Multidisciplinary Journal for Applied Research in Engineering and Technology (MJARET)

Vol. 1 Issue 2, September – 2021, Pages: 1-4

Personal Identity Identification and Authentication Statistics Based on Countermeasures against Spoofing

T. Thomas Leonid
M. Mary Grace Neela
Received: 25 August 2021 / Accepted: 18 September 2021

Abstract:

To make the online banking system secure, a three-step authentication method using the face, iris, and fingerprint is used. To improve security, spoofing detection has also been included. A spoofing attack happens when someone attempts to impersonate someone else and gets unauthorized access. The face and iris are captured by the camera, while the fingerprint is captured by the fingerprint module. Gray Level Co-occurrence Matrix is used to extract a picture of a person's face, iris, and fingerprint (GLCM). A reference module is constructed using the extracted picture so that the input may be compared to it, and if the input matches the module, a one-time password (OTP) is delivered to the user's mobile phone. Only the online transaction may take place if the OTP is entered correctly. Otherwise, the account holder will get an alert message. This method allows for a very secure online transaction.
Keywords— Spoofing detection, face, iris, fingerprint, image extraction, Gray Level C-occurrence Matrix, reference module.

1. INTRODUCTION

Human biometric characteristics are increasingly frequently utilised for identifying and authenticating people. It's utilised in surveillance, security, and access control systems. Data collection methods for importing and processing data have become more efficient because of enormous technological advancements. With the advancement of technology, different spoofing attack strategies to counterfeit these biometric systems are also being created. There are numerous techniques to fake biometric systems. Direct and indirect attacks are the two most common methods. Synthetic biometric samples are produced and utilised to spoof the system in a direct assault. Deep knowledge of the system is necessary in an indirect assault, for example, the algorithm used for matching, the method used for feature extraction, database access, and also the system's vulnerabilities. We used spoofing detection for all three extracted characteristics of iris, face, and fingerprint to develop a trustworthy biometric system. The present system lacks spoofing detection in addition to the three-step authentication that we used here to ensure secure online banking transactions.

✉ *T. Thomas Leonid*

thomasleonid@gmail.com

[1] *Asst Prof, Department of ECE, KCG College of Technology*
[2] *Asst Prof, Department of ECE, TJS institute of Technology*

2. RELATED WORKS

We will review some of the existing antispoofing works for iris, face, and fingerprint in this part.

A.IRIS SPOOFING:

The feel of color contact lenses with someone's iris pattern printed on them can be used to determine iris liveness. Image quality was assessed, and the best characteristics, such as focus, motion, and pupil dilation, were chosen, and then a well-known classifier was employed to make a choice. In conclusion, picture quality measurements and texture pattern were used to develop Iris anti-spoofing techniques. The solutions differ depending on the dataset. Deep analysis of the pattern is used to extract the characteristics.

B.FACE SPOOFING:

There are four Face anti-spoofing methods:

Techniques that rely on additional devices, approaches that rely on user participation, and data-driven characterization methods are all examples of user behavior modelling. LBP is utilized to capture micro-texture patterns that are employed in the creation of forged biometric samples. To differentiate between false and real biometric data, the color, texture, and form of the face are recorded and combined using a Partial Least Square (PLS) classifier. The use of visual analysis to gather temporal information on face

spoofing during video playback assaults was also proposed.

Image quality measurements and texture pattern were also used in face anti-spoofing techniques. The characteristics are extracted straight from the input.

C.FINGERPRINT SPOOFING:

There are two types of fingerprint spoofing attacks: hardware-based and software-based. Ridge strength, ridge clarity, ridge integrity, and ridge continuity may all be used to identify liveness in fingerprints. The pores and texture of the skin are used to identify fake biometric fingerprint samples. Gelatin fingerprint samples are an example of a false sample. The fingerprint sensors in hardware-based methods are faulty, allowing even false samples to get through. Deep learning algorithms are used to evaluate fingerprint samples. Tsai C. A. et al. (2012) present a new planar compact eye-shaped Ultra Wide Band (UWB) antenna based on an eye ball-shaped patch supplied by a 50-Ohm microstrip line in [4]. This antenna's core delivers a good efficiency and gain of around 85 percent to 90 percent. The etched ground plane functions as a reflector, which is an important factor in increasing directivity. A planar antenna with low return loss, near constant group delay, improved directivity, and a good radiation pattern can be made along these lines.

