Project Proposal

Project Proposal	March 2017	Note:

Student to complete this section						
Mills	**DSM.**	**Mr.**	**13081650**			
Biometric vehicle immobilizer based on driver facial features			**Study leader: Dr. HC. Myburgh**			
Class group: English		**Project number:**	HCM6	Revision number:	1	
Type of project: Design		Degree programme enrolled for: Computer Engineering				
Student declaration: I understand what plagiarism is and that I have to complete my project on my own.		______________ Student signature		____________ Date		

Declaration by language editor (proofreader)	
I have been allowed adequate time to read this document carefully and to make corrections where necessary (date received indicated below). To the best of my knowledge, correct formatting, spelling and grammar are used throughout the document.	
______________________________ DS Mills (language editor)	___________ Date

Declaration and recommendation by study leader		
1. Have you (the study leader) been allowed adequate time to read and comment on the Project Proposal?	Yes	No
2. Is the Project Proposal a <u>correct</u> and <u>complete</u> description of what is required?	Yes	No
3. Is the Project Proposal <u>clear</u> and <u>unambiguous</u>?	Yes	No
4. Recommendation: Do you recommend that the Project Proposal be approved?	Yes	No
______________________________ Dr. HC Myburgh (Study leader)	___________ Date	

This section to be used by the Project lecturer					
Content /20		Attended lectures:	Yes	No	
Subtract for editing errors /10		Language editing adequate:	Yes	No	
Final mark /20		Approved? (If "No", a revision must be submitted):	Yes	No	Prof. J.J. Hanekom

1. Problem statement

Motivation.
South Africa is synonymous with a high violent crime rate[1]. In 2015/16 (1^{st} of April 2015 to 31^{st} of march 2016) based entirely on police reports there were 14602 reported carjackings, this being a 14.3 % increase from the previous year [2]. This is only an indication of the reported incidents of car hijacking and does not mention the incidents of truck hijacking. Most modern vehicles have some theft protection in place, however, the theft protection is more in the line of protecting an unwatched vehicle from being stolen then aiding in the prevention of hijacking. Modern vehicles will generally have some sort of central locking mechanism tied to an alarm/immobiliser the problem with the already implemented security measure is the fact that all that is need to not only have access to the interior of the vehicle but drive the vehicle is the set of keys. The implication being if a criminal can obtain the keys for the vehicle then full access will be granted (this includes entering and driving the vehicle). The motivation of this project is to provide motor vehicle owners with an extra layer of security; ensuring their vehicle is only responsive to them and a few trusted people, preventing other unauthorized people accessing their vehicle based on something that cannot merely be stolen, something that is intrinsic and unique to every person, namely their identity. The problem addressed is a facial recognition solution to vehicle security, ensuring that a vehicle may only be driven by the owner of a vehicle and a few trusted people (trusted by the owner).
Context.
Facial recognitions is a very important field in the study of computer vision and has been around for quite some time. Its simple beginnings have now lead into a vast intricate field, and is widely being used today by many different industries. Two notably different examples would be the Federal Bureau of Investigation (FBI) and Facebook (an extremely popular social media website). Approximately half of all adult American face's are stored in facial recognition databases accessible by the FBI [3], these faces are obtained from multiple means; anything from mug shots to passport and drivers license photos. The FBI database is impressive, however, algorithms used for facial recognition are inaccurate about 15 % of the time. Facebook has a much higher recognition accuracy. Their algorithm, Deepface, is extremely accurate and boasts near human accuracy in identifying human faces[4]. A large part of this impressive result is the enormous amount of training data that Facebook has at its disposal. Having a significantly high facial recognition accuracy is achievable thus making facial recognition more viable as a security measure then it was before.
Technical challenge.
The technical challenge of this project is to detect and run a facial recognition algorithm on a potential drivers face. Within this, the system will need to overcome the following challenges: To detect a face from video on a low cost embedded system quickly and accurately, to send that face to an external server implying the system will need to have wireless connectivity that is fast and reliable, to host a server capable of running a facial recognition algorithm and to have a working accurate facial detection algorithm used to recognize a potential driver when the input face is subjected to varying lighting conditions as found in a vehicle.

