IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 1 July 2023, accepted 23 August 2023, date of publication 7 September 2023, date of current version 11 October 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3313094

APPLIED RESEARCH

Creating Realistic Presentation Attacks for Facial Impersonation Step-by-Step

ROBERTO GALLARDO-CAVA[1], DAVID ORTEGA-DELCAMPO[1], JULIO GUILLEN-GARCIA[1], DANIEL PALACIOS-ALONSO[2], AND CRISTINA CONDE[1]

[1]Face Recognition and Artificial Vision, Universidad Rey Juan Carlos, 28933 Móstoles, Spain
[2]Bioinspired Systems and Applications, Universidad Rey Juan Carlos, 28933 Móstoles, Spain

Corresponding author: Daniel Palacios-Alonso (daniel.palacios@urjc.es)

This work was supported in part by Spanish Ministerio de Ciencia e Innovación under Grant PID2021-124176OB-I00, in part by Universidad Rey Juan Carlos, and in part by the Spanish General Directorate of Police.

ABSTRACT Presentation attacks are one of the many dangers facing law enforcement today. In addition, material science is constantly advancing and criminals, aware of this fact, are taking advantage of new composites to manufacture new artifacts that allow them to cross borders by breaching border control points. This article presents the creation of several presentation attacks using make-up, hyper-realistic latex, and prosthetic masks. It is worth noting that such attacks do not receive adequate attention, due to the difficulty in their elaboration. The work of professionals in the make-up sector is required. Each stage of processing is analyzed for any artifacts that would facilitate the detection of the attack, using a multispectral approach in the visible and thermal spectra. The methodology evaluates three different face recognition systems (FRS), the different stages of impersonation, i.e. when a specific part of the face such as nose, cheekbones, jaw, or eyes is incorporated. The results show that certain parts of the face improve impersonation and make it more difficult for the algorithms to detect possible impersonation. However, other parts of the face, such as the jaw, not only do not improve impersonation but also significantly worsen performance. Using OpenFace as an FRS example, which is one of the FRS employed in this research work, the bonafide comparison of the target yields a score of 0.304, while with the make-up attack before applying make-up to the jaw, it gives 0.291, and after applying make-up, it gives 0.421.

INDEX TERMS Biometric systems, presentation attack construction, make-up attack, prosthetic mask attack, latex mask attack.

I. INTRODUCTION

The use of biometric technologies is growing in relevance as it becomes part of our daily lives. There is a wide variety of biometric traits, being the most commonly used the fingerprint, face and iris. Biometric systems use these traits to identify or verify different persons.

Biometric systems are divided into different modules that include a biometric sensor, as well as the feature extraction and the matching module. All these modules and all their connections are vulnerable to spoofing attacks. However, these systems tend to be encapsulated systems, making the sensor the only way to introduce an attack without gain access to the system. The sensor module captures the biometric trait to be used by other modules of the system.

The associate editor coordinating the review of this manuscript and approving it for publication was Khoa Luu.

Since the implementation of specialized attack detection systems, attack techniques have evolved in tandem, progressing and adapting alongside the new defenses. Attacks that were initially dangerous have now been overcome and are easily detected with high levels of precision. However, other attacks remain a threat and cause for concern because they are difficult for even experienced security personnel to detect automatically. These attacks include the use of make-up, prosthetic, or hyper-realistic latex masks.

A presentation attack (PA) occurs when a false reproduction of the biometric is presented to the system with the aim of impersonating a legitimate user. There are two different approaches to this type of attack. On the one hand, the attacker could present a fake biometric, such as an altered image, to the sensor. Alternatively, the attack could be inserted into the internal data of the document. The fraudster could insert

the altered photo into the document's internal memory and gain access at a biometric checkpoint.

This research focuses on the creation of three types of facial PAs that are less noticeable and harder to detect. In the make-up attack, the impersonator uses make-up to resemble the target. The prosthetic mask attack involves the use of a prosthetic mask and make-up to impersonate the target. Prosthetics are made of a material similar to human flesh. Finally, the latex mask attack involves the impostor impersonating the target using a soft, hyper-realistic latex mask. A trafficking network using such techniques was recently uncovered in Spain [1].

These attacks were analyzed with the aim of characterizing an impersonation. They have been divided by facial regions, trying to categorize the most relevant areas and the point of greatest similarity between the impostor and the target. These attacks have been studied in visible and thermal spectra. The images shown in this paper do not have any kind of digital retouching, simulating the case where the attacker tries to pass himself off as the verifiable owner of an identity document stolen from the target.

The make-up attack and the prosthetic mask attack were created by Amarante [2], a professional make-up artist, and Rosa [3], a professional FX make-up artist. The mask attack was created by Crea Fx Special Effects [4], a laboratory specialized in the creation of special make-up effects.

This paper is organized as follows: Section two presents the state-of-the-art. The following section describes the construction of the attacks. Section four is addressed displays the outcomes and provides a brief discussion. Finally, section five highlights the main conclusions and suggests future avenues of research.

