure problem. The term spoofing refers to fake access by an illegal user into fingerprint biometric system by generating identical fake fingerprint. The term spoofing refer to fake access by an illegal user into fingerprint biometric system by generating identical fake fingerprint. These spoofing have been carved through materials like play-doh, gelatin, etc.

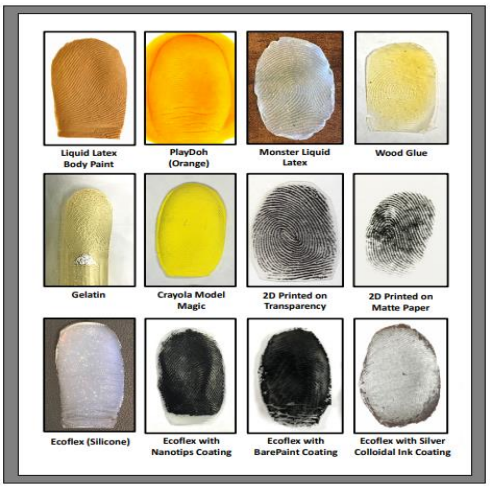

Fig. 1. Fingerprint spoof attacks can be realized using various readily available fabrication materials, such as PlayDoh, WoodGlue, Gelatin, etc.

2. RELATED WORK

Han et.al proposed a fingerprint Spoof Detection using contrast enhancement and convolutional neural networks [4]. This technique largely proceeds to the preprocessing process and the fake fingerprint detection process. The preprocessing step histogram equalization method increases the contrast of the fingerprint image. Then, the fingerprint image is divided into several non-overlapped blocks. They proposed CNN, which composed of 6 weight layers and totalizing the results. The author claimed that their proposed method attains 99.8% accuracy. Luca et.al analysed the fingerprint liveness detection using local texture features [5]. Binarised statistical image features for fingerprint liveness detection. BSF encodes the local fingerprint texture into a feature vector by using a set of

filters are used. Aditya et. al developed a fingerprint liveness detection method using local ridge frequencies and multiresolution texture analysis [6]. The approach is based on underlying texture and density of the finger print images. Abhyankar and Schuckers have developed a wavelet- based approach to detect fingerprint liveness [7]. This method is based on detection of a perspiration pattern from two successive fingerprints captured at zeroth second after placement and after 2s. The main reason behind using wavelet analysis is to separate the perspiration pattern. The low frequency content was extracted using multi-resolution analysis and the high frequency content was extracted using wavelet packet analysis. Then, the classification was performed using energy content of changing coefficients intensity.

3. PROPOSED MODELLING

The framework of the method includes the training process and the testing process. A classifier is trained using two classes of feature vectors in the training process. Then, the trained classifier is utilized to detect the fingerprint image. Feature extraction is a key step to deal with this classification problem. The datasets provided by the Liveness Detection Competition (LivDet) in the years of 2009 , 2011 , and 2013 are used in this research. To produce a qualitative finger print spoofing detection, the image pre-processing plays an important role. The image cropping is carried out first in which only the print is taken and the remaining portions are deleted. The contrast enhancement portion is done using Histogram Equalization method. Finally with canny edge detector algorithm is used to obtain the boundary. Image quality features based on ridge-valley properties of fingerprints are vital to detect fake fingerprints. The elasticity of the materials used for fabricating replica of fake fingerprints introduces non-uniformity in the ridge-valley structure of the captured image. As ridges and valleys are core part of a fingerprint image, scanning the differences between the ridge-valley structure of real and fake fingerprints is crucial in fingerprint liveness detection. Given a fingerprint image I and a set of k detected minutiae pointsM = fm1;m2; : : : ;mkg, a corresponding set of k local patches L = fl1; l2; : : : ; lkg, each of size [p _ p] where (p = 96), are extracted. Each local patch (li) is centered at the corresponding minutia point (mi). In case the detected minutiae is close to the image boundary, i.e. some region of the local patch lies outside the image region, then the patch region is shifted inwards such that it is completely embedded within the fingerprint region, ensuring the size of each patch to be [p _ p]. Ridge and valley width smoothness is measured by first cropping the block having a vertical ridge-valley structure to remove invalid regions. The resulting block is binarized using linear regression. Thereafter, the width of ridges and valleys is computed for each horizontal line of the block having alternate ridge-valley structure. Widths of the each ridge and valley of the block will be aligned. The feature extraction is an important part in Machine learning. Feature vector X describes the biometrics and it is generated by the feature extraction procedure as explained by the equation below.