Limitations.
The proposed system will have the following limitations:

- The system will not work efficiently under adverse lighting conditions; facial recognition algorithms generally struggle when lighting conditions are not optimal. Shadows created on the face may result in poor results. The system will account for this limitation by toggling a light to properly illuminate a potential drivers face.
- The system will not be perfectly accurate. This will always be true for facial recognition. This particular system will suffer more so than most since it will not have large amounts of training data. Accuracy in facial recognition systems are bolstered by the amount of training data.
- The system will not be as accurate when the potential driver is visually expressing emotion, this could be a broad smile or large frown. This is a limitation of facial recognition and can only be solved with large amounts of training data.
- The system will not be effective if the owner of the vehicle face significantly changes, due to injury or excessive facial hair growth for instance.
- The system will not be able to work at night. The system will need a certain range of lighting conditions to work, the absence of light will mean that the system will be unable to detect a person's face and subsequently send that face back to the server for recognition.

2. Project requirements

ELO 3: Design part of the project

The project will be a facial recognition system that is made up of two parts, namely a prototype of an immobiliser and a server. The prototype is what would be built into the vehicle and the server is where the facial recognition algorithm will train and verify users. The overall system should show that it would be possible to implement a car immobilizer based on the drivers facial characteristics

2.1 Mission requirements of the product

The following mission requirements should be met by the proposed system(the system is made up of two parts the prototype of the car immobiliser and the server).

- The prototype has to determine when the door has been opened and closed. This is indicative of a change in state and the system should now verify that the person attempting to drive the vehicle is indeed authorized to access this vehicle.
- The prototype will use a camera to record the area where a potential driver will be. This recording will be used to determine the identity of the driver.
- The prototype will make use of the video obtained by the camera and detect a face. This face will then be isolated from the rest of the video and the rest of the video will be disregarded.
- The prototype and server will need to communicate wirelessly over the Internet both sending and receiving information.
- The prototype will be implemented on a small low cost embedded device. The device used will be Raspberry Pi 3 Model B SBC.
- The server will receive an image from the prototype and a message to train the network on that particular face or to verify the identity of that face. It will be capable of both those tasks. Once completed a message with the outcome will be sent back to the prototype
- The server will be run a facial recognition algorithm to verify the potential driver of the vehicle. Determining if the driver is allowed to start the vehicle or not.
- The server will consist of a neural network that will need to be trained. This training will enable the network to determine the identity of a potential driver.

2.2 Student tasks: design

The following items will need to be designed.

- A method for the system to determine when the driver's side door has been opened and subsequently closed.
- A method for the system to isolate a potential driver's face from the video obtained using a facial detection algorithm.
- A method to determine if a driver is a valid one or not. A facial recognition algorithm will be used to accomplish this task. The algorithm will need to be trained to recognize a face.
- A method to achieve wireless communication between the prototype and server.

ELO 4: Investigative part of the project

2.3 Research questions

The following questions will need to be dealt with.

- What is an adequate internal neural network structure when the network should recognize faces?
- How many hidden layers should be used?
- How much training data will be required to train the network to an adequate accuracy?
- How much of an effect will shadows have on the systems ability to perform facial recognition?

2.4 Student tasks: experimental work

The following experimental work will be done:

- Train neural networks that have been coded with slightly different internal structures and record results.
- Train neural networks that contain a varying amount of hidden layers and record the results.
- Using the various trained networks attempt to recognize a face and record accuracy.

3. Functional analysis

The system will have both hardware and software components and each will be given functional units. Figure 1 is a representation of the overall hardware functional units.

