FACIAL RECOGNITION TECHNOLOGY USED IN THE PAYMENT SYSTEM

Bogdan Ion BOLDEA
PhD, Associate Professor, West University of Timisoara, ROMANIA
e-mail: bogdan.boldea@e-uvt.ro

Costin Radu BOLDEA
PhD, Associate Professor, University of Craiova, ROMANIA,
e-mail: cboldea@inf.ucv.ro

Abstract
This paper show if the facial recognition technology is ready to be used as an alternative to the existing payment methods used by individuals. The retina scan technology and iris scan technology are also presented as alternatives to the facial recognition technology in order to determine if any of the methods is more suitable to be used and to determine how should the next generation payment method look and what are the key factors that need to be taken into account before developing such a technology. The advantages and disadvantages of all technologies are discussed with pros and cons with a group of 220 participants. The case study includes all 220 participants to take part to an online interview followed by a 14 questions survey based on the discussions related to the presented technologies.

Keywords: *Facial Recognition Technology, Iris Scan Technology, Retina Scan Technology, Payment Methods, Data Privacy, Security Risk*

JEL Classification: *E71, EF15, F65,O11*

INTRODUCTION

Facial recognition technology is named until now, one of the few biometric methods that can be used worldwide in order to verify the identity of a person. When method was first developed, it was mainly used by government and law enforcement agencies for security purposes.

The Facial recognition technology is a biometric instrument used by capturing images of people's faces for either identity check or to identify a person based on the indexed data. In order to perform an identity check on a person, the facial recognition software cross-checks the picture taken at the given time with the image database that contains a list of pictures with people's faces and confirms the identity if that person is already added within the image database. To identify a person based on the indexed data, relevant features of the person must be configured within the feature database, for example: eye color, skin tone, hair color, etc. The similar process as in identity check is followed in the background, but this time, the picture taken of the person is not cross-checked with the image database, but with the features database [by I Berle's book].

LITERATURE REVIEW

Facial recognition algorithms can be described as a process or set of rules that must be followed in order to calculate or analyze facial characteristics, especially by a computer. As with any rules, there is always the question of interpretation and exceptions [by I Berle's Book].

Shang-Hung Lin explains that in most cases, face recognition algorithms are divided into at least two functioning modules: a face image detector which locates human faces and a face recognizer which identifies the person. This is accomplished when image pixels are converted into a representational vector and the pattern recognizer searches the database to find the best image match.

Therefore, face recognition is a form of pattern recognition,13 by which the process analyses the measurements of a person's facial characteristics that are captured by a camera. The pattern recognition process then synthesizes the overall facial structure, using distances between the pupillary center of the eyes, nose, mouth, and jaw edges including the chin. These measurements calculated by proprietary algorithms are stored in a database and used as a comparison the next time a person stands before a camera.

Driessen and Durmuth's description of the process assists in conceptualizing the process:

> "First, one needs to find the approximate position of the face in the image; this is called face-detection and a separate line of research. Most work on face recognition considers this job to be completed before; commonly used face image databases such as the FERET database annotate the images with the eye coordinates. Second, images are normalized, which usually includes an affine transformation [that is, the vectors between points of the space] to align the eyes, histogram equalization, and sometimes masking of the background. Third, in feature extraction algorithm-dependent features the probe image [is] extracted. Representing an image by a set of features can be seen as a step-in data reduction that aims at extracting a compact but discriminating description of the image. Ideally, the output of this step is at the same time robust against changes in posture, lighting, face expression, etc. Finally, the pre-processed probe image is matched against gallery images.the output of a face recognition algorithm is a list of identifiers, where the algorithm estimates that the first identifier (e.g. name) is the most likely one, matching the subject on the probe image".

This can be generically summarized as: acquisition and pre-processing, feature extraction, classification, and verification/identification.

Driessen and Durmuth also responded to the need to achieve anonymity against face recognition algorithms, especially in the context of improving privacy in social networks and other on-line albums, note that the eigenface algorithm "still provides very competitive performance for images taken in a moderately controlled environment. Also, it forms the basis for a wide range of algorithms, including Linear Discriminant Analysis (LDA) which can be applied after PCA and the Bayesian classifier…".Bayesian face recognition differs from most algorithms, because "in order to recognize a face the algorithm iterates over all stored persons (not faces), and for each decides if this is the correct person or not", and is therefore based on an inferred "probabilistic" similarity.

