Irish Interdisciplinary Journal of Science & Research (IIJSR)
Vol.5, Iss.1, Pages 118-130, January-March 2021

Multi Biometric Authentication using SVM and ANN Classifiers

T. Thamaraimanalan[1], Pranavakumar S.[2], Lingeswaran R.A.[3], Kabileshar R.M.[4] & Sarankarthick M.[5]

[1]*Assistant Professor,* [2-5]*UG Student, Department of ECE, Sri Eshwar College of Engineering, Coimbatore.*

Article Received: 21 January 2021 *Article Accepted: 13 March 2021* *Article Published: 26 March 2021*

ABSTRACT

Data variability can be categorized based on the capture, analysis and treatment of biometric sample dataset. Initial interpretation of the data is necessary and this knowledge must be integrated into the identification system and an important feature of biometrics should be tested. This paper provides an examination of various biometric quality definitions and interpretations. In comparison to a bogus synthetic or reconstructed sample, the real existence of a legitimately valid phenotype is an essential issue for biological authentication that involves the creation of new and appropriate security mechanisms. The suggested solution introduces a modern fake identification programmed tool which can be used to identify various kinds of illegitimate access attempts in multiple biometric systems. It is also very difficult to use with 25 general image quality measurement features taken from an image, which makes it ideal for real time applications, to separate valid and impostor samples using the classification of artificial neuronal network. The study of actual biometric samples' general image quality provides extremely useful details which could be used extremely effectively to distinguish them from false properties. The experimental findings, obtained with publicly accessible fingerprint, iris, and 2D facial data, suggest that the proposed method is highly competitive with other cutting-edge approaches.

Keywords: Image quality assessment, Biometrics, Attacks, Artificial neural network.

1. Introduction

1.1 Overview

The use of a quality test is inspired by the hypothesis that: "The false image obtained in an attempted attack would have a quality that is different from the true sample in which the sensor has been developed in the usual operating scenario." The expected discrepancies in consistency between actual and counterfeit samples could include: degree of sharpness, color levels and luminance, local objects, sum of image data (entropy), structural distortions or natural appearance. In reality, iris photographs taken from printed text, for example, are most often distorted or out of focus because of tumor; facial images collected from moving devices are likely to be over- or out of focus; and it is not infrequent to see local objects such as spots and patches caught from fingerprints captured from rubber fingers. Moreover, in a potential attack in which an image generated synthetically is inserted directly into the communication channel before the extractor feature, any properties found in natural images would most likely fail. Following this theory, we discuss the possibilities of a general evaluation of image quality as a tool for protecting against various biometric attacks. This offers a new multibiometric calculation system [1-7].

1.2 Background

In Iris, face- and fingerprint recognition, the best-known biometric authentication system used in recent years is. Entry checks, ATMs and government programmers are the key applications. Recently, companies have realized and offered goods to understand the benefits of biometric authentication. Biometrics is an identification function and becoming more relevant.

1.3 Problem Statement

The existing system was not able to consider:

- Dynamic, characteristically characteristic LDA and SVM classification algorithms; (e.g. minutiae points, iris position and face detection).
- AO data obtained from the efficiency of SOTA (State of the Art) and the measurement of the weights of the filter slows up the operation computationally for about 45 milliseconds.

1.4 Objective

The purpose of the proposed method is to improve the protection of biometric recognition frameworks through the use of image quality assessment, by incorporating liveliness measurement easily, user-friendly and intrusively.

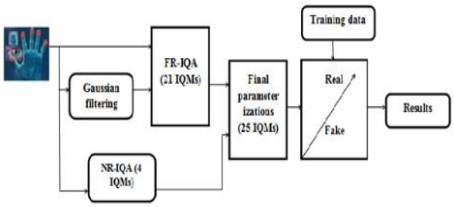


Fig.1. Block Diagram of Biometric Recognition

2. Literature Survey

2.1 Introduction

Biometrics plays an important part in safety procedures in the modern world. An significant method in the field of image processing is the consistency measurement of images. It focuses on a texture consistency evaluation and seeks to determine whether texture can be applied to existing state-of- the art image methods. A measure especially designed for textures, the focus of further efforts, is needed to make testing methods perform well on used textures. Most of the new approaches are often intended to deal with grey images only. The use of knowledge of both sizes is the merit of the image consistency measurement methodology. This approach also makes a more detailed test of the various textures. The key implementations of the current method are the following two techniques [1, 8-14].