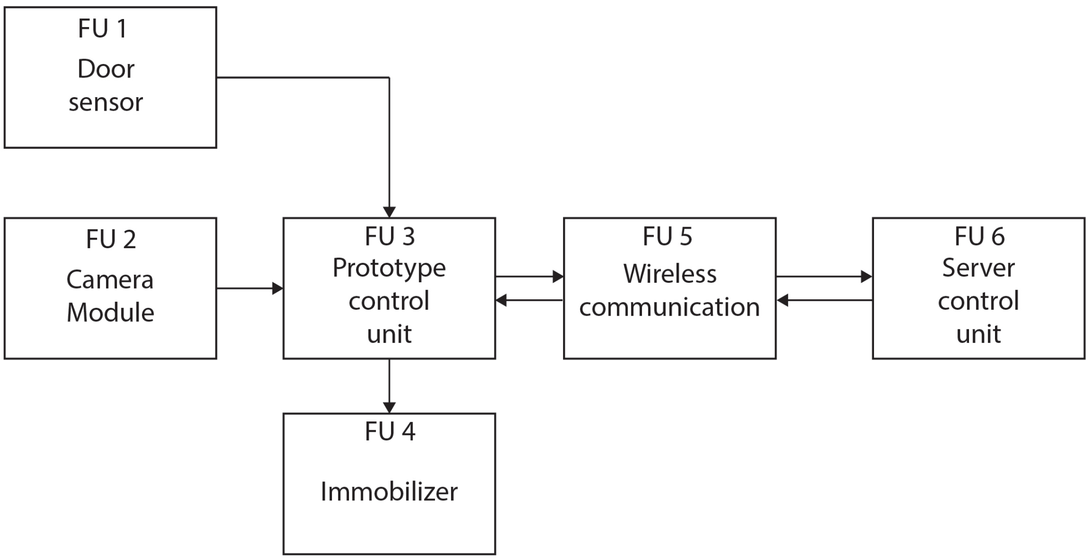

Figure 1. Functional unit diagram of the system's hardware

The prototype control unit [FU 3] will start by waiting for information from the door sensor [FU 1]. This information will indicate that the drivers side door has been opened and closed. Once the door has been opened and closed the prototype control unit initializes the system and waits for a video stream from the attached camera module [FU 2]. The system wirelessly sends information [FU 5] to the sever control unit [FU 6] where that information is processed by the server. The server will then need to respond once ready using the same wireless communication [FU 5]. Upon receiving the information from the server the system ensures that the car may or may not be started by the driver currently sitting in the drivers seat [FU 4].The software portion of the system will reside inside [FU 3] and [FU 6] (the prototype and server respectively). The prototype control unit is the embedded system whereas the server control unit is the externally hosted server. Figure 2 is a representation of the high level software functional units for the prototype.

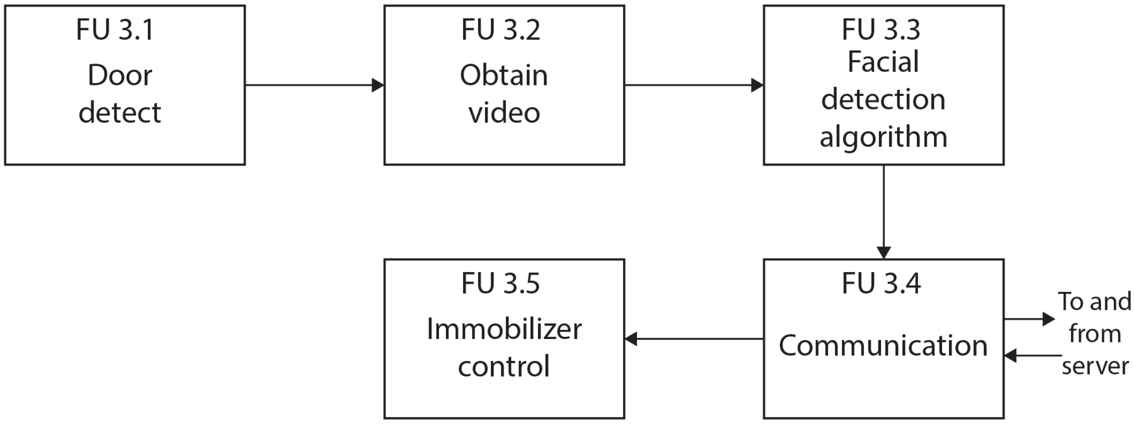

Figure 2. Software functional unit diagram of the prototype control unit

The prototype will wait for the door to be opened and closed [FU 3.1]. Once this has occurred it will start up the camera and record the area where a potential driver will be sitting [FU 3.2]. The video obtained will be run through a facial detection algorithm where the face of a valid driver will be detected and isolated [FU 3.3]. After this the prototype sends the isolated face along with a message to instruct the server to take the necessary action[FU 3.4]. The prototype will sit idle until it receives a response from the server [FU 3.4]. This response will be decoded and the system will act on the message by unlocking the vehicle (allowing for the key to be inserted) or leaving the vehicle locked (ensuring the key cannot be inserted) [FU 3.5]. Figure 3 is representation of the sub-functional units required for the facial detection [FU 3.3].

