# PRIVACY PRESERVING CLOUD BASED FACE RECOGNITION WEB PORTAL

Răzvan-Daniel ALBU
University of Oradea, Faculty of Electrical Engineering and Information Technology, Romania, E-mail: ralbu@uoradea.ro

ABSTRACT: Regardless of the significant progress in face recognition algorithms, current systems are still defenceless to spoof attacks. Several anti-spoofing approaches have been proposed to control if there is a living individual or an artificial duplication, in front of the camera. So far, well-organized safety methods against this threat have proven to be a thought-provoking mission. In this paper, I present a web application I developed for IsItYou, a company from Israel, that tries to approach this issue creating a reliable and secure BEWARE (Biometric Early Warning Rating Engine) solution.

KEYWORDS: web services, face recognition, liveness detection, BEWARE

## 1. INTRODUCTION

IsItYouWebDemo is a web application I have developed for a company from Israel named IsItYou Ltd [1]. The main goal of IIY is to develop a reliable and secure BEWARE (Biometric Early Warning Rating Engine) solution that can replace passwords. As current research trends show, passwords are things of the past and face biometrics are taking their place. But the main problem of all face based authentication systems is security. They are not secure since anyone can take a photo of you, from a social network, and log in with that photo into your bank account protected with such a system. The need of a solution that can determine if the user is a real human or not, is mandatory to turn biometric into a real thing. After 5 years of research, development and testing, in 2017, IIY released a new solution that can solve this challenge. The main advantages of this technology are:

- It is convenient and simple, the user needs just to take a selfie, and we already live in a world of selfies.
- It is reliable since it has a multi-layered architecture to determine if a user is a real human or not, so there is no single point of failure.
- It is engine agnostic, it can be added to any other already existing face recognition systems.

You can see demo videos with this technology, how it works on mobiles, and how it can detect various spoof attempts, in [2, 3]. As you will see, IIY engine can detect spoof attempts made by using a high-resolution TV screen, other mobile device, a printed copy of your face or even using a 3D mask.

## 2. LIVENESS DETECTION METHODS

Searching the literature, I have identified various live detection approaches. Here I will mention some of them that I and the IIY team studied while developing the unique BEWARE solution.

- Frequency and Texture based analysis: Here the main assumption is: images taken from the 2D objects tend to suffer from the loss of texture information compared to the images taken from the 3D objects. Using description methods based on Local Binary Pattern (LBP), we tried to analyse the textures on the given facial images for extraction of the frequency information, and the image was converted into the frequency domain with help of Fourier transform.
- Variable Focusing based analysis: The key approach is to use the variation of pixel values by focusing between two images sequentially taken in different focuses of the camera. We tried to find the difference in focus values between real and fake faces when two sequential images are collected from each subject. In case of real faces, focused regions should be clear. In contrast, there is little difference between images taken in different focuses from a printed copy of a face, because they are not solid.
- Movement of the eyes based analysis: This is a method very popular in literature, but in real life is easy to spoof by simulating fake eye movement so we do not waste much time on it. Here the assumption is that because of blinking and uncontrolled movements of the pupils in human eyes, there should be big shape variations in sequential input images of same person. Well, our experiments

showed this is not a very solid assumption and not true.