VULNERABILITIES AND FAILURES OF FACIAL RECOGNITION TECHNOLOGY

Biometric face recognition relies on the ability of the algorithm to identify a known individual. Yet, all forms of biometrics have error rates that affect the accuracy of the method and the overall performance between the computed dataset and the working system used in the real world. These error rates consist of either incorrectly accepting or rejecting an individual when presented for verification. An incorrectly accepted result or false positive is known as the False Acceptance Rate (FAR) and an incorrectly rejected result is known as the False Rejection Rate (FRR). These measures are inversely proportional; that is the threshold of one affects the other, for example by tuning the system to reject impostors and thereby minimizing FAR, it may also affect the FRR and reject some authorized users. These rates are determined by the designer or operator, and are functions of the system's 'decision-threshold'. For example, this could mean a 1:25 chance of not unlocking your mobile phone when switching it on (the false negative) or a 1:1000 chance of someone else doing so if your phone was lost or stolen (the false positive). Moreover, the 2010 NIST Interagency Report 7709 noted the improvement in accuracy of face recognition algorithms, whilst maintaining a False Acceptance Rate (FAR) of 0.001, False Rejection Rates (FRR) are falling—2002: FRR of 0.2; 2006: FRR of 0.01; 2010: FRR of 0.003. On that 2010 basis an individual has a 1:3000 chance of rejection at an airport e-gate. Or as Carl Gohringer reported in 2016, most European e-gates operate with an FRR of approximately 6% (0.006) set against a corresponding FAR of 0.1% [by I. Berle's Book].

Although the weaknesses and failures have yet to be entirely eliminated, which may be impossible in practice, we can see there have been significant improvements. Whilst this is good news for travelers, there is one difficulty that remains, in that, the false rejection rate can be influenced by poor quality images (photographs or video capture stills) and the false acceptance rate can be influenced by spoofing using a photograph of a registered user, which exposes the legitimate data subject to harm such as the risk of injustice, identity theft or fraud.

An ethical and legal risk exists when biometric face recognition is compromised when an impostor circumvents the system by spoofing the identity of a registered user. The ethical and legal risks are predicated by poor safeguarding and security of the system used, and the potentially fraudulent activity the access allows. Face spoofing by photograph is the most common abuse of the system. The 'photo-attacks' occur when a photograph is presented to an unmonitored system. This can be either a hard-copy or an image displayed on a smartphone or portable computer. Given that the face is an unconcealed biometric feature that is readily and easily obtainable, either directly by photographing the registered user or by copying their image from social network websites, the system is clearly exposed to spoofing attacks. I see no reason why such an ethical/legal risk should not increase as the public becomes more aware of the vulnerabilities of the system.

RETINA AND IRIS SCANNING TECHNOLOGIES AS ALTERNATIVES

In order to be able to have a decent understanding of how both scanning methods work, we need to know the difference between the two methods, hence they will be briefly explained below.

Retina scanning

The retina is a thin layer of cells in the back of the eye which is composed of a complex network of blood vessels, unique for each individual.

First discovered and studied in 1981, retina scanning is to date one of the most famous biometric technologies, but it is also one of the least used. When your retina is scanned, the unique pattern of the blood cells inside the eye is mapped (Figure 1).