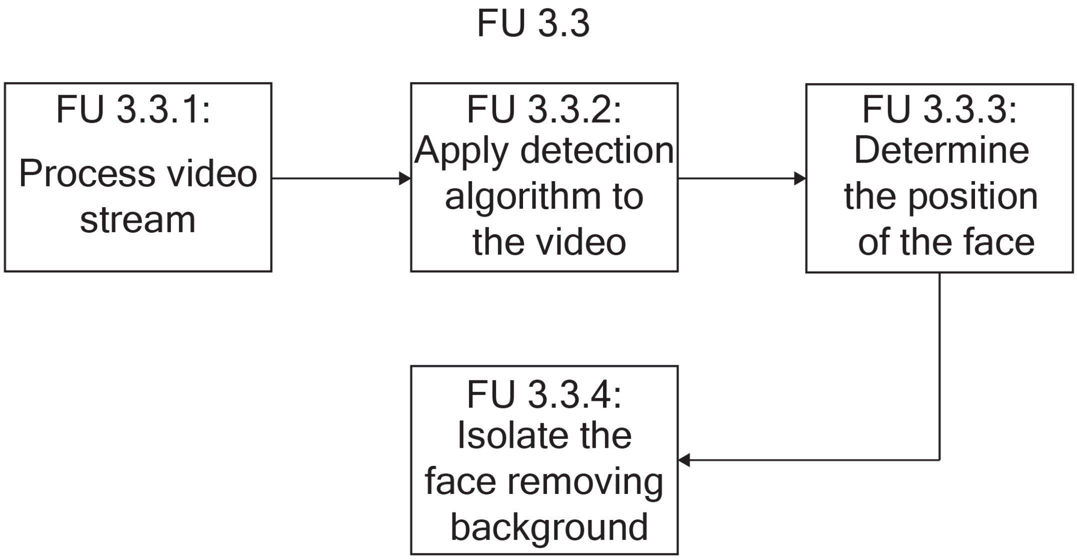

Figure 3. Sub-functional unit diagram of the the facial detection algorithm

The video stream will need to be converted into a usable form [FU 3.3.1]. Once in this usable form the facial detection algorithm can be applied [FU 3.3.2] which will determine if a face exists in the video stream and if the a face exists where it is located [FU 3.3.3]. The positions of the face will be used to isolate the face, removing unnecessary information [FU 3.3.4]. Figure 4 is a representation of the high level software functional units for the server.

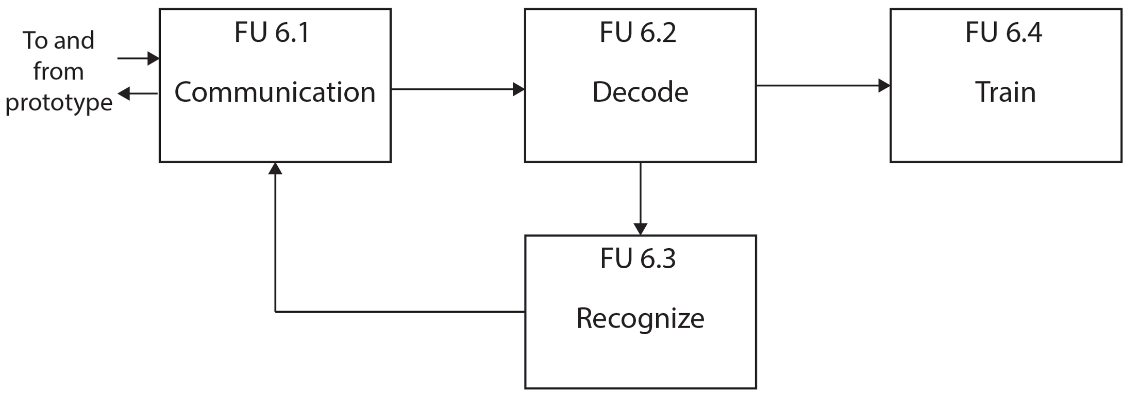

Figure 4. Software functional unit diagram of the server control unit

The server will wait for a message from the prototype. Once one has been received [FU 6.1], the given message will be decoded [FU 6.2]. Decoding will obtain the image as well as the instruction sent to the server. The instruction will either tell the server to train the network

[FU 6.4], this training process alters the structure of the neural network allowing for more accurate recognition, or to recognize the face [FU 6.3], to determine if the potential drive is a valid one or not. After the recognition the result will be sent back to the prototype [FU 6.1] so the appropriate action may be taken. Figure 5 is a representation of the sub-functional units required for the facial recognition [FU 6.3].