- Living Detection Image Quality Assessment
- Detailed IQ steps with comparison and no reference.

2.2 Image Quality Assessment Technique

The estimation of the quality of the image aims to measure the visual quality of a given picture. These distortions are unavoidable in any automated pipeline (acquisition, compression, transmission, etc. of images). The only "right" way to assess the optical consistency of the pictures viewed by human beings is to measure them. Unfortunately, this is a costly, extremely time intensive technique that is not used in real-time applications (adjustment of the rate of transfer etc.). Consequently, an automated method is necessary which predicts the visual quality perceived by the person as near as possible. The groundbreaking work in this field was to experiment with manipulating textures to figure out what is necessary for a human being to differentiate between two textures. This analysis is based on a texture consistency assessment. Their job

varies from the standard evaluation of consistency. The optimal calculation will predict and calculate how much one can, or cannot, discern from a human's initial texture from the test texture (e.g. converted). This cannot be done by some kind of pixel comparison because the exact correspondence from pixel to pixel is normally not required or often unwanted. Structural analysis or predictive features may be the best way. Most current approaches are developed to assess the optical consistency of images such as photographs around the world. In this paper, the most widely used approaches were surveyed to see whether they could be refined and used or at least any of their concepts. The monospectral (grey) photographs all of the techniques tested. They may also be used after preprocessing of multispectral files, but this result in information loss.

2.3 IQ Assessment for Liveness Detection

The use of a quality assay is inspired by the hypothesis that: "The false image obtained in an attempted attack would have a quality that is different from the true sample in which the sensor has been developed in the usual operating scenario." The expected discrepancies in consistency between actual and counterfeit samples could include: degree of sharpness, colour levels and luminance, local objects, sum of image data (entropy), structural distortions or natural appearance. In this case, iris photographs taken from printed text, for instance, are more likely to get blurred or out of sight because of shaking. It are certain that the fingerprint photographs taken from rubber fingers show local acquisition artefacts; and it is not uncommon for them.

Moreover, in a potential attack in which an image generated synthetically is inserted directly into the communication channel before the extractor feature, any properties found in natural images would most likely fail. Efficiency, completeness, sophistication and speed are the requirements for choosing liveliness detection systems. In the current research work, we discuss the possibility for a general image quality evaluation as a method of defense from various biometrics, pursuing this hypothesis of "quality discrepancy" different biometric attacks.

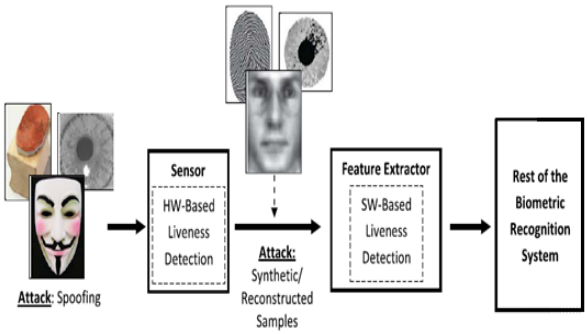


Fig.2. Types of Attacks Potentially Detected by Hardware-based and Software-based Liveness Detection Techniques

3. Liveness Detection

3.1 Introduction

Image quality is a feature of an image which measures the deterioration of the perceived image. That is called an evaluation of image consistency. Imaging systems can enter certain quantities of distortion or artefacts into

the signal, such that the quality evaluation is a significant issue. A picture forms on the camera image plane and then tests the photograph electronically or chemically. In some circumstances, the content determination photograph is not mostly the result of a camera photography operation, but the result of the picture being stored or transmitted. A common example is a compressed, saved or transferred digital file, which is then again decompressed. Statistical techniques may be used to calculate the average quality of the lossless compression process by taking a broad series of images in consideration and calculating a quality measurement on each. The resulting image quality in a standard digital camera depends on all three of these factors: how often the camera's imaging process differs to the pinhole, the quality of the image measuring process, and the artefacts introduced by the camera image, usually by JPEG coding technique.