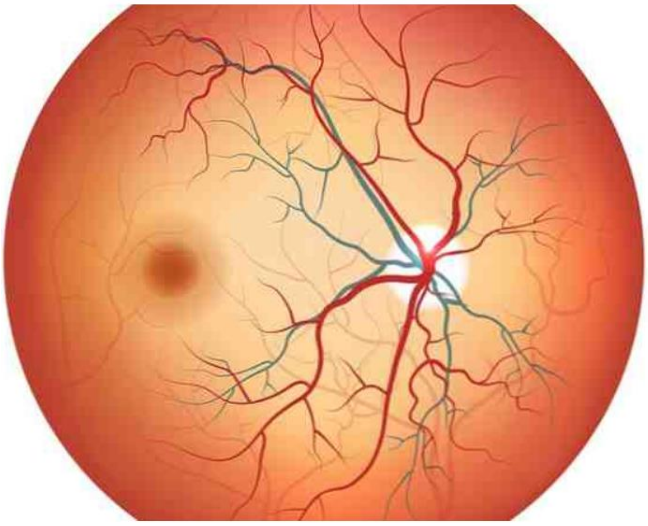


Figure 1. Retina blood vessels display

The blood vessels are easily identified when compared with other tissue from the eye, because they attract more light. The retina scan itself is performed by shooting an unseen beam of infrared laser light into a person's eye as they hold their eye close to the scanner. The beam of light then traces a standardized path on the retina.

After the image is captured by the scanner, the background software does all the computations needed to analyze the blood vessels pattern and to transform them into a unique template. The retina scanner does require high-quality images in order to be able to process the network of blood cells from an individual's eye. If the image is unstable or blurry the scanner will not let the user proceed. The unique template that is generated by the retina scanner is one of the smallest of any biometric technology.

Because the network of blood vessels of the retina is more absorbent of infrared light than the rest of the eye, the amount of reflection varies during the scan, after which the entire template pattern is converted into computer code and migrated in a database. Retina scan should therefore not be confused with other ocular scanning technology such as iris scanning which is the process of identifying an individual by the pattern it the iris.

Although, retina scan technology is not used as often as iris scanners or facial recognition, it is a highly dependable technology because of its high accuracy when talking about identification [by Ephesos Software article].

Advantages and disadvantages of Retina scanning

Unfortunately, as studies show, the retina does not remain unchanged over the course of years for around 20% of the earth population, which does not give us good reassurance in this method. Most of the retinal changes in an individual's life are cause by diseases such as diabetes and glaucoma. This would mean that if an individual is relying on a payment method that is strictly based on retina scan, and his retina has been damaged or it has changed due to an infection or disease, he will not be able to make that payment, thus, the method being unreliable.

The difficulty of image capturing and acquisition is considered to be one of the most notable disadvantages, due to the fact that for the retina scan enrollment process, the process takes a lot of time because multiple images are required to be taken which causes discomfort for the user.

The retina scanner requires an individual to get very close to the device; his eye should be at 5-7 centimeters distance from the scanner, which can cause distress for users. The retina scan technology has robust matching skills and is configured by default to do one-to-many identification against a database of users. As mentioned above, because the high-quality of the image required is difficult to obtain, an individual might be asked to go through the process several times until getting clearance.

On the bright side, the retina scan offers a great variety of medical applications on leading smartphone application markets. The advantage of using such an application in combination with the iris scanner is that the developers and engineers have programmed the software in such a way that it is able to detect possible diseases in an individual's system, such as AIDS or malaria. Specialists recommend that if you have the possibility, scan your retina with an licensed app once per week in order to know if you might of caught a disease up and to be able to reach professional medic help before it would be late [by R. King].

Iris scanning

An individual's iris is the colored part of his eye that surrounds the black dot called the pupil. The iris is also referred to as the "eye color" (Figure 2).

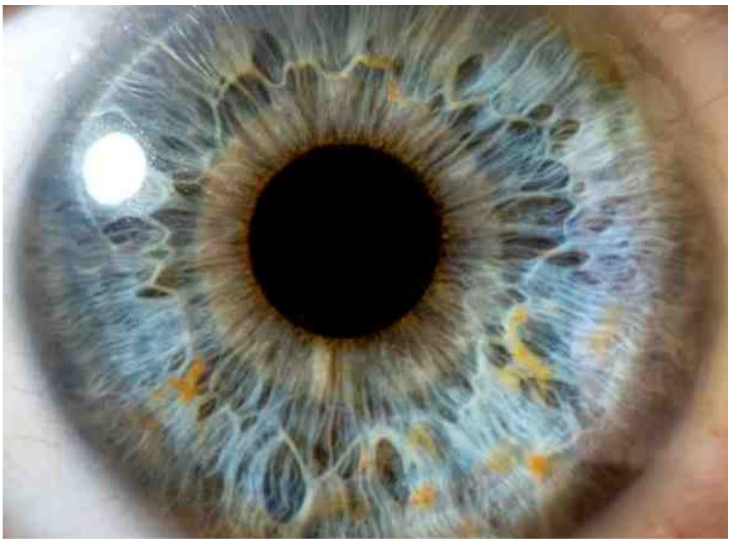


Figure 2. Display of the eye including iris and pupil

When looking closely into a mirror, you can observe that the iris is not a very deep and solid color, but more like a web of cells all combined together to form this magnifique and most importantly, unique display for each individual.