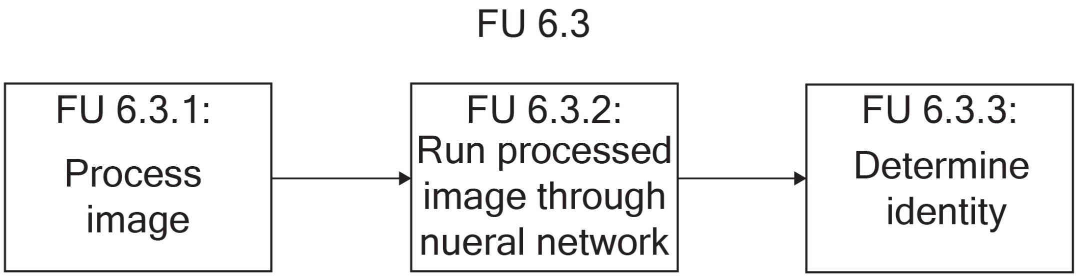

Figure 5. Sub-functional unit diagram of the the facial recognition algorithm

The image received will need to be converted into a usable form [FU 6.3.1]. Once processed the image will be run through the trained neural network [FU 6.3.2]. The neural network will be trained to recognize a particular user thus it’s output will be an indication of the identity of the person attempting to drive the vehicle [FU 6.3.3].

4. Specifications

4.1 Mission-critical system specifications

The mission critical specifications found in table 1 are the conditions the system must meet.

SPECIFICATION (IN MEASURABLE TERMS)	ORIGIN OR MOTIVATION OF THIS SPECIFICATION	HOW WILL YOU CONFIRM THAT YOUR SYSTEM COMPLIES WITH THIS SPECIFICATION?
The facial recognition algorithm should ultimately have an accuracy of 80 % and complete the facial recognition in less than 20 seconds.	The accuracy of the facial recognition may seem low for the purpose of security however with extensive training data this value can be greatly increased. The system will make multiple attempts to recognize a potential drivers face. The system will need to recognize a valid driver within the allowed number of attempts 80% of the time.	A valid driver's face will be run through the facial recognition algorithm allowing for the multiple attempts that the system will allow. The number of times the valid user is permitted to driver the vehicle after all the attempts of facial recognition have been made versus the number of times the valid user is not permitted to drive the vehicle will be recorded.
The facial recognition algorithm should have a false rejection rate of less than 40 %.	This value will be considerably high as there could be a number of possible reasons for a valid face to be rejected these include but are not limited to altering facial expressions (displaying emotion), shadows, errors in the transmission of the user face and so on.	A valid driver's face will be run through the facial recognition algorithm. The result of each and every attempt will be recorded. The number of false rejections will be recorded.
The facial recognition should have a false acceptance rate of less than 20 %.	This specification is given since the accuracy after multiple attempts should be around 80%. The system will need to air on the side of caution when making a decision rather then having the possibility for an invalid user to be allowed to start the vehicle.	An invalid driver's face will be run through the facial recognition algorithm. The result of each and every attempt will be recorded. The number of false acceptances will be recorded.

The system will detect a face within 5 seconds of it stabilizing in the frame with an accuracy of 90%.	Once the face has stabilized in the frame,it should be relatively quick to to detect the position of the face in the images. 5 seconds is given as the system is running on an embedded system that may run slowly. The accuracy of the system will depend on the quality of the training data.	A timer can be used, once the system feels it has detected the face it will stop the timer and the value can be outputted as well as the face it has detected. This will give an indication of how long the system takes to detect the face also allow for accuracy calculations.
Data transmissions between the server and prototype will be sent and received within 5 seconds and the success rate of the data transmission should be greater than 90%. The system will provide a minimum data transmission rate of 120Kbps	The transmission of data is vital in the functioning of the system. The transmission will be using existing wireless networks which should be established enough to have low error rates. The 120Kbps is the minimum cellular speed as cellular networks will make use of the EDGE service.	Multiple files of varying size can be sent to and from the server. The speed and success rate can be recorded. If speed cannot directly be recorded, a file of known size can be sent and the time to receive it on the other end recorded.