3.2 Liveness Detection Method

Face identification has been used extensively in biometrics. However, mechanisms of face recognition are vulnerable to non-real facial spoof attacks. In order to prevent such spoofing, a stable device needs lifespan identification. Face-life identification approaches in this work are classified on the basis of the different methods used to detect liveliness. This categorization helps to explain various scenarios of spoof attacks and their ties to solutions established. Liveness is the difference between live and non-living function space. The fundamental aim is to distinguish the mask from the false in form and detail. Further evaluation of image quality results will be based on the Liveness detection.

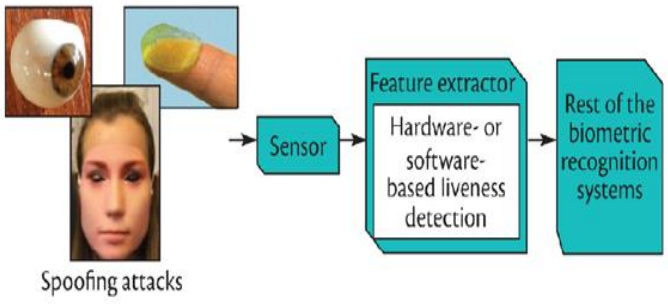


Fig.3. Liveness Detection

3.3 Liveness Detection IQA methods

Methods for the identification of life are normally divided into one of two groups [1].

- Hardware strategies that add a specialized sensor system to identify specific characteristics of a living characteristic (e.g., fingerprint sweat, blood pressure, or specific reflection properties of the eye)
- Software-based methods for detecting the false property when a regular sensor is added to a sample (i.e., features used to distinguish between real and fake traits are extracted from the biometric sample, and not from the trait itself).

Both approaches show some benefits and disadvantages over the others, and in general the most suitable safety solution for increasing the security of biometric systems will be a mixture of both. Hardware-based systems typically have a higher fake detection rate as a rough contrast, whereas software-based technologies

are often cheaper (as no additional device is required) and less invasive because their implementation is user transparent.

3.4 Frequency and Texture Based analysis

A single image-dependent fake face detection approach for differentiating living face from 2-D paper masks based on a frequency and texture analysis was suggested. The power spectrum-based frequency analysis method has been developed, which utilizes both low frequency and high frequency information. In order to evaluate the textures of the given face pictures, the definition approach based on Local Binary Pattern was also used. The textures are taken as the images taken with the 2-D (lighting components) objects appear to experience a lack of detail about texture relative to images taken with the 3-D objects.

For function extraction, extraction of frequencies, extraction of textures based functions and extraction of fusion based functions is introduced. The texture-based vividness identification is achieved on the basis of a single face picture study through Fourier Spectra. Their approach is focused on live face details on shape and movement.

4. ANN Classifications

4.1 Introduction

The purpose of an image quality evaluation is to include computer models to calculate the perceptive quality of a particular image. The techniques of image quality can be subjective and analytical in two sections. Subjective image evaluation is based on subjective experiments [5].

Objective methods of image quality evaluation are focused largely on some statistical tests. Over the last five years, the massive and inevitable demands for visual output measurement in a number of applications have been shown and shown.

4.2 Objective Methods

This is a quantitative method in order to quantify a number indicating image consistency by the strength of the two images, references and distort types. A complete reference, diminished reference or no reference can be listed in the objective Image Quality Assessment (IQA) [6]. IQA focused on reference image supply. The aim is to automatically determine perceptional content in a way which is linked to human appreciation, as part of objective model picture quality evaluation.

4.3 Full Reference (FR) model

This approach offers access to a "perfect version" of the image or video that can be linked to a "distorted version." The 'perfect version' normally emerges from a high-quality acquisition system until, for instance, compression and transmission errors distort it. In general, two groups are available for the quantitative quality control methodology, basic mathematical error measurements and human visual system metrics.

Full reference counter measures

Error sensitivity measurements: 1.