We can say that an iris scanner works similar to an ordinary photo camera or smartphone camera, the key difference factor being that, after the iris scanner takes a photo of your eye or records a short video of your eye movement, it also does some heavy computing tasks behind the curtains in order to extract the exact measurements of an individual's iris.

In order for the iris scanner to do those computing tasks, it shoots a beam of infrared laser inside the ocular globe. The beam of laser is then reflected back into the objective of the iris scanner together with a blueprint of the entire cell design from that individual's eye [Ephesos Software].

Advantages and disadvantages of Iris scanning

Between the two methods or iris scanning and retina scanning, the iris scanning is considered to be the best. It can be done from a longer distance, in some cases somewhere around 1 meter, thus being less invasive when compared to the 5-7 centimeters that the retina scanning requires. The iris is considered to be less exposed to modifications during the years when thinking about diseases, because even if a disease is caught, in most of the cases, the iris does not suffer any modifications, not considering here a physical injury to the eye.

Although we already have several factors that can point out the unicity of a person, the figures and details an iris contains is considered to be the best chance for humans to be perfectly identified.

Because the iris scanner works as a normal photo camera or video camera, it is possible that a number of different iris scanner devices can be tricked by a very qualitative photo of an individual's iris, or by a neat reproduction of someone's ocular globe. Saying that only a number of devices can be tricked because, in the last couple of years, most of the iris scanners have been updated and incorporated with a different technology which can see if the eye presented in front of the scanner is indeed a living person's eye. This is the main reason that the latest iris scanners do not take a photograph of your eye only, but as an extra step, it also records your eye movement for a few seconds. Although these security measures are not so convenient when it comes to time, the audience should always choose extra security over seconds of their time [S-L Surveillance].

THREATS OF IRIS SCANNING

One of the threats of iris scanning technology is the fact that a government agency can track people without them knowing or without their consent, without getting extremely close to them and even if they are in motion. This points out to some serious privacy issues and civil rights which will be clearly increased if more people agree upon sharing their iris information with an iris scanner.

With the latest iris scanning technologies available, a police officer could scan your iris form a long distance, such as pointing the scanner into your side view mirror once you are being pulled over. The unwanted picture would be that in some time, we could identify every individual at any place, even if he doesn't have a criminal record.

Without doubt, the most discussed threat of iris scanning, which can be considered same threat for retina scanning is the security of an individual's personal data. Until now, it has not been made available for the public what measures are taken by the government agencies to protect the biometric data they pull together.

We live in an era that cyber-attacks and data hacking are at an all-time high, thus the databases with sensitive information are targeted by criminals. If a criminal gets his hands on an individual's biometric information such as iris information or retina information, it is impossible for that individual to renew his iris or retina, as it could be possible with a smartphone, credit card, etc., making the risk of cyber-attacks even more high.

Government agencies often use external contractors and vendors for their information databases for support and maintenance, and given the current pandemic situation, almost all of those engineers are accessing those databases remotely, which means they can be in an unsecure place while doing so, and can be targeted more easily by criminals.

In the below picture we can find the process that a customer needs to go through at the initial payment step with an Alipay device (Figure 3).

