Fine Representation of Spoofing Detection Using Convolutional Network Algorithm

Dr.B.Nataraj[1], P.Kavithanjali[2], K.Menaka[3] and T.Pavithra[4]

[1]Associate professor, Department of ECE, Sri Ramakrishna Engineering College, Coimbatore, Tamilnadu, India
nataraj.b@srec.ac.in
[2]UG Scholar, Department of ECE, Sri Ramakrishna Engineering College, Coimbatore, Tamilnadu, India
kavithanjali.1202101@srec.ac.in
[3]UG Scholar, Department of ECE, Sri Ramakrishna Engineering College, Coimbatore, Tamilnadu, India
menaka.1202114@srec.ac.in
[4]UG Scholar, Department of ECE, Sri Ramakrishna Engineering College, Coimbatore, Tamilnadu, India
pavithra.1202134@srec.ac.in

ABSTRACT

Biometrics is the unique identity for every human which can be measured and used for accessing ones important information. In this project the biometrics used are Iris, Fingerprint and Face have been taken as an identity to prevent spoofing. Here Matlab image acquisition tool box is used to load the iris and fingerprint images from the datasets and face image is taken from the HD Webcam and processed via convolutional network. Finger print module is also used to take input images of finger prints and micro-controller is used to process it. The image is processed as a quadric kernel. Hyper parameter (i.e) the boundary strength is used to plot the values in a two-dimensional space. Those values are called as Pixel in Pixel (PIP) values, which are used to detect real and fake images and that prevent spoofing.

Keywords: Biometrics, convolutional network, spoofing, Matlab, MPLAB

1. INTRODUCTION

Security has been easily weakened nowadays. So, in order to prevent spoofing, that is faking someone's identity, can be prevented because of the steady progress of researchers in developing anti-spoofing systems. Images of biometrics are processed; that processing involves enhancement of the image, noise removal etc,. A digital image is an information that is spread variedly across the two dimensional space of X and Y axes. These images are taken from a data acquisition tool and then manipulated by converting them into numerical values with the help of a digitizer.[2] Image processing involves following functions: Acquisition, segmentation, representation & description, preprocessing, recognition and interpretation. After processing it can be stored in different formats. Image processing, also involves complex algorithms for functioning, which has led to the development of many real time devices. For example: sensor modules, digital cameras and displays. The objective of the project is to process the image inputs that are loaded from the dataset and prevent spoofing. The entire strength the image quality is found. Quality assessment is done by finding signal to noise ratio, absolute error and maximum difference and other quality measures. This results whether the The results are displayed using Matlab software. software module will process the already taken 8-bit gray scale images of Iris and fingerprint. Face images will be taken from the webcam and is then converted into gray scale image. By comparing specific pixel values with that of its boundary

2. RELATED WORK

N. K. Ratha proposed the following theory

The development in the field of biometrics which provided authentication to applications and based on the authentication, which offers several merits over possession-based methods such as password/PIN-based systems (i.e) ATM machines[1]. Also, it is important that biometrics-based authentication systems are developed to withstand different kinds of attacks

on the system when it is deployed in security-critical applications. This has more importance in remote applications such as e-commerce. The sophisticated security holes in a biometrics-based authentication scheme, quantify the numerical strength of one method of fingerprint matching.