$$E(x(i,j)) = \mathbf{x} = \begin{bmatrix} c_1 \\ c_2 \\ \dots \\ c_n \end{bmatrix} \qquad (1)$$

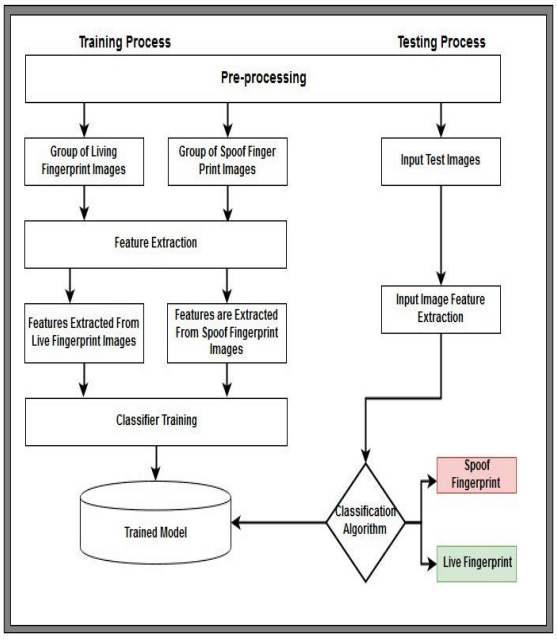

Fig .2.Architecture of Proposed Model

The x(i,j) is the finger print image, E is the set of feature extraction functions and N represents the size of the feature extraction. In the proposed work the size of N is 10. Each of the features is described by the individual pore spacing feature: through the analysis of pixels along the ridges, it is possible to find sweat pores in the image. Live fingerprint images fingers should have these information strongly defined. Residual noise feature: the coarseness of the surface of the sample can be measured as the total amount of Gaussian white noise in the original image. An additional effort has to be done to produce fingerprint spoofs as coarse as live fingers. Due the perspiration phenomenon, live fingers demonstrate a distinctive spatial moisture pattern which implies on gray level variations along the image.

Fingerprint Spoof Detection Algorithm Using SVM

Training Phase

1. Read the Input fingerprint training Images from the database.

2. Obtain the Image Quality Assessment Measures as No reference and Full reference from the training images.

3. Combine the entire obtained image Quality Measure as a IQA feature.

4. Make a Target for SVM classification.

5. SVM classifier trained with two classes as Spoof or Live.

Testing Phase

1. Read the test fingerprint Images from the database.

2. Obtain the Image Quality Measures from the test Images.

3. Combine all the Quality Measure as a feature template.

4. Feature template is now compared with the trained Feature values using SVM classifier.

5. Finally the output is given that the test image is Spoof or Live.

4. RESULTS AND DISCUSSIONS

We have tested the proposed work with the fingerprint images obtained from the Liveness Detection Competition (LivDet) in the years of 2009 , 2011 , and 2013.we used the spoof and live fingerprint for experimentation. The research work is implemented on Intel core i3 processor using Dotnet2012. The proposed system can analyze to predict whether a person should be claimed as a live or spoof. In order to evaluate the success of the system, a standard measurement is used to verify the acceptance errors and rejection errors. They are defined as follows:

- False Reject Rate (FRR)
- False Acceptance Rate (FAR)

The FRR is the percentage of clients or authorized person that the biometric system fails to accept. FRR is defined as

$$\text{FRR} = \frac{\text{Number of rejected clients}}{\text{Total number of client access}} * 100\%$$

The FAR is the percentage of imposters or unauthorized person that the biometric system fails to reject. FAR is defined as

$$\text{FAR} = \frac{\text{Number of accepted imposter}}{\text{Total imposter access}} * 100\%$$