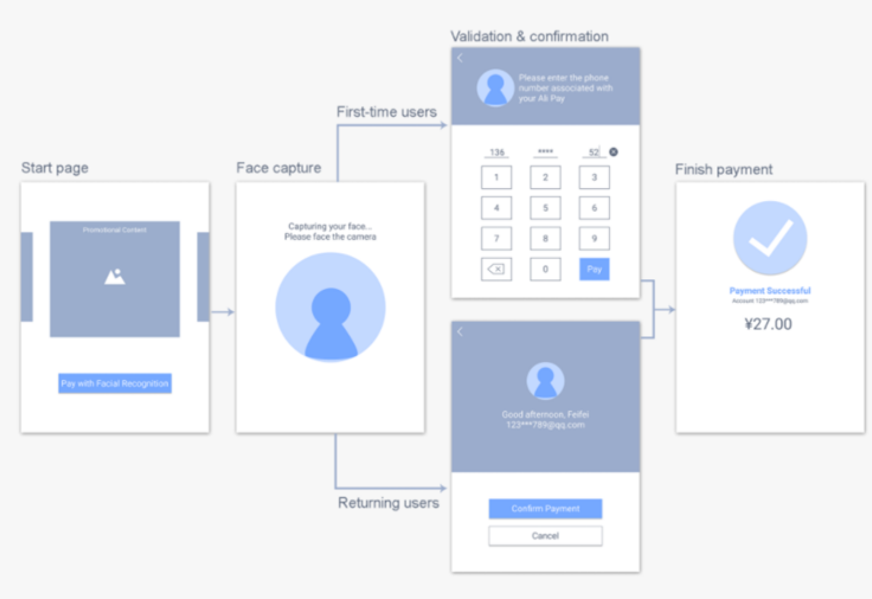


Figure 3. First time user steps need to be taken on Alipay FRP

Before the above image is prompted on the display of the device, the cashier must input the amount that the customer has to pay. After the cashier inputs the amount, the customer will have to touch the button that has the message "Pay with Face Recognition" on the device, at which point the device captures the customer's face and starts to cross-check it with its image database in order to find the data and the Alipay account linked to that customer. After the face has been captured by the device, the customer will be prompted with a new screen where he needs to enter his phone number registered with his Alipay account. If both the picture has a match within the image database and the phone number is correctly associated with that account, then the "Confirm Payment" button appears on the screen.

Everything sounds just about right until now, but actually, 8 out of 10 participants that were asked to participate in this interview rather stick to either cash payments, or to card payments for now, mentioning that they might think about it in the future when the methods will have some time to improve. Even though, they saw a great opportunity with this fast way of paying, most of the participants had questions regarding their data privacy and regarding the onboarding process.

If the onboarding process is poor that means that it will generate less trust. In the cases we presented, the payment duration was considered very short, but the onboarding experience for people who were using FRP for the first time was poor and, proceeding this, our participants started to become suspicious and did not show a trust relationship between them and the payment method and decided that they will not want to use it for the time being. As it is mentioned in an article found in the references, this can be called a Halo effect – their first interaction not positive, hence they gave the entire technology negative feedback.

MISTAKES FOUND

The first mistake that was observed was that Alipay did not ask users for a consent before proceeding with the process (Figure 4).

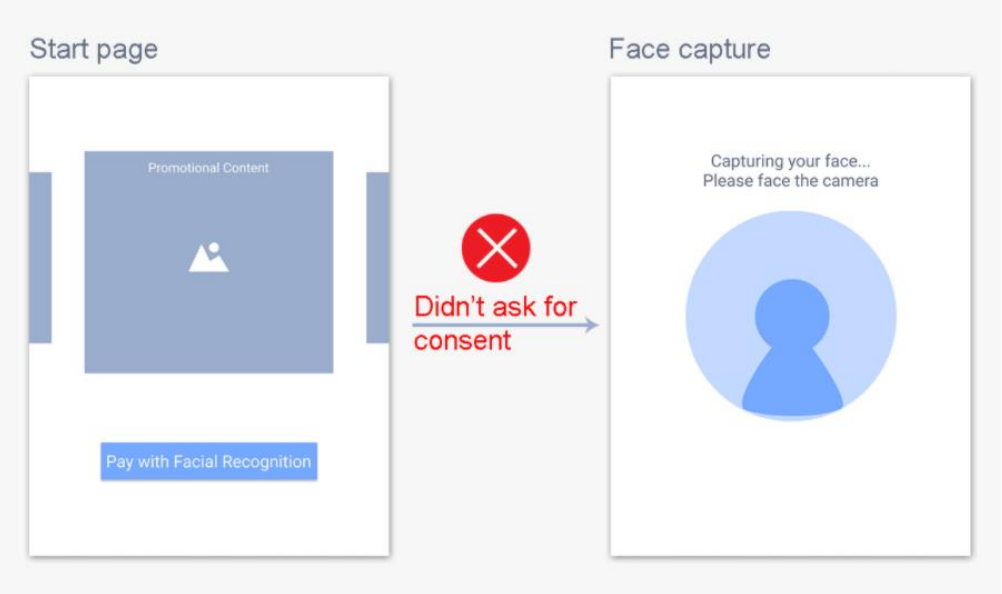


Figure 4. Display of user not being asked for consent on Alipay Facial recognition technology

