Remote KYC: Attacks and Counter-Measures

# Marc PIC Digital Labs m.pic@surys.com

## 2019

Remote Biometric Onboarding will become widespread in the coming years in various categories of service

# Abstract

Onboarding of new customers is a sensitive task for various services, like Banks who have to follow the Know Your Customer (KYC) rules. Mobile Onboarding Applications or KYC by Streaming are expanding rapidly to provide this capacity at home. Unfortunately, this leaves the authentication tools in the hand of end-users, allowing the attacker to directly tamper the video stream. With the rise of new digital face manipulation technologies, traditional face spoofing attacks such as presentation attacks or replay attacks should not be the only one to be considered. A new kind of face spoofing attacks (i.e. digital face spoofing) needs to be studied carefully. In this paper, we analyze those new kinds of attacks and propose a method to secure identity documents against both the traditional attacks and the new ones.

# Scholarcy Synopsis

Novel attack pattern for DeepFake anti-forensics, namely, the trace removal attack.  
We propose a trace removal network based on an adversarial learning framework involving one generator and multiple discriminators to remove various traces simultaneously.

Deep face forgeries, known as DeepFakes, are raising serious social concerns for information security.  
They focused on an anti-forensics attack against DeepFake detectors.  
The authors presented a novel detector-agnostic attack, called a trace removal attack, that is capable of refining DeepFake images.  
The authors present a novel detector-agnostic attack that is capable of refining DeepFake images by removing all possible DeepFake traces via an one-versus-multiple adversarial learning network.  
The refined Deepfake images are closer to the real images and can bypass arbitrary and even unknown detectors.  
They assessed the efficacy of the trace removal attack against a wide range of state-of-theart detectors.  
  
There were 66000 semantically-closest pairs in the study.

# Scholarcy Highlights

* Remote Biometric Onboarding (RBO) includes all the methods allowing to collect and secure data concerning a notpreviously-known applicant
* Secure RFID chips are only available on few ID documents and the majority of smartphones or computers are not able to communicate through RFID
* Remote Biometric Onboarding will become widespread in the coming years in various categories of service
* Identity theft will rely on hacker's tools and photo-realistic image doctoring
* We demonstrate in this paper that portrait seals can be applied to protect the authenticity of the face images present on ID Documents with a level of confidence higher than human capacity to recognize the document holder
* Such Portrait Seal can be embedded in the original document as a simple QRCode or Data-matrix or in a more sophisticated pattern like Photometrix [11]

# Scholarcy Summary

## INTRODUCTION

Remote Biometric Onboarding (RBO) includes all the methods allowing to collect and secure data concerning a notpreviously-known applicant.

Secure RFID chips are only available on few ID documents and the majority of smartphones or computers are not able to communicate through RFID.

Remote identification relies mostly on images or video processing.

Images of the ID documents can either be acquired by a webcam or a smartphone.

Until recently most of the attacks against this process came from physical counterfeited or fraudulent ID documents, but a variety of new technologies providing photorealistic computergenerated images bring new ways of fooling RBO.

New processes and tools must be defined to provide secured RBO against those emerging threats

## Physical attacks and counter-measures

To deceive the RBO process, fraudsters have several physical possibilities to spoof the system: Present a face printed on paper instead of his face: liveness detection has been conceived to detect such kind of presentation attacks.

Use a mask to mimic someone else, with the possibility to close the eyes or open the mouth to succeed in liveness tests: color reflection on the skin/mask or lack of facial activity can be analyzed to detect it.

Use a high-resolution screen to display an animated version of the target face: interactive sessions or moireartifacts analysis [1] will unveil the fraudster.

Except picture replacement, require: Expensive components; Risks; Delays.

Digital attacks are a lot easier but maybe a bit riskier for the fraudster.

In the case of a face morphing attack, the attacker will inject part of his identity into the image

## Digital attacks

The image or video comes from a physical sensor

At this point, a digital representation of a real-world scene is generated and send to the software which extracts features and performs biometrics matching.

Deepfake [3] is probably the best-known method to do this process and today it is becoming possible to create a deepfake without a subject specific training [4], Portrait Animation [5] allow the reenactment of a single portrait from a live face acquisition, Face2Face [6] is one of the most efficient allowing real-time animation of a target face from a facial live capture.