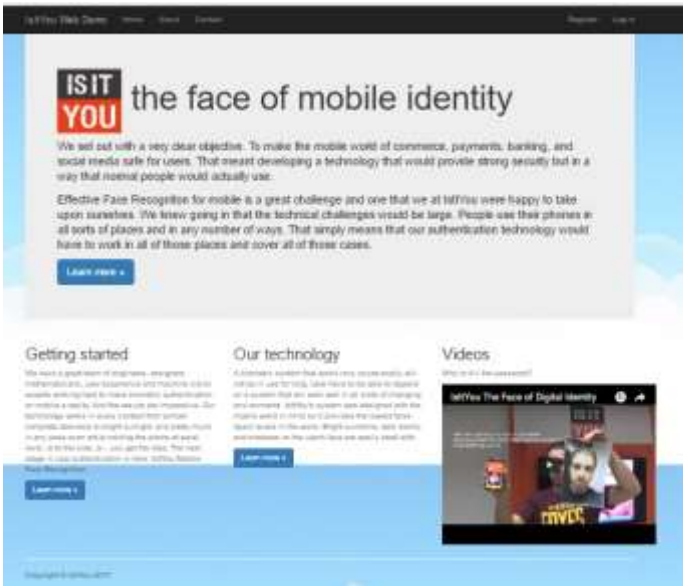
- Optical Flow based analysis: The motion of optical flow field is a combination of four basic movement types: translation, rotation, moving and swing. Here the key element is swing. Swing creates the actual differences in optical flow field of fake and real images. But we wanted a method that uses a single image, and here is required a short video.
- Blinking based analysis: Some authors used Conditional Random Fields (CRFs) to model blinking activities. Here is also required a video, a single image is not enough, and there are many YouTubes that show how to simulate fake blinking and spoof Google blinking based implementation.
- 3D Face Shape based analysis: Here the lack of surface variation in the scan is one of the key evidence that the acquisition comes from 2D source. Based on the computation of the mean curvature of the surface, a simple and fast method can be implemented to classify fake/real images. Another idea is that structures recovered from real faces usually contain sufficient 3D structure information, while structures from fake faces are usually planar in depth. A simple algorithm will do the following steps:

1. From a given sequence of images which are captured from more than two viewpoints, facial landmarks are detected and key frames are being selected.
2. From the selected key frames, the sparse 3D facial structures are recovered.
3. A SVM classifier is trained to differentiate living faces from fake faces.

I also published some research papers about a new method I developed, based on Radon transform. My innovative method uses Radon transform to generate a signature for an image, and then compares signatures of fake/real images and tries to classify them. And we tried also many other methods like: colour analysis, context based analysis, and ensemble base combination of standard techniques [3,4]. All methods have advantages and disadvantages, for example texture based methods do not require user collaboration, but there are also images with low texture information. Motion based methods are hard to be spoofed by 2D images, but requires a video. Methods that search for life signs require user collaboration, a short video to be acquired, but are independent of texture.

## 3. IMPLEMENTATION AND FUNCTIONALITY

IsItYouWebDemo can be accessed using [6]. The main page is displayed in figure 1 and contains a YouTube video demonstrating anti-spoofing capabilities of IIY technology.



We set out with a very clear objective. To make the mobile world of commerce, payments, banking, and social media safe for users. That meant developing a technology that would provide strong security but in a way that normal people would actually use.

Effective Face Recognition for mobile is a great challenge and one that we at IsItYou were happy to take upon ourselves. We knew going in that the technical challenges would be large. People use their phones in all sorts of places and in any number of ways. That simply means that our authentication technology would have to work in all of those places and cover all of those cases.

**Figure 1.** IsItYouWebDemo home page

IsItYouWebDemo is an MVC 4 application deployed on Azure Cloud, and developed with .NET framework version 4.6.1. This web application allows a user to test and play with IIY technology, inside a web browser. To be able to access face recognition application, a user need to register and then log in. Registration is simple, it can be accessed from top menu bar, it requires a valid email address and a password to create an account. If a user does not want to create an account on IsItYouWebDemo database, there are also other available option, the user can choose to log in using a Facebook, Twitter or Gmail account.