2. METHODOLGY

For authentication, the current method employs the face, fingerprint, and iris independently. However, we've utilised all three for online banking authentication. The fingerprint of a person is first taken using a fingerprint scanner, such as the HR5Z5C that we are utilising. As a result, we'll need a TTL to USB converter to connect it to the Raspberry Pi. This scanner may now be used to obtain a person's fingerprint. The camera is then used to capture the face and eye. This is used to generate a database, and then iris recognition is performed using MATLAB on the recorded eye. After that, the pictures of the face, fingerprint, and iris are extracted. The picture is extracted with the help of python and openCV. Denoising the image first using a filter, then scaling it by making the value of row equal to column. The RGB is then transformed to grey scale. To transform the 3d array matrix into a 2d array matrix for our convenience, we must convert it. The array will then be generated using the GLCM method. The array will be created by distinguishing the row and column, and then noting the row and column locations. The 2d array matrix is then used to extract the values of

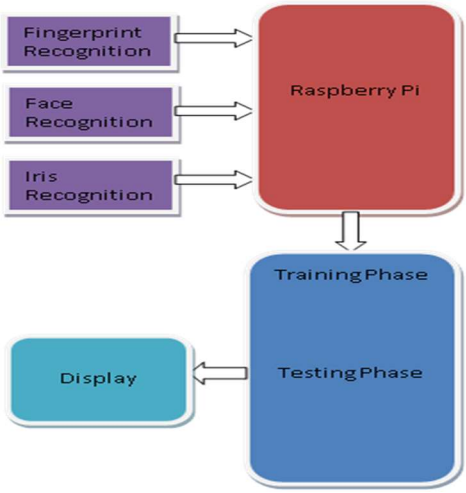

Figure 1: Block diagram

energy, entropy, contrast, correlations, and homogeneity. An array is formed using these functions. And the retrieved picture value is known to be in this array. The reference module is made out of pictures of numerous people's fingerprints, faces, and iris. The name of the individual will be in the reference module, and inside each person's name will be extracted pictures of their face, iris, and fingerprint.

The next step is to match the inputs. After that, the input is compared to the reference module. Fisher Recognizer is the algorithm used for face recognition. The input is a picture of a person's face. After that, the image is resized and transformed to grey scale. The picture is then extracted with the GLCM method. After that, the input is compared to the reference module using the Fisher Recognizer method. Because certain values may be concealed during comparing, back propagation is used to ensure that the input is compared to all of the values in the reference modules. It will check for spoofing attacks if the input matches any of the person details in the reference module. If spoofing is used, the message will read "ILLEGAL ACCESS." Otherwise, the authentication process moves on to the next stage.

The input for fingerprint is then obtained from a fingerprint scanner connected to the Raspberry Pi board. After that, the input picture is retrieved using the GLCM technique after it has been resized and converted to grayscale. A comparison is made between the retrieved picture and the reference module. After back propagation is finished, the input must be matched with the same person's name that was

used for facial recognition. If this isn't the case, the result will be labelled "NOT AUTHENTICATED." If the input matches that of the same individual, the system will check for spoofing and show "ILLEGAL ACCESS" if spoofing is detected. Otherwise, the authentication process moves on to the next stage.

The next step of authentication is using iris. In this project we have just provided the iris recognition using MATLAB code and not checked using real time approach. The image which is already present in the database is given as input. After that, the input is compared with reference module. After back propagation is finished, the input must be matched with the same person's name that was used for facial recognition. If this isn't the case, the result will be labelled "NOT AUTHENTICATED." If the input matches that of the same individual, the system will check for spoofing and show "ILLEGAL ACCESS" if spoofing is detected. Otherwise, the authentication process moves on to the next stage.

3. EXPERIMENTAL RESULTS

The experimental assessment of the suggested system is detailed in this section. Figures 2 and 3 demonstrate the picture resizing and conversion of RGB to grayscale images, respectively.

Figure 2

Figure 3

Figures 4 and 5 show the pictures of the face and eye recorded by the camera, respectively. These pictures are just for one individual. Because the individual will not be in the same posture each time he comes in front of the camera, 30 photos are captured for a single person.

Figure 4

Figure 5

Figures 6 and 7 illustrate the fingerprint and iris images that were utilized to create the reference module, respectively. Only the region of interest will be seen in the pictures.