3. BLOCK DIAGRAM

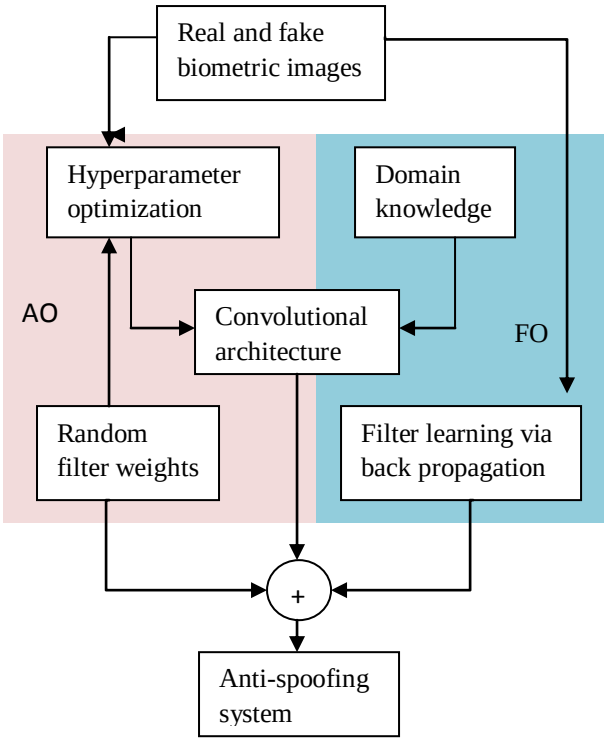

Fig 1. Systematic block diagram

4. HARDWARE DESCRIPTION

The fingerprint module once if connected to PIC 16f877A , the Embedded C language describing the control and manipulation of the fingerprint.

4.1. PIC Controller 16F877A

PIC microcontroller is based on the RISC architecture. The device is fabricated with CMOS technology. The main advantage of CMOS is that it has immunity to noise than other fabrication techniques. It has 3 memories ROM, RAM, EEPROM etc. Memory that is used frequently in pic16F877 is flash memory, so that data is retained even when the power is switched off. All microcomputer systems are based on certain building blocks.

CPU - the part that does all logic and arithmetic functions

RAM - storage for programs and program variables.

ROM - read-only parts of programs.

I/O - connection to external devices

Features

1. Speed: Harvard Architecture, RISC architecture, 1 instruction cycle = 4 clock cycles.
2. Instruction set simplicity: The instruction set consists of just 35 instructions (as opposed to 111 instructions for 8051).
3. Power-on-reset and brown-out reset. Brown-out-reset means when the power supply goes below a specified voltage (say 4V), it causes PIC to reset; hence malfunction is avoided. A watch dog timer (user programmable) resets the processor if the software/program ever malfunctions and deviates from its normal operation.
4. PIC microcontroller has four optional clock sources. Low power crystal
    a. Mid-range crystal
    b. High range crystal
    c. RC oscillator (low cost).
5. Programmable timers and on-chip ADC.
6. Up to 12 independent interrupt sources.
7. Powerful output pin control (25 mA (max.) current sourcing capability per pin.)
8. EPROM/OTP/ROM/Flash memory option.
9. I/O port expansion capability.

PIC16F877 is a 40 pin microcontroller. It has 5 ports port A, port B, port C, port D, port E. All the pins of the ports are for interfacing input output devices. The crystal oscillator speed that can be connected to the PIC microcontroller range from DC to 20MHz. Using the CCS “C” compiler normally 20MHz oscillator will be used and the price is relatively cheaper. The 20 MHz crystal oscillator should be connected with about 22pF capacitor.

4.2. Fingerprint Module

Fingerprint processing includes two parts: fingerprint entry and fingerprint matching (the matching can be 1:1or 1:N). When entering, user needs to enter the finger two times. The system will process the two time finger images, generate a template of the finger based on processing results and store the template. When matching, user enters the finger through optical sensor and system will generate a template of the finger and compare it with templates of the finger library. For 1:1 matching, system will compare the live finger with

specific template designated in the module; for 1:N matching, or searching, system will search the whole finger library for the matching finger. [8]In both circumstances, system will return the matching result, success or failure.

5. SOFTWARE DESCRIPTION

Matlab is a high level programming language software and is high interactive in computational and visualization aspects. Matrix laboratory is abbreviated as MatLab. Because every data it processes, for example: a signal, an image or a video it manipulates a numerical value for the entire input[5]. Those numerical values are arranged in definite rows and columns based on their apprehension. Matlab is also a simulation software that was created to implement numerical algorithms for a number of applications. The basic language used is very similar to standard linear algebra notation, but there are a few extensions that will likely cause you some problems at first.

MPLAB is a Windows program package that makes writing and developing a program easier. It could best be described as developing environment for some standard program language that is intended for programming a PC computer. Some operations which were done from the instruction line with a large number of parameters until the discovery of IDE "Integrated Development Environment" are now made easier by using the MPLAB. Still, our tastes differ, so even today some programmers prefer the standard editors and compilers from instruction line. In any case, the written program is legible, and well documented help is also available.