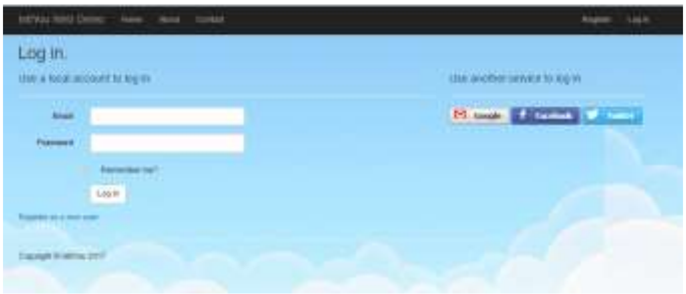


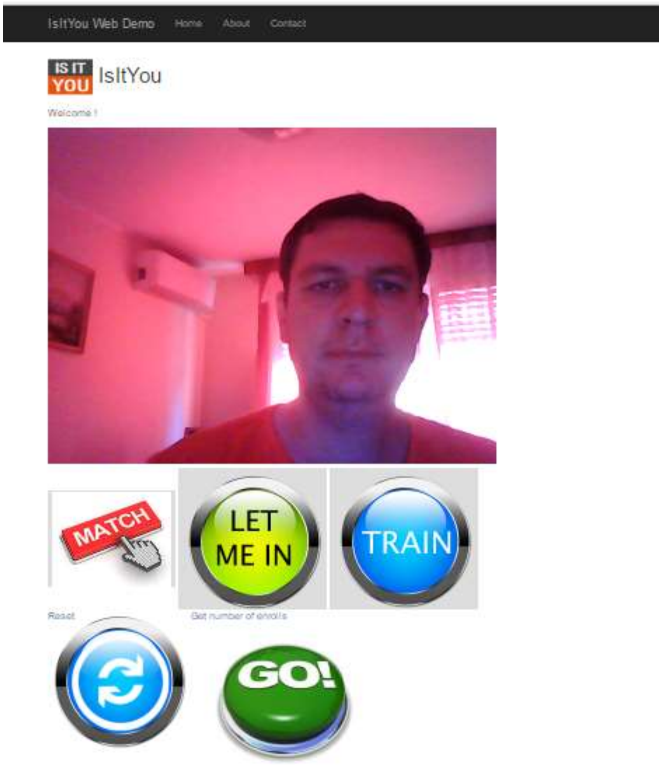
**Figure 2.** IsItYouWebDemo log in page

To implement this feature, I used OWIN NuGet package. OWIN defines a standard interface between .NET web servers and web applications.

The goal of the OWIN interface is to decouple server and application, encourage the development of simple modules for .NET web development, and, by being an open standard, stimulate the open source ecosystem of .NET web development tools [7]. Then, I created Google, Twitter, and Gmail apps for OAUTH2 and I connected them to my application. OAuth 2 is an authorization framework that enables applications to obtain limited access to user accounts on an HTTP service, such as Facebook. It works by delegating user authentication to the service that hosts the user account, and authorizing third-party applications to access the user account. OAuth 2 provides authorization flows for web and desktop applications, and mobile devices [8]. To create a Google app, I used Google development console, and I obtained an APPID and an APPSECRET. Those keys I used as parameters to UseGoogleAuthentication method called inside ConfigureAuth from my MVC application.

```
app.UseGoogleAuthentication(clientId:"000-
000.apps.googleusercontent.com",        clientSecret:
"00000000000");
```

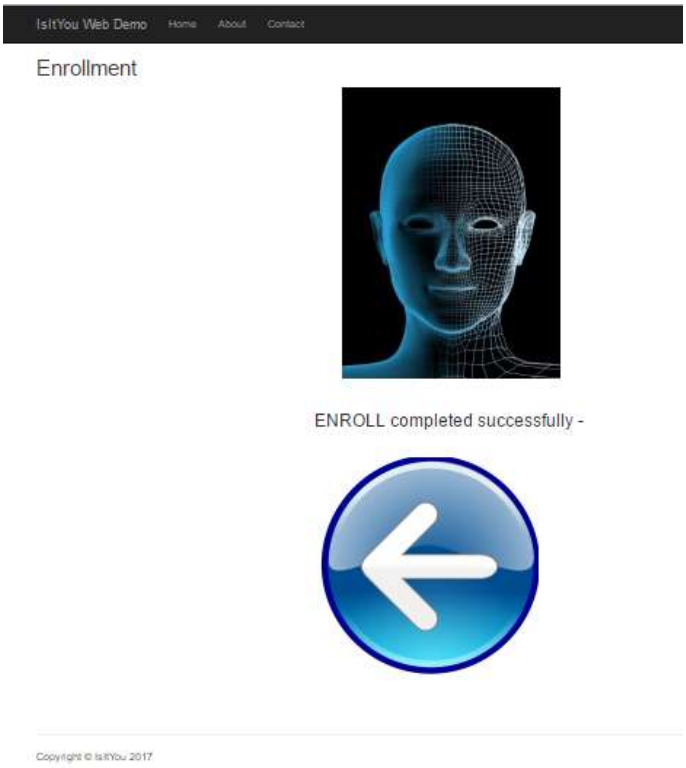
Using a similar procedure, I implemented OAuth2 apps for Twitter and Facebook. Detailed info on how to implement those apps can be found in [9]. After logging in, the user can access IsItYouWevDemo menu option from the top bar, the laptop camera will start, and will see the page in figure 3.