4.4 Feature Extraction pixel difference metrics

The principle of function detection refers to methods used in computer vision and image processing to compute the abstract information on an image and make local decisions on each picture point whether or not there is an image of the same kind at this point. The characteristics arising from the picture are sub-sets, often as isolated points, continuous curves or contained areas. If the input data to an algorithm are notoriously redundant and too large to process, the input data will then be converted into a reduced set of features (also named features vector). To transform the input data into feature collection, extraction of functionality is named. In order to accomplish the desired purpose with this reduced representation instead of the complete size input, the functionalities that have been extracted are required to exclude valid information from their input data.

5. Parameter Calculations & Outputs

5.1 Introduction

The results of multiple attack identification experiments on the image and its measured values are graphically displayed.

5.2 Parameter Calculations

The Proposed system is evaluated by calculating the following parameters,

Table 1. Comparison between existing and proposed system

Parameters	Existing System	Proposed System
Algorithm used	SVM, LDA & Fuzzy logic	ANN
Pixel Resolution	320X280 pixels input image	640X480 pixels and 320X280 pixels for iris and finger print
Data base analysis	Morph data base & 3D Mask Attack Data Base	3D mask attack data Base & Real and synthetic Data base

5.3 Processing of images

Face Input Image Processing images are first loaded into the software to detect their genuineness. The three Iris, Face and Fingerprint templates are loaded with a multi-assault identification technique. Original image is filtered using the complete reference filtering system Gaussian. In more operations they are contrasted with initial and blurred or corrupted images.

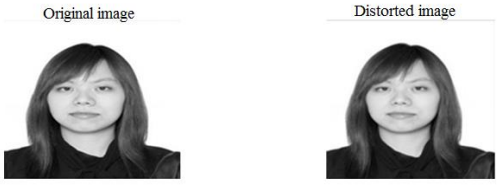


Fig.4. Original Input Image and Filtered Image

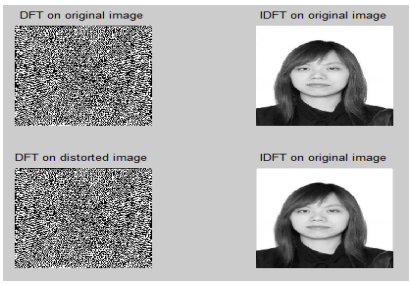
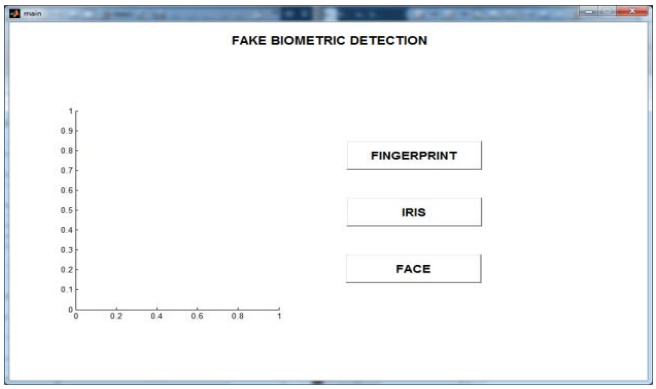


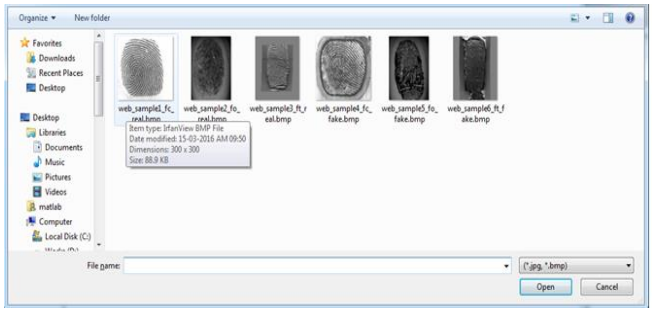
Fig.5. Performance of DFT and IDFT on Original and Distorted Image