The accuracy of the biometric system is defined as

Accuracy = max (100 – (FRR+FAR)/2)

Traits	Algorithm	FAR (%)	FRR (%)	Accuracy (%)
Fingerprint	SVM	8.49	0.87	95.37

Table1: FAR, FRR and Accuracy Rate

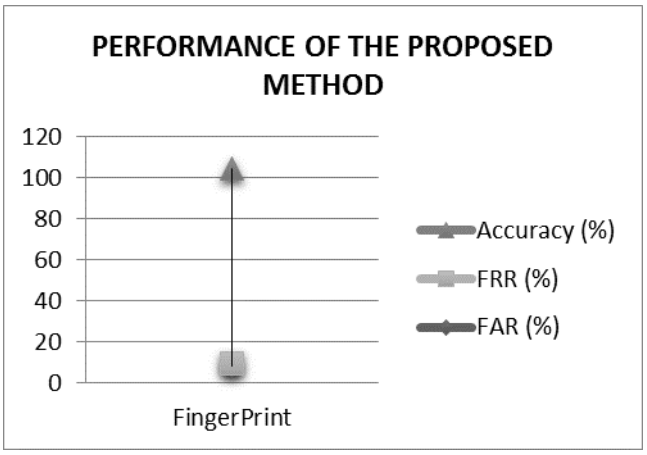

Fig.3. FAR, FRR and Accuracy Rate

5. CONCLUSION

In this work, we have proposed a novel method for fingerprint liveness detection, owing to the dispersion and variations in the ridge-valley structure of the fake fingerprint images. In this research Support Vector Machine approach has been developed to classify the fake and genuine fingerprint. The proposed SVM classifier has been successfully applied to fingerprint spoofing detection process .The achieved high accuracy rate in classifying the fingerprint is 95.37%. It demonstrates greater effectiveness over existing fingerprint detection system.

REFERENCES

[1] J. G. Kreifeldt, "An analysis of surface-detected EMG as an amplitude-modulated noise," presented at the 1989 Int. Conf. Medicine and Biological Engineering, Chicago, IL.

[2] J. Williams, "Narrow-band analyzer (Thesis or Dissertation style)," Ph.D. dissertation, Dept. Elect. Eng., Harvard Univ., Cambridge, MA, 1993.

[3] Rodrigo Frassetto Nogueira ; Roberto de Alencar Lotufo ; Rubens Campos Machado, "Fingerprint Liveness Detection Using Convolutional Neural Networks", IEEE Transactions on Information Forensics and Security (Volume: 11 , Issue: 6 , June 2016).

[4] Han-Ul JangHak-Yeol ChoiDongkyu KimJeongho SonHeung-Kyu Lee, "Fingerprint Spoof Detection Using Contrast Enhancement and Convolutional Neural Networks",

[5] Luca Ghiani University of Cagliari, Italy ; Abdenour Hadid ; Gian Luca Marcialis ; Fabio Roli, "Fingerprint liveness detection using local texture features", IET Biometrics (Volume: 6 , Issue: 3 , 5 2017).

[6] Aditya Abhyankar, "Fingerprint Liveness Detection Using Local Ridge Frequencies and Multiresolution Texture Analysis Techniques", 2006 International Conference on Image Processing.

[7] Y.S. Moon ; J.S. Chen ; K.C. Chan ; K. So ; K.C. Woo, "Wavelet based fingerprint liveness detection", Electronics Letters (Volume: 41 , Issue: 20 , 29 Sept. 2005).

[8] Luca Ghiani ; David Yambay ; Valerio Mura ; Simona Tocco ; Gian Luca Marcialis, "LivDet 2013 Fingerprint Liveness Detection Competition 2013", 2013 International Conference on Biometrics (ICB).

[9] Ramandeep Kaur ; Parvinder S. Sandhu ; Amit Kamra, "A novel method for fingerprint feature extraction", 2010 International Conference on Networking and Information Technology.

[10] P.GnanasivamS.Muttan, "An efficient algorithm for fingerprint preprocessing and feature extraction".