Welcome !

**Figure 3.** IsItYouWebDemo in action

Here the user can test IIY technology by pressing on of the following buttons: Match, Let Me In, Train, Reset, or Go. If the user is here for the first time, the first step is to create some biometric templates with his face, using Train button. The user just looks at the camera, presses Train button and if the IIY engine can find his/her face, the following screen will appear (Figure 4).



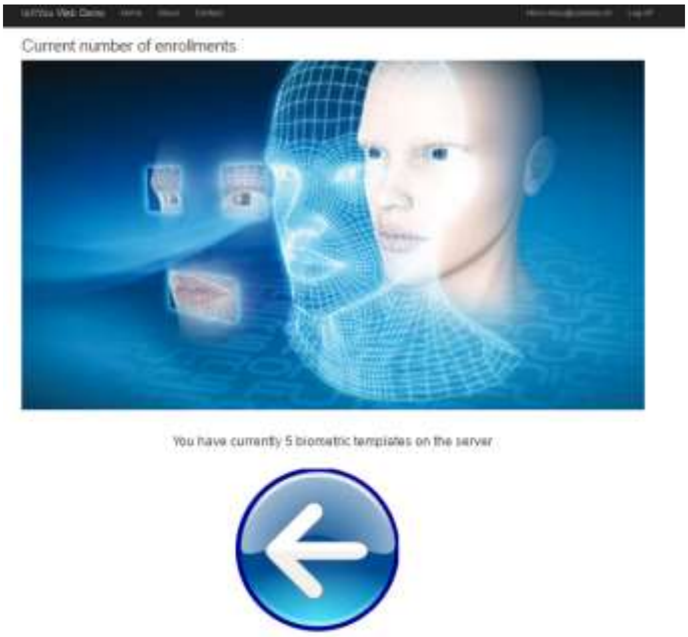
Enrollment

ENROLL completed successfully -

Copyright © IsItYou 2017

**Figure 4.** Enrolment process

To check how many biometric templates already exists on the server, a user will press the Go button and will see a screen like this (figure 5).

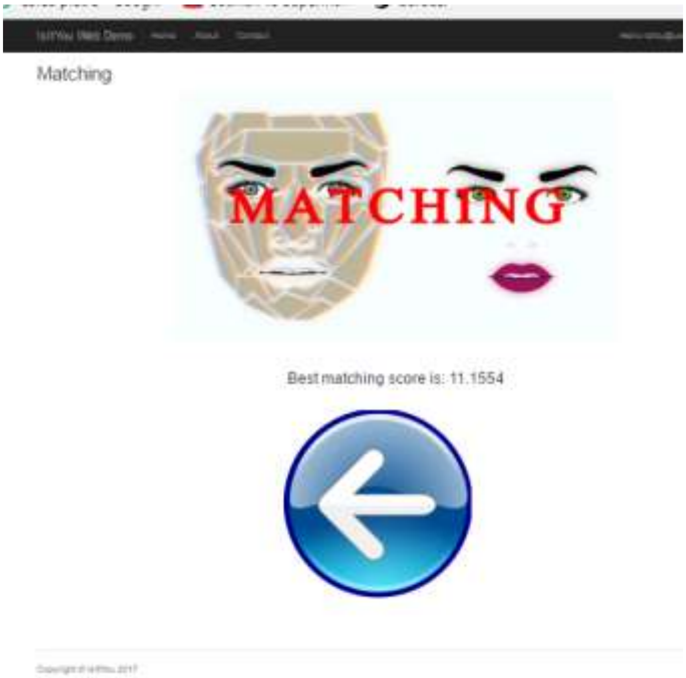


Current number of enrollments

You have currently 5 biometric templates on the server

**Figure 5.** Getting the number of existing templates for a user

After the user has at least one biometric template of his/her face on the server, the Match and Let me in operation will make sense. Matching means the generation of a biometric template, for a given image of the user and the comparison of this template with all already existing templates. The result of this comparison will be a matching score (figure 6).