After tapping the button on the display which says “Pay with Facial Recognition”, the figure capturing window appeared on the display which made some of the participants a little confused. One of the participants mentioned that Alipay allowed anyone to do this FRP with no consent at all; he said he should first have to authorize the paying method, before using the service.

The second mistake that Alipay did was to not explain to customers how the software actually works and how was their face recognized (Figure 5).

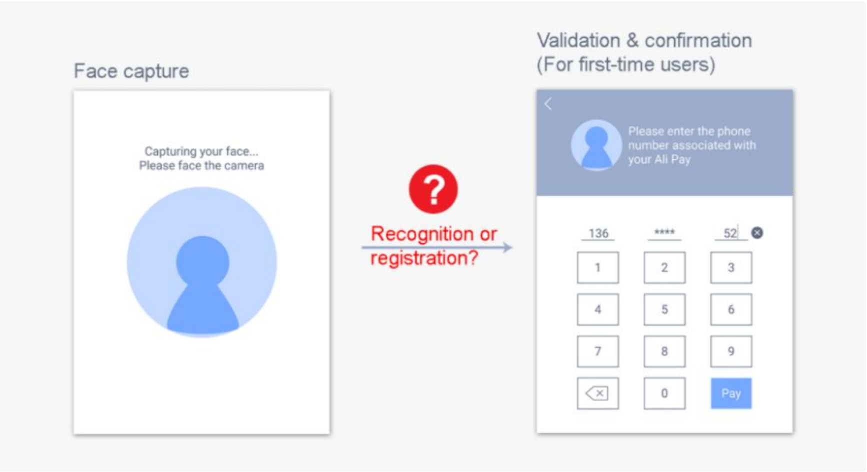

Face capture
Capturing your face...
Please face the camera
Recognition or registration?
Validation & confirmation
(For first-time users)
Please enter the phone number associated with your Ali Pay
136
****
52
1
2
3
4
5
6
7
8
9
0
Pay

Figure 5. Alipay Facial recognition technology not explaining how face detection works

When using a smartphone and you are setting up your Face ID, users of that smartphone are prompted to record their face from all front angles on a 180 degree axis. This process that is available on smartphones makes more sense to users because they can understand and visualize the actual recording process of their face. The Alipay does not have such process when using it for the first time.

It is actually based on your government issued personal ID card which all users of Alipay must have linked with their account. The information present on the ID is required in the vast majority of online payment services that can be found in China, and of course, this ID contains a photo of its user.

What some of our participants believed is that when they were to first use the payment method, it would be a registration process and not a recognition process. The first impression was that when the device was taking the picture, there was a link created on the spot by the application software between the customer's face and the database account that had the phone number registered with it. If this were to be true, it would be a huge disaster, meaning that, anyone can go to a FRP location, buy some goods and perform a registration of their face with a different phone number which could be assigned to another users account. We need to mention again that this is not the way the technology works, and that this was just the interpretation of some users when first seeing the process.

Another mistake that was observed is that there was no way of choosing a different card/account from which the money should be charged (Figure 6).