5.1 SOFTWARE TOOLS

- Programming Language: Embedded C
- Development Tool: MPLAB IDE

PIC microcontrollers achieve low-risk product development by providing varied program size expansion. Pin compatibility facilitates drop-in replacements of package types as well as variations of reprogrammable and one-time programmable (OTP) program memory without having to completely re-write code. Microchip's MPLAB Integrated Development Environment (IDE), a simple yet powerful development environment, supports low-risk product development by providing a complete management solution for all development systems in one tool.

To maintain the process, the controller is commanded using embedded C language. The code is written in the editor and is compiled by High-tech Compiler. After compilation the program is build, so that its hex file is generated. The hex file information is easily understandable by the PIC controller so that the further process of finding double precision, gray scale conversion and quality assessments are done.

5.2. MATLAB Output

The output of the system has double precision image, Gaussian noise removed image and its interpolation. The output is like providing secured access (i.e) it gives the info, whether the input is real or fake or unidentified one. Based on the inference from the command window of Matlab spoofing is detected.

OUTPUT 1

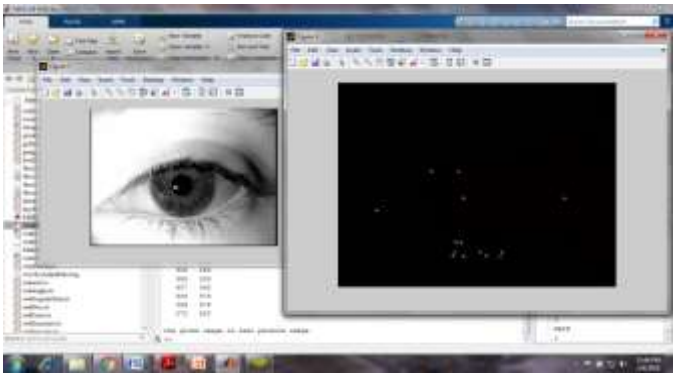

Fig 2. Iris interpolation, result is displayed as " given image is Real "

Above figure is the result of Iris Interpolation, the iris image which is real because of its fine interpolating points recovered from pixel in pixel values computed by the quality assessment including the noise removal and Average differences.

The Iris image can be faked by wearing contact lenses of different iris colors [7]. These kind of vulnerabilities to the biometrics system acts as the mask in the captured image. That can be removed by analyzing the layer into four equiquadrants and taken for preprocessing.[4].

OUTPUT 2

The figure 3, representing the fingerprint interpolation, the result is Fake image because the Pixel in pixel values before and after Quality assessment is not in correlation. Hence, the result is Unreal.

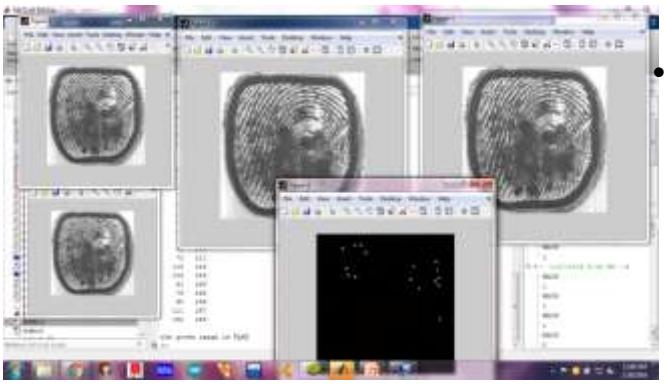

Fig 3. Fingerprint interpolation, result is displayed as "given image is Fake"

OUTPUT 3

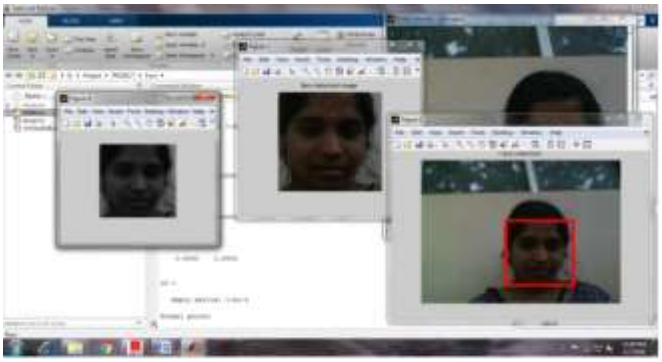

Fig 4. Detection of face in an image captured, using Viola and jones method.