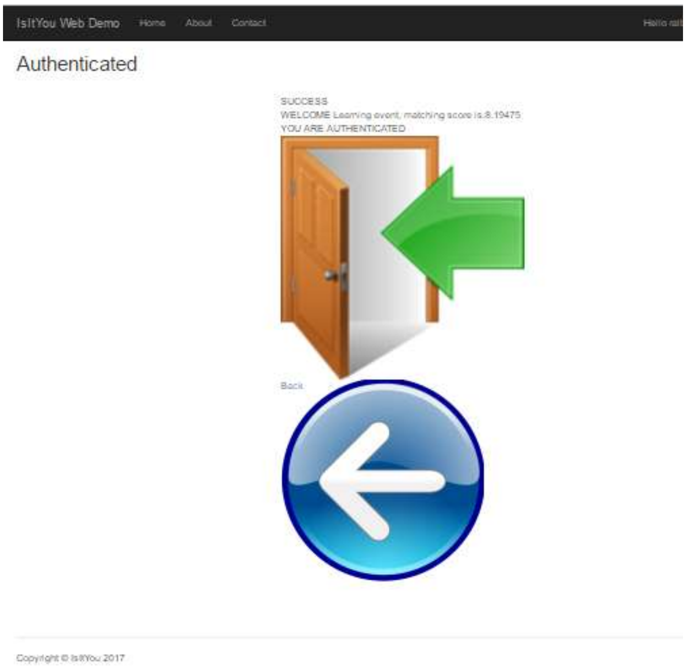


Best matching score is: 11.1554

Copyright © IsItYou 2017

**Figure 6.** Matching process

Let me in operation is more complex, will perform a matching and other anti-spoofing tests, and if the user is a real human, will return a page like in figure 7.



SUCCESS
WELCOME Learning event, matching score is:8.19475
YOU ARE AUTHENTICATED

Copyright © IsItYou 2017

**Figure 7.** Let me in process

## 4. EXPERIMENTS AND RESULTS

In my experiments, I utilized of the following image data bases, to evaluate the face recognition performances:

- The NUAA Photograph Database [9] was built making use of quite a few generic cheap webcams. They have created this database in three sessions with about 2 weeks' interval between two sessions, in diverse places and illumination. 15 subjects were part of this work.
- JAFFE the Japanese Female Facial Expression [10] that holds 213 images of 7 facial expressions posed by 10 Japanese female models.
- The Facial Recognition Technology (FERET) Database [11] corpus consists of 14051 eight-bit grayscale images of human heads with views fluctuating from frontal to left and right profiles.
- PUT Face Database [12], is available for research purposes, containing almost 10000 hi-res images of 100 people. Images were taken in controlled conditions and the database is supplied with additional data including: rectangles containing face, eyes, nose and mouth, landmarks positions and manually annotated contour models. In table 1 are summarized the face recognition engine results.

TABLE I.
SUMMARY PERFORMANCES

| **Database name** | **Performances** | | |
|---|---|---|---|
| | ***No of enrolls per person*** | ***Average FAR% / FRR%*** | ***No of identification attempts*** |
| NUUA<br>15 subjects | 5 | 4.23% / 5.45% | 150 |
| JAFFE<br>10 subjects | 5 | 4.33% / 5.54% | 100 |
| FERET<br>20 subjects | 5 | 5.66% / 5.84% | 200 |
| PUT<br>100 subjects | 5 | 8.5% / 4.12% | 100 |
| NUUA<br>15 subjects | 10 | 2.82% / 3.35% | 150 |
| JAFFE<br>10 subjects | 10 | 3.32% / 4.54% | 100 |
| FERET<br>20 subjects | 10 | 1.26% / 2.84% | 200 |
| PUT<br>100 subjects | 10 | 4.5% / 5.32% | 100 |

For each subject of a database I performed 2 set of tests, with 5 and 10 images of that person enrolled. Each test is made using the number of identification attempts specified in the last column. The test images are random selected from each database. The number of subjects in each database is also specified in first column of the table. After each subject test, the obtained FAR (False Acceptance Rate) and FRR (False Rejection Rate) are computed [13, 14, 15].