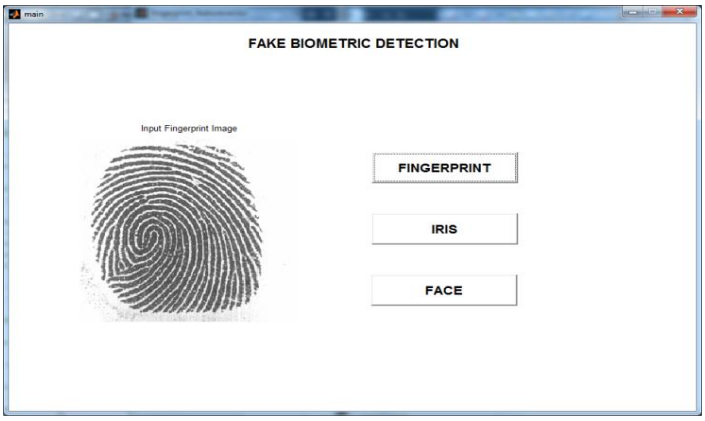
Fingerprint Processing

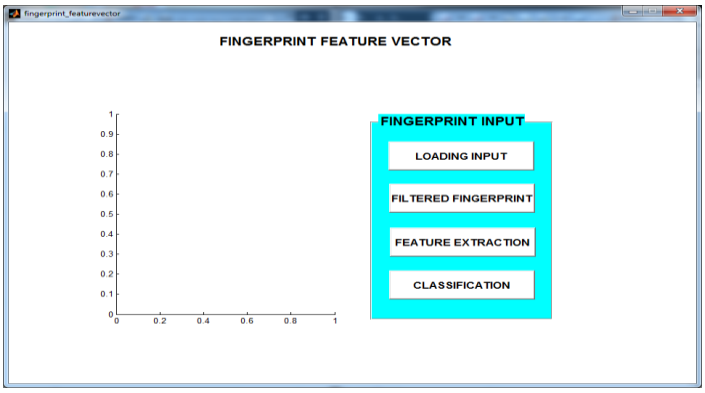
Fingerprint processing involves in the operation of loading a fingerprint model and filtering it using Gaussian filtering method which uses Gaussian co-efficient = 0.5 .