The first set of technologies are very promising for counterfeiters because they do not compromise the face of the fraudster, but in practice those methods are not easy to manipulate, and it is still difficult to maintain a real-time production with high-resolution video

## Analysis of counter-measures

Methods of fake detection based on neural networks have been proved efficient [8], in particular with the MesoNet approach [9] or the FaceForensics++ approach [10], but it is not yet clear how those methods are robust to the evolution of the deepfake generation process.

This area does not appear as sufficiently mature.

As mentioned in the previous paragraph, passive forensic methods, which try to detect the image or video stream forgeries without any indication may not be sufficient against an always evolving threat.

We believe that active forensic methods, which secure the media by watermarking it or digitally signing it, are more adapted and more robust against face and ID spoofing attacks

## Portrait seal

How to prove the authenticity of a picture? in our case of a portrait? In a fully digital scenario, there are many ways to protect an image.

Fragile watermarks can ensure that no information in the image content has been altered and can locate any alteration performed

Another common method to authenticate a file is to digitally sign it.

A set of salient point is extracted from the portrait

The location of those points are stored in a 2D visible seal and digitally signed using a public-key cryptography strategy [12], [13].

The authentication of the portrait is performed by comparing the stored locations against the recomputed locations on the reacquired picture

This method ensures that the biometric traits of the portrait have not been altered in any way while not being a biometric fingerprint.

A potential implementation of the seal requires fewer than 100 bytes with usual ECDSA cryptography, which can be embedded in a QR-Code or a Datamatrix added to the physical document or store in a separate database or file

## Attacks

Four main types of attacks have been evaluated: 1) Complete Photography Replacement: Is the basic case which requires to be evaluated because it is a very common and easy attack.

The original photography is replaced by the attacker portrait

In this case the complete biometry is altered.

2) Face Swapping: Is similar to the complete photography replacement but only the facial area is replaced

This has the advantage of being more subtle than a complete replacement and might be harder to detect.

4) Identity Deletion: Consists in altering the biometric characteristics of one person in order to erase the possibility to recognize himlher or to erase some specific identifiable traits of this person.

Of growing interest [15], is mainly used for preserving privacy

## Creation

Original face images were taken from the FERET dataset [17], [18] and gathered from IMDB.

Face morphing and Face swapping were generated as in [19] with a = 0.5 for morphing and a = 1 for swapping.

A is warped to match the biometric traits of B as in [19] but no blending is performed afterwards.

Random post-processing are applied to simulate the Print-Scan and Print-Cam process.

Those random post-processing are applied to the original images

## RESULTS

To assess the performance of our method, experiments were conducted on the dataset described in III.

Every image in the dataset is compared against every other images.

It can be seen that our method as very little chances to falsely match two different portraits even under Print-Scan and PrintCam scenarios.

The difference in performance against different attacks is due to the randomized post-processing described in III-B

## CONCLUSION

Remote Biometric Onboarding will become widespread in the coming years in various categories of service.

Identity theft will rely on hacker's tools and photo-realistic image doctoring

To fight such risks, two strategies will be necessary: the detection of digital fakes and the usage of light-weight content seal.

We demonstrate in this paper that portrait seals can be applied to protect the authenticity of the face images present on ID Documents with a level of confidence higher than human capacity to recognize the document holder.

Such Portrait Seal can be embedded in the original document as a simple QRCode or Data-matrix or in a more sophisticated pattern like Photometrix [11]

# Builds on previous work

We believe that active forensic methods, which secure the media by watermarking it or digitally signing it, are more adapted and more robust against face and ID spoofing attacks. **Methods of fake detection based on neural networks have been proved efficient [8], in particular with the MesoNet approach [9] or the FaceForensics++ approach [10], but it is not yet clear how those methods are robust to the evolution of the deepfake generation process**

# Contributions

Remote Biometric Onboarding will become widespread in the coming years in various categories of service. Identity theft will rely on hacker's tools and photo-realistic image doctoring. To fight such risks, two strategies will be necessary: the detection of digital fakes and the usage of light-weight content seal.We demonstrate in this paper that portrait seals can be applied to protect the authenticity of the face images present on ID Documents with a level of confidence higher than human capacity to recognize the document holder. Such Portrait Seal can be embedded in the original document as a simple QRCode or Data-matrix or in a more sophisticated pattern like Photometrix [11].