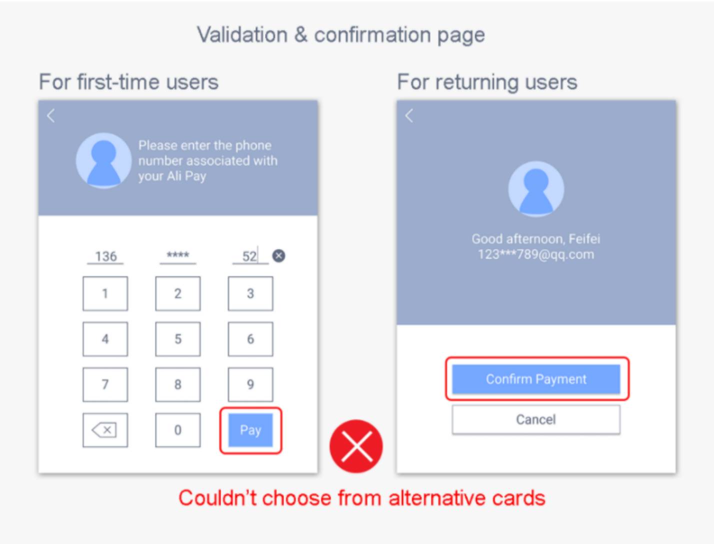
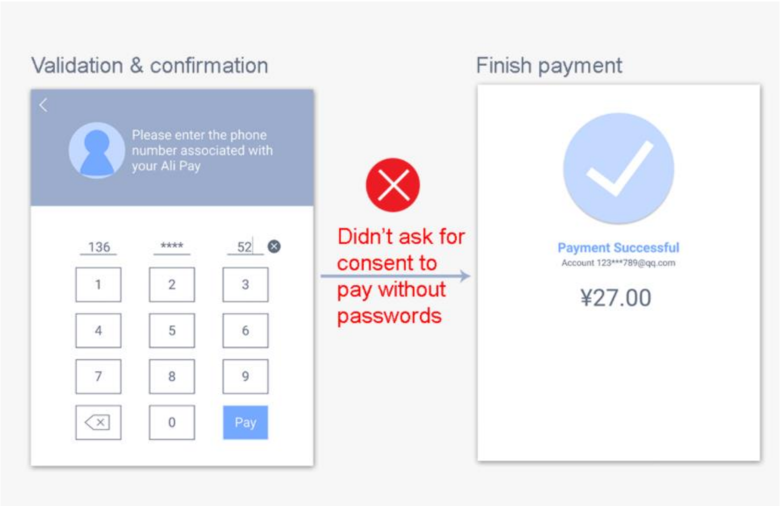

Validation & confirmation page
For first-time users
For returning users
Please enter the phone number associated with your Ali Pay
136
****
52
1
2
3
4
5
6
7
8
9
0
Pay
Good afternoon, Feifei
123***789@qq.com
Confirm Payment
Cancel
Couldn't choose from alternative cards

Figure 6. Display of validation & confirmation page without the option to choose between different cards

On the smartphones used by our participants, you can add multiple payment cards in your virtual wallet and before placing a payment, you have the option to choose with which card you want to pay, hence they compared this common payment method with the FRP. One online article mentioned that a customer of Alipay was mad after using FRP because the card that was charged was not in use by him anymore and had no balance, but still, the payment went through as successful and he later on needed to transfer money back into that account to have his balance on 0 again.

It could be that Alipay did not want to give out the option to choose a different card for charge because the whole point of facial recognition payment was to be very fast and not have to go through multiple steps during the payment. Most of our participants felt that this is indeed the right way to go, but not for the customers using the method for the first time. An option should be available at least for deciding which of your cards is the default payment method, and not assume a random one from your list. Again this was made a statement after comparing the facial recognition payment with the NFC smartphone payment that the participants are currently using.

The fourth mistake that was discussed was that for the customers using the payment method for the first time, the final step of the payment process did not include any type of password confirmation (Figure 7).



Please enter the phone number associated with your Ali Pay

Figure 7. Display of final payment page and confirmation

When thinking of smartphones, in order to make any payment, by default you are required to either enter a password or scan your fingerprint, and of course that is what our participants mentioned as well. By observing this, our participants have decreased their level of trust in the security of the process. One of our participants even mentioned that he uses his password for any amount in a payment and that if there are no passwords, there is no trust.

It could be that Alipay was so sure that the FRP is secure and that it did not need another protection step. None the less, while Alipay may consider its security very trust worthy, our participants did not see it that way. Some modifications should be made in order to make the process more customer friendly and more secure.