Figure 6

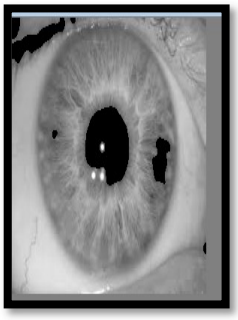

Figure 7

In the output screen, the extracted picture value will be shown. And it will look like figure 8 in the image below.

```
[ 6.41785826e-01   6.05920439e+02
6.65120351e-01   9.04503025e+02
  8.19496889e-01   1.78851266e+01
3.01209166e+03   2.09150127e+00
  2.79235505e+00   2.53835966e-03
1.85350432e+00  -3.03545357e-01
  7.93345350e-01]

[[ 8.91339953]] [[ 30.03020606]]
```

Figure 8

The retrieved pictures of numerous people will be detailed in the reference module. The input is then supplied, and a comparison is made. If the input matches the comparison, it will be shown as "AUTHENTICATED." Otherwise, the message "NOT AUTHENTICATED" will appear. Figures 9 and 10 exhibit the pictures of both verified and non-authenticated documents, respectively.

Figure 9

Figure 10

If a spoofing attempt is identified in any of the authentication steps, the message “ILLEGAL ACCESS” will appear, as illustrated in Figure 11.

4. CONCLUSION

The approach presented above allows for enhanced security in online transactions. Three-step authentication is used to safeguard the online

transaction. Fingerprint, face, and iris authentication make up the three-step authentication process. Attacks based on spoofing are also avoided. The model number for a fingerprint scanner that must be interfaced with the Raspberry Pi board is different, and it is more expensive. However, we utilized a low-cost scanner and connected it to a Raspberry Pi board through a converter. The iris is taken from the person's eye picture. Furthermore, this project does not have real-time authentication.

Iris capturing scanners can be used to capture a person's iris for future work. It is possible to do iris authentication in real time using this method. As a result, security will be enhanced even more.

References

[1] Gustavo B. Souza, Daniel F. S. Santos2, Rafael G. Pires1, Aparecido N. Marana2, Joao P. " Deep Boltzmann Machines for Robust Fingerprint Spoofing Attack Detection using Deep Boltzmann Machine". Citation information: 978-1-5090-6182-2/17/$31.00 ©2017 IEEE transactions on Information Forensics and Security.

[2] Jukka Mtitittti, Abdenour Hadid, Matti Pietiktiinen, "Face spoofing detection from single images using micro-texture analysis." Citation information: 978-1-4577-1359-0111/$26.00 ©2011 IEEE transactions on Information Forensics and Security.

[3] Santosh Tirunagari, Norman Poh, David Windridge, Aamo Iorliam, Nik Suki, and Anthony T.S. Ho. "Detection of Face Spoofing Using Visual Dynamics." Citation information: DOI

10.1109/TIFS.2015.2406533, IEEE Transactions on Information Forensics and Security.

[4] Shervin Rahimzadeh Arashloo, Josef Kittler and William Christmas. "Face Spoofing Detection Based on Multiple Descriptor Fusion Using Multiscale Dynamic Binarized Statistical Image Features." Citation information: DOI

10.1109/TIFS.2015.2458700, IEEE Transactions on Information Forensics and Security.

[5] M. Fons, F. Fons, and E. Cantó.A. "Fingerprint Image Processing Acceleration Through Run-Time Reconfigurable Hardware" IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—II: EXPRESS BRIEFS, VOL. 57, NO. 12, DECEMBER 2010.

[6] Chenhao Lin, Ajay Kumar, "Tetrahedron Based Fast 3D Fingerprint Identification Using Colored LEDs Illumination." DOI 10.1109/TPAMI.2017.2771292, IEEE Transactions on Pattern Analysis and Machine Intelligence.

[7] YANN LECUN, MEMBER, IEEE, LEON BOTTOU, YOSHUA BENGIO, ´ AND PATRICK HAFFNER, "Gradient-Based Learning Applied to Document Recognition." PROCEEDINGS OF THE IEEE, VOL. 86, NO. 11, NOVEMBER 1998.

[8] Timo Ojala, Matti PietikaÈinen, Senior Member, IEEE, and Topi MaÈenpaÈa, "Multiresolution Gray-Scale and Rotation Invariant Texture Classification with Local Binary Patterns." IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, VOL. 24, NO. 7, JULY 2002.

[9] David MenottiY, Member, IEEE, Giovani ChiachiaY, Allan Pinto, Student Member, IEEE, William Robson Schwartz, Member, IEEE, Helio Pedrini, Member, IEEE, Alexandre Xavier Falcao, ˜ Member, IEEE, and Anderson Rocha, Member, IEEE. " Deep Representations for Iris, Face, and Fingerprint Spoofing Detection." IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 10, NO. 4, APRIL 2015.