Fig.6. Original Input Image and Filtered Image for Fingerprint

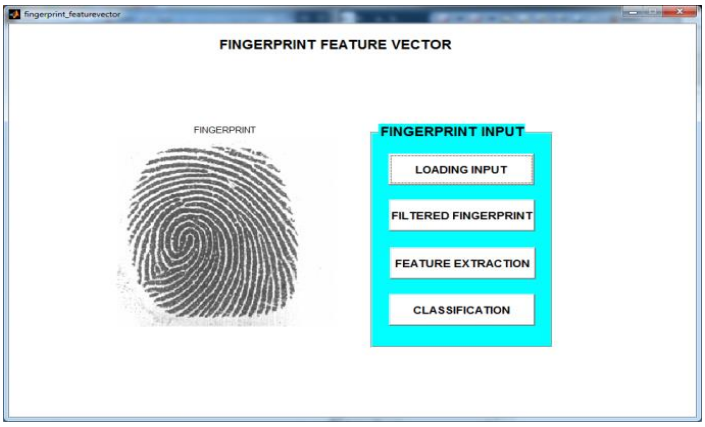




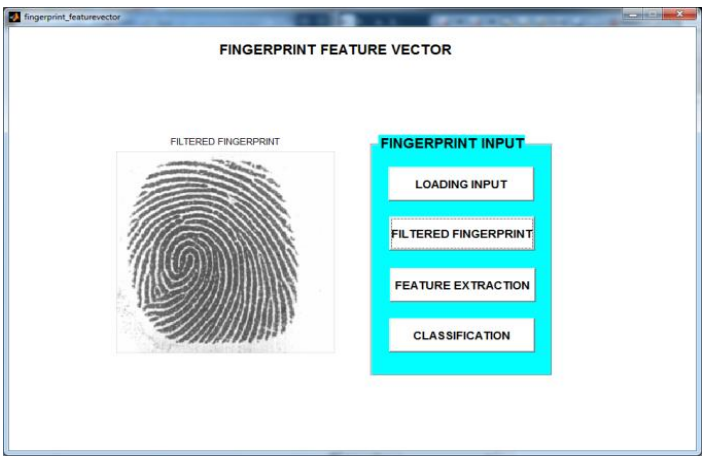




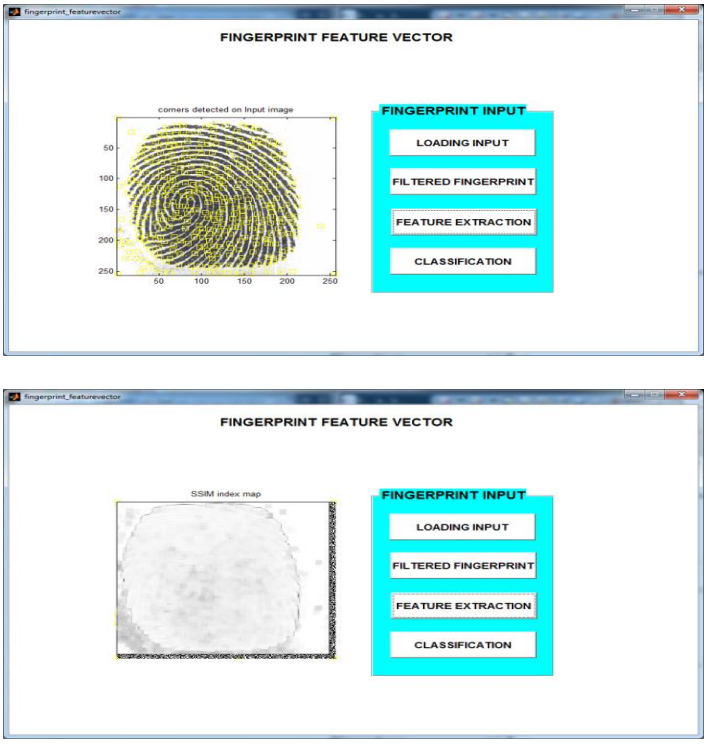
After clicking load the input:



After clicking filter finger print:



After clicking filtered Image:



After clicking Classifications:

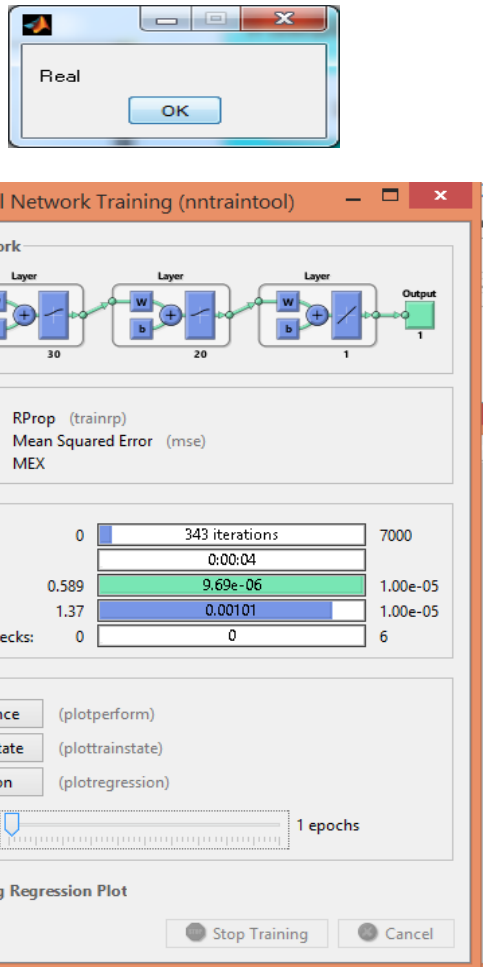


Fig.7. Analysis of ANN

The above Fig.7 describes the starting function of the ANN Performances. This has three categories namely Performance, Training State and Regression methods. The performance is analyzed based on Mean Squared Error method (MSE).

The following graph describes about the Performance analysis of ANN.

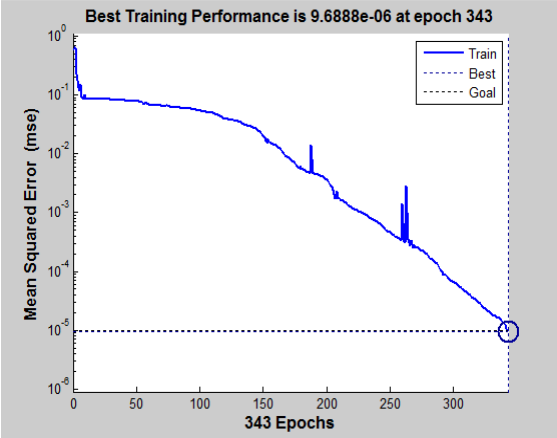


Fig.8. Training Performance of ANN

The following graph says about the Training state analysis.