Above figure is the systematic output of Face detection from 1026x512 video frame captured via webcam. If the attributes regarding the face description matches the expected result either as a normal person or Intruder, the result is displayed appropriately in the Command window of Matlab.[3].

6. PROPOSED WORK

The spoofing detection of various biometrics such as Iris, fingerprint and face detection are done using Matlab software by reducing the layer architecture by Convolutional algorithm. The Gaussian noise removal followed by average and maximum difference calculation convolved with nearby pixel values[9][10]. Those values are inclusive within the average error rate. Almost 13% error is minimized when compared with the existing advancements.

7. ADVANTAGES

- Very high accuracy.
- Verification time is generally less.
- Is the most economical.
- Easy to use.

Small storage space required for the biometric template, reducing the size of the database memory required.

- It is a cheap technology.

8. APPLICATION

ATM iris recognition

Using iris recognition ATM, a customer simply walks up to the ATM and looks in a sensor camera to access their accounts. The camera instantly photographs the customer's iris. If the customers iris data matches the record stored a database access is granted. At the ATM, A positive authentication can be read through glasses, contact lenses and most sunglasses. Iris recognition proves highly accurate, easy to use and virtually fraud proof means to verify customer's identity.

9. CONCLUSION

In this work, we investigated two deep representation research approaches for detecting spoofing in different biometric modalities. On one hand, we approached the problem by learning representations directly from the data through architecture optimization with a final decision-making step atop the representations. On the other, we sought to learn filter weights for a given architecture using the well-known back propagation algorithm. As the two approaches might seem naturally connected, we also examined their interplay when taken together. In addition, we incorporated our experience with architecture optimization as well as with training filter weight for a given architecture into a more interesting and adapted network, spoofnet. The resultant data gives the decision to follow in a destined path. Using the evaluation or validation set during the process of training, we can optimize both filter and the system architecture.

REFERENCES

1. K. Jain and A. Ross, "Introduction to biometrics," in Handbook of Biometrics. New York, NY, USA: Springer-Verlag, 2008, pp. 1–22.
2. C. Rathgeb and A. Uhl, "Attacking iris recognition: An efficient hillclimbing technique," in Proc.

IEEE/IAPR 20th Int. Conf. Pattern Recognit. (ICPR), Aug. 2010, pp. 1217–1220.

3. W. R. Schwartz, A. Rocha, and H. Pedrini, "Face spoofing detection through partial least squares and low-level descriptors," in *Proc. IEEE Int. Joint Conf. Biometrics (IJCB)*, Oct. 2011, pp. 1–8.
4. J. Galbally, J. Fierrez, and J. Ortega-Garcia, "Vulnerabilities in biometric systems
5. N. K. Ratha, J. H. Connell, and R. M. Bolle, "An analysis of minutiae matching strength," in Audio- and Video-Based Biometric Person Authentication. Berlin, Germany: Springer-Verlag, 2001, pp. 223–228.
6. A. F. Sequeira, H. P. Oliveira, J. C. Monteiro, J. P. Monteiro, and J. S. Cardoso, "MobILive 2014—Mobile iris liveness detectioncompetition," in Proc. IEEE Int. Joint Conf. Biometrics (IJCB), Sep./Oct. 2014, pp. 1–6.. inescporto.pt/
7. K. W. Bowyer and J. S. Doyle, "Cosmetic contact lenses and iris recognition spoofing," Computer, vol. 47, no. 5, pp. 96–98, May 2014.
8. L. Ghiani *et al.*, "LivDet 2013—Fingerprint liveness detection competition," in *Proc. Int. Conf. Biometrics (ICB)*, 2013, pp. 1–6. [Online].
9. I. Chingovska, A. Anjos, and S. Marcel, "On the effectiveness of local binary patterns in face anti-spoofing," in Proc. Int. Conf. Biometrics Special Interest Group (BIOSIG), 2012, pp. 1–7.
10. N. Erdogmus and S. Marcel, "Spoofing in 2D face recognition with 3D masks and anti-spoofing with Kinect," in Proc. IEEE 6th Int. Conf. Biometrics, Theory, Appl., Syst. (BTAS), Sep./Oct. 2013, pp. 1–6.