As the most common seen issues have been talked about above, we want to see what could actually be changed in order to modify the participant's opinion formed until this point and to have a better result when it comes to trust. As we can see other domains such as artificial intelligence, cloud computing, compute learning, etc, it is very easy to create distrust.

When talking about a new technology, the engineers and designers may have a really good understanding on how the process works, but this information needs to be translated for all users and to be made understandable even by non-technical individuals whom have little interaction with modern technology.

CONCLUSIONS

When we brought into discussion the safety of iris scanning technology, all of our participants wanted to know how will their personal and unique information be protected from any kind of cyber criminals who might want to gain access to personal data or banking accounts that could be linked to their iris scanners. The answer provided was not very satisfactory, because as we explained in the literature review, for now government agencies are using external contractors for operations and maintenance of their databases, which rises the risk of potential cyber-attack due to the fact that most employees are working from remote locations. We discussed further about iris scan technology being implemented into the banking operations system, but as the technology advanced until now, participants do not seem confident in choosing this as an alternative of facial recognition technology. This can be based on the fact that there are no examples of individuals using iris scanning technology for making a simple payment at a store, and the participants cannot see the entire process that would need to take place in order to use this payment method.

BIBLIOGRAPHY

1. Berle, I. (2020). *What Is Face Recognition Technology?*, Springer, available at https://link.springer.com/chapter/10.1007/978-3-030-36887-6_2
2. Boldea, B., Burz,R., (2012), *Sustainability Of Economic Growth And Inequality In Incomes*, Available at: http://anale.steconomiceuoradea.ro, 2012, ISSN 1582-5450
3. Boldea, B., (2016), *Human Capital Contracts as Investment Portfolio*, Available at: http://www.lsma.ro/index.php/lsma/article/view/977/pdf
4. Boldea, B., Boldea, C., (2016), *An Evolutionary Adaptive Method for Short Term Forecasting of The Exchanges Rate*, Available at: http://www.lsma.ro/index.php/lsma/article/view/976/pdf
5. Kunar, V. (2019). *Health Research Alliance: Understanding Retinal Changes after Stroke*, Available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6450536/
6. Kingt R. (2020). *Biometric Update: Retinal scan Technology article*, Available at: https://www.biometricupdate.com/201307/explainer-retinal-scan-technology
7. Liao, S. (2020). *Chinese subway experimenting with facial recognition to pay for fares*, The Verge, Available at: https://www.theverge.com/2019/3/13/18263923/chinese-subway-facial-recognition-fares-pay-ai
8. Liu, F (2018) *Making Cutting-Edge Technology Approachable – Case study of Facial Recognition Payment in China*, NNGroup, Available at https://www.nngroup.com/articles/face-recognition-pay/#:~:text=How%20Facial%2DRecognition%20Payment%20Works&text=The%20user%20taps%20Pay%20with,face%20and%20recognizes%20the%20user
9. Mullen, J. and Want, S. (). *Pay with your face at KFC in China*, CNN, Available at: https://money.cnn.com/2017/09/01/technology/china-alipay-kfc-facial-recognition/index.html
10. Symanovich, S. (2019). *How does facial recognition work?* NortonLifeLock, Available at: https://us.norton.com/internetsecurity-iot-how-facial-recognition-software-works.html
11. Turk, M. and Pentland A. (2017). *Eigenfaces for recognition*, Available at: https://pubmed.ncbi.nlm.nih.gov/23964806/
12. *** (2020). *Ephesos Software: Retina and Iris scanners at next security level?* Available at: https://ro.ephesossoftware.com/articles/security/are-retinairis-scanners-the-next-level-of-mobile-security.html
13. *** (2019). *Will facial payment technology work?*, Bluepay blog, Available at https://blog.bluepay.com/will-facial-payment-technology-work
14. *** (2020). *Street-Level Surveillance: Iris recognition article*, Available at: https://www.eff.org/pages/iris-recognition#:~:text=Biometric%20iris%20recognition%20scanners%20work,block%20parts%20of%20the%20iris
15. *** (2017). *How to facial recognition cameras work?*, SpyShop, Available at https://www.spy-shop.ro/blog/camere-cu-recunoastere-faciala?utm_source=2parale&utm_medium=quicklink&utm_campaign=6e871ea97