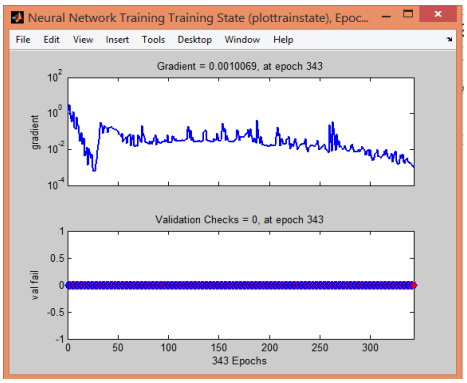


Fig.9. Graph on Training State

The following graph describes about the regression state analysis.

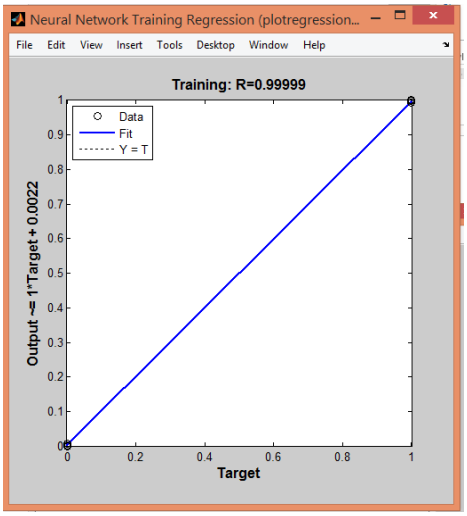


Fig.10. Graph on Regression State Analysis

Compared output values from SVM and ANN:

Fingerprint Features:

Mean Square Error = 1.3655

Peak Signal to Noise Ratio = 46.7778

Normalized Cross-Correlation = 0.9985

Average Difference = 0.1135

Structural Content = 1.0028

Maximum Difference = 19

Normalized Absolute Error = 0.0041

R-Averaged MD = 0.2455 R-Averaged SD = 1.9000 LEDs = 22, 6801 LMSE (Laplacian Middle Squared Error)

Difference of total edge = 0.0014.

Difference of the total corner = 1.9847e-05

Magnitude Spectral Error = 0.

Error in spectral phase = 0

Magnitude Gradient Error = 22.3719

Error phase gradient = 5.2905

Measurement index of structural similarity = 0.9950

Fidelity to Visual Information = 0.9498

• ***SVM-ANN Contrast Comparison***

The performance characteristics of SVM and ANN are focused primarily on determinist and non-deterministic SVM and ANN algorithms.

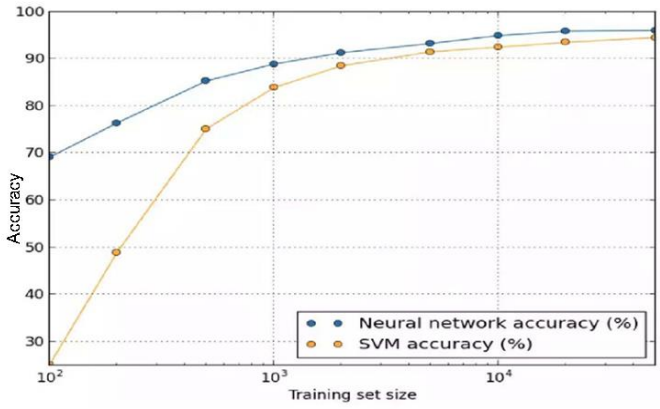


Fig.11. Accuracy plot of SVM and ANN

6. Results and Discussion

A biometric device is a computer system that uses fingerprint, facet, iris, keystrokes, signature, speech etc to identify the user with his or her behavioural and physiological features. False anti-spoofing biometrics must be detected as well. Our project entitles users to identify the spoofed image using the image consistency measurement method for the identification of animal life. It involves the *IRIS FACE AND FINGERPRINT SPOOFING DETECTION QUALITY TECHNIQUE.* This paper presents a non-deterministic ANN system which uses multi-layer perception (non-trivial), including facial recognition, fingerprint recognition and iris recognition (Multi Biometric System). It also initiates system attacks using image quality evaluation for the detection of life, how to defend the system from counterfeit biometrics and how the multi-biometric system is safe than that of a single biometric system.