Table 1. Mission-critical system specification

4.2 Field conditions

The field conditions found in table 2 are the conditions that the prototype should meet

REQUIREMENT	SPECIFICATION (IN MEASURABLE TERMS)
The system will have to work in normal natural daylight conditions within a motor vehicle.	These conditions imply a light intensity of 4000-10000 lumens outside of the vehicle.
The system will need to be small and compact as it will need to remain in the vehicle even while the vehicle is moving	The system should not obstruct more then 10% of the drivers total field of view (FoV)
The system will need to work under normal vehicle cabin conditions based on South African weather	Temperatures ranging from -1 $^\circ$ C to 40 $^\circ$ C

Table 2. Field conditions

4.3 Functional unit specifications

The Functional unit specifications found in table 3 are the conditions that each functional unit should meet.

SPECIFICATION	ORIGIN OR MOTIVATION
FU 3.3 The facial detection will need to be completed in 5 seconds and provide a 90% accuracy once the person's face has stabilized.	The facial detection algorithm may take some time to run on the embedded device and error will be present since the training data will be limited.
FU 5 Sending information between the prototype and server (prototype control unit and the server control unit) should be completed in less than 5 seconds, at a minimum speed of 120Kbps with a maximum error rate of 10%.	Making use of the EDGE service or better speeds of 120Kbps should be achieved. Information being sent between server and prototype will be small files.
FU 2 and FU 3.2 the video obtained should have a minimum frame rate of 10 frames a second.	The system should run above 10 frames per second but it need not have a high frame rate to work. Somewhere between 10 and 60 will be adequate.
FU 3.3 The isolated face should be an image less than 512×512 pixels^2.	The isolated image of the face should be large enough to contain enough information about the driver to determine the drivers identity but small enough so that the facial recognition algorithm can work in a timely manner.
FU 4 The key stopper should be moved when instructed by the system 99% of the time.	The system will be controlling a motor of some kind. Error rate here should be low, there should be no signal integrity problem.
FU 6.3 Running a face through the neural network should provide a result in less than 20 seconds.	The neural network will be hosted externally on an external machine. It's speed or performance is not easily controlled.

Table 3. Functional unit specifications

5. Deliverables

5.1 Technical deliverables

Table 4 is a list of deliverables of this project and indicates if they will be implemented by the student.

DELIVERABLE	DESIGNED AND IMPLEMENTED BY STUDENT	OFF-THE-SHELF
Door sensor		×
Camera Module		×
Haar Cascades		×
Facial detection algorithm	×	
Facial recognition algorithm	×	
Key stopper to prevent the key from being able to start the car	×	
Server where facial recognition will take place	×	
Internet Connectivity, connect the server and the prototype		×
Embedded system (Raspberry Pi 3 Model B)		×

Table 4. Deliverables

5.2 Demonstration at the examination

The demonstration will be of the following.

- The car will be parked in an adequate position. This positioning will vary depending on the amount of light on that given day.
- The car will be unlocked and started without the system in place, this will be done to show the examiners how the car works under normal conditions before the system has been installed.
- The system will be placed in the car and the car will be locked.

- The system will be explained and shown working in three different scenarios.
  - The door will be opened and closed with no driver entering the vehicle.
  - A valid driver will enter the vehicle and it will be shown that the system can recognize the drive and will allow the car to be started.
  - An invalid driver will enter the vehicle and it will be shown that the system will not allow the car to be started.
- The training of the network to recognize a new face may be started, however, results from this training will not be available during the demonstration as they will not be completed.

6. References

[1] Clements Worldwide. (2016) Countires with the highest and the lowest crime rates. [Online]. Available: https://www.clements.com/resources/articles/Countries-with-the-Highest-and-Lowest-Crime-Rates

[2] Africa Check. (2016) FACTSHEET: South Africa's 2015/16 crime statistics. [Online]. Available: https://africacheck.org/factsheets/factsheet-south-africas-201516-crime-statistics/

[3] O. Solon. (2017) FBI facial recognition software. [Online]. Available: https://www.theguardian.com/technology/2017/mar/27/us-facial-recognition-database-fbi-drivers-licenses-passports

[4] Y. Taigman, M. Yang, M. Ranzato, and L. Wolf, "Deepface: Closing the gap to human-level performance in face verification," in *2014 IEEE Conference on Computer Vision and Pattern Recognition*, June 2014, pp. 1701–1708.