After testing all subjects from a database, an average FAR and FRR are also computed and shown in second and third column. In table 2 are presented the best performance (in terms of accuracy) obtained for each database.

TABLE II.

BEST PERFORMANCES

| Database name | Accuracy |
|---|---|
| NUUA | 93.83% |
| JAFFE | 92.14 % |
| FERET | 95.9% |
| PUT | 90.18% |

## 5. CONCLUSIONS

In this paper, I have presented the implementation of an MVC 4 application with face recognition and liveness detection capabilities. IsItYouWebDemo can detect various spoof attempts like a printed copy of your face, screens of various devices such as smart phones and TVs, and even 3D masks. IsItYouWebDemo offers a flexible login system and is a perfect demo tool that can be consumed by anyone inside a web browser. IsItYouWebDemo is hosted on Azure Cloud, and it consumes a SOAP web service named ARGOS, to perform all biometric functions. The presented results demonstrate it has a high face recognition capability, tested on 4 different public databases. The best results, the highest accuracy was obtained on Facial Recognition Technology (FERET) Database. In this research work I tested only the face recognition performances, and the anti-spoofing capabilities will be analyzed and measured on a separate research work.

## 6. REFERENCES

1. http://www.isityou.biz/ [June 2017]
2. https://youtu.be/SjOQkud889g [June 2017]
3. https://youtu.be/xHGl6SaB-RA [June 2017]
4. ALBU Razvan-Daniel, „Face recognition using Radon transform”, 21st International Symposium for Design and Technology in Electronic Packaging (SIITME), 22–25 October 2015, Brașov, Romania, Page(s): 103 - 106, ISBN: 978-1-5090-0332-7.
5. 24. ALBU Razvan-Daniel, „Face anti-spoofing based on Radon transform”, 13th International Conference on Engineering of Modern Electric Systems (EMES), 2015 , Oradea 11-12 June 2015, Pages: 1 – 4, DOI: 10.1109/EMES.2015.7158435, IEEE Conference Publications, Print ISBN:978-1-4799-7649-2,.
6. https://isityouwebdemo.azurewebsites.net/ [June 2017]
7. http://owin.org/ [June 2017]
8. https://www.digitalocean.com/community/tutorials/an-introduction-to-oauth-2 [June 2017]
9. https://docs.microsoft.com/en-us/aspnet/mvc/overview/security/create-an-aspnet-mvc-5-app-with-facebook-and-google-oauth2-and-openid-sign-on#goog [June 2017]
10. http://parnec.nuaa.edu.cn/xtan/data/nuaaimposterdb.html [September 2015].
11. http://www.kasrl.org/jaffe.html [September 2015].
12. http://www.itl.nist.gov/iad/humanid/feret/feret_master.html [September 2015].
13. https://biometrics.cie.put.poznan.pl/ [August 2015]
14. M. Curilă, S. Curilă, O. Novac, Mihaela Novac, “A new Artificial Vision Method for Bad Atmospheric Conditions”, International Joint Conferences on Computer, Information, and Systems Sciences, and Engineering (CIS2E 08), December 5 - 13, 2008, USA, no. 292, Publisher: Springer-Verlag Berlin, Germany, Pages: 227-331, Published: 2010, ISBN: 978-90-481-3659-9.
15. D. Nuzillard, S. Curilă, M. Curilă, “Blind Separation in low frequencies using Wavelet analysis, Application to artificial vision “, Fourth International Symposium on Independent Component Analysis and Blind Signal Separation, pp. 77 - 82, Avril 1-4, 2003, Nara, Japan, ISBN 4-9901531-1-1, ICA2003 Proceedings.
16. Sorin Curilă, Cornelia E. Gordan and Mircea Curilă, “Tracking of polyhedral objects in image sequences”, 2008 IEEE 4th International Conference on Intelligent Computer Communication and Processing (ICCP 2008), August 28-30, 2008, Cluj-Napoca, Romania, Page(s):61 – 66, ISBN: 978-1-4244-2673-7.