7. Conclusion

From the assessment findings provided in the parts of the paper some hypotheses may be extracted: (1) The proposed method is capable of consistently performing highly for different biometric characteristics on an on-going basis ('multibiometrics';) (2) The proposed method can be used to adapt to various attack types providing all of them with a high level of protection ('multi-attack').

Declarations

Source of Funding

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Competing Interests Statement

The authors declare no competing financial, professional and personal interests.

Consent to participate

Not Applicable

Consent for publication

We declare that we consented for the publication of this research work.

Availability of data and material

Authors are willing to share data and material according to the relevant needs.

References

[1] Javier Galbally, Sébastien Marcel, “Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition” Javier Galbally, Sébastien Marcel, Member, IEEE, and Julian Fierrez IEEE Transactions On Image Processing, Vol. 23, no. 2, February. 2014.

[2] S. Bayram, I. Avcibas, B. Sankur, and N. Memon, “Image manipulation detection,” J. Electron. Imag., Vol. 15, no. 4, May. 2016.

[3] I. Avcibas, N. Memon, and B. Sankur, “Steganalysis using image quality metrics,” IEEE Trans. Image Process., Vol. 12, no. 2, February. 2003.

[4] M. A. Saad, A. C. Bovik, and C. Charrier, “Blind image quality assessment: A natural scene statistics approach in the DCT domain,” IEEE Trans. Image Process., Vol. 21, no. 8, August 2012.

[5] Combining and Selecting Indicators for Image Quality Assessment Proceedings of the ITI 2009 31st Int. Conf. on Information Technology Interfaces, June, 2009.

[6] Z. Wang, A. C. Bovik, L. Lu, “Why is Image Quality Assessment so Difficult?”, in Proc. of Int. Conf. on Acoustics, Speech and Signal Proc, Orlando, Florida, USA, May 2002.

[7] R. F. Zampolo, R. Seara, “A Measure for Perceptual Image Quality Assessment”, in Proc. of Int. Conf. on Image Proc., Barcelona, Spain, September. 2003.

[8] S.Prabhakar, S. Pankanti, and A. K. Jain, “Biometric recognition: Security and privacy concerns,” IEEE Security Privacy, Vol. 1, no. 2, March/April. 2003.

[9] Nesli Erdogmus and Sébastien Marcel,Spoofing Face Recognition With 3D Masks,IEEE Transactions On Information Forensics And Security, Vol. 9, no. 7, July 2014.

[10] L. Jubairahmed, S. Satheeskumaran, and C. Venkatesan, “Contourlet transform based adaptive nonlinear diffusion filtering for speckle noise removal in ultrasound images,” Cluster Computing, vol. 22, no. S5, pp. 11237–11246, Nov. 2017.

[11] T.Thamaraimanalan, D.Naveena, M.Ramya & M.Madhubala, (2020) “Prediction and Classification of Fouls in Soccer Game using Deep Learning”, Irish Interdisciplinary Journal of Science & Research, Vol. 4, Issue 3, pp 66-78.

[12] L. J. Ahmed, “Discrete Shearlet Transform Based Speckle Noise Removal in Ultrasound Images,” National Academy Science Letters, vol. 41, no. 2, pp. 91–95, Apr. 2018.

[13] G. Rajesh Hien Dang, K. Martin Sagayam, S. Dhanasekar, "Image Fusion based on Sparse Sampling Method and Hybrid Discrete Cosine Transformation", International Journal of Scientific and Technology Research, vol.8, no.12, pp.1103-1107, December 2019.

[14] V.V.Teresa, "Low Power Optimization of Finite Impulse Response Filter Feature Extraction by Using Thyroid Cancer Region Identification in Medical Images", Journal of medical imaging and medical sciences, vol.9, pp.99-107, 2020.