II. PREVIOUS WORK

The PA can be constructed with any type of biometric feature such as fingerprints [5], [6], [7], [8], [9], the iris of the eye [10], [11], [12] and the face [13], [14], [15].

Focusing on the facial attacks, there is a wide variety of presentation attack instruments (PAIs), including pictures [13], [14], [16], videos [13], [14], [15] and cardboard masks [14]. Other types of attacks include make-up and 3D masks, which are the main topic of this research work.

The use of make-up allows faces to be modified in a temporary way. Make-up can change the perception of the face or its regions, such as the shape of the face; the shape and size of the nose; the size or appearance of the mouth; the shape, color, and position of the eyebrows; the shape, size, and contrast of the eyes; the concealment of dark circles; and the color of the skin [17]. Make-up can also reduce our ability to recognize faces [18] and also degrade the performance of face recognition systems [19], [20]. For these reasons, make-up is a widely used technique in visual performances such as films, series and theatre.

There are two ways to achieve make-up effects: using digital beautification techniques or programs, which are widely used in social media, [21], [22], [23], and using physical make-up, which is the focus of this research.

Make-up attacks can be countered by presentation attack detection (PAD) methods. These methods are mostly at the sensor level, processing the system inputs. Several make-up PAD approaches have been proposed in the literature. Make-up has been detected by analyzing different facial features such as face shape, color, and textures [24], [25]. Fusing information from different features was also used to create a robust, make-up-resistant recognition system [26]. MIFS [27] is a public database containing images of the impostor, targets, and impostors spoofing the target using make-up obtained from YouTube videos. In addition, the authors demonstrated that some systems can be vulnerable to make-up attacks and that the make-up can be used to adversarial attacks [28]. In [29], the authors propose a new approach to make-up-invariant face verification using a bi-level adversarial network, while in [30] a make-up-invariant face verification method based on weakly supervised learning is presented. The main idea in the latter is to learn discriminative facial features using facial images with varying degrees of make-up.

3D masks pose a problem because they can be purchased at a moderate cost to impersonate a desired person. There are different types such as rigid or flexible and can vary in manufacturing materials e.g. ceramic, latex, or silicone. There are some public 3D mask datasets in the literature. Some of them focus on rigid mask attacks, such as 3DMAD [31] and HKBU-MARs [32], while others like SMAD [33] or MLFP [34] are datasets of flexible masks. Datasets like MLFP [34] and ERPA [35] provide images captured by different types of cameras like RGB, NIR or thermal.

PAD for mask recognition can be divided into three approaches. Appearance-based methods aim to detect differences in micro-appearance, such as colour or texture, between a real or texture, between a real face and a mask. In order to achieve this goal, texture detection algorithms, in particular, local binary patterns (LBPs). Motion-based approaches attempt to detect the absence of involuntary movements of facial muscles, such as eye blinks, mouth movements, movements or head rotation, in synthetic mask materials. The first two approaches are beneficial for detecting rigid masks but may fail for flexible masks, as these are of higher quality and have movements and textures and textures that are more similar to those of the skin.

The liveness detection approach uses other cues of real faces for determining liveness. It uses intrinsic liveness signals like gaze information [36] or remote photoplethysmography signals (rPPGs) [32], [37], which attempts to measure a subject's heart rate through a camera remotely. The technique is based on the principle that the light reflected by the skin of the face varies slightly depending on the blood flow that changes with each heartbeat. Another technique uses thermal information; in face, comparing images across different cameras, exploiting the thermal spectrum was the

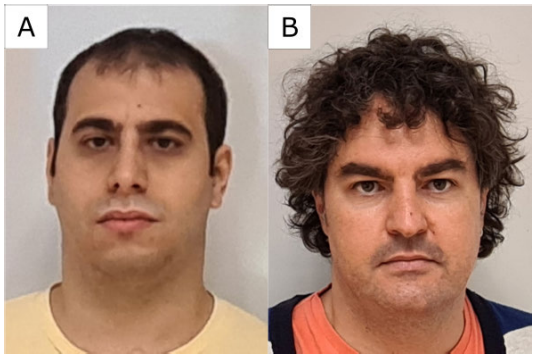

FIGURE 1. Images of the impostor and the target.

most effective way of detecting this type of attack [34]. However, in [38], a study was conducted to detect different types of PAIs, from images to 3D masks, using various deep learning models, and it was found that latex masks were the most difficult to detect with thermal cameras.

In the last years, most of approaches in PAD have focused on detecting as many possible attacks in a more generic way [39], [40], [41], [42], [43].

III. ATTACK CONSTRUCTION

This chapter is divided into three subsections. The first subsection is devoted to presenting the make-up attack method. The second subsection shows the prosthetic mask attack; it is further composed of two steps. The third subsection is addressed to the latex mask attack. These attacks are analyzed in the visible and in the thermal spectrum, with the impostor attempting to impersonate the same target. Although the attack examples were created using different individuals (the authors) as models, all the images feature the identical impostor and target for the sake of readability. Figure 1 displays the impostor's and the target's faces.

A. MAKE-UP ATTACK

This technique is commonly used in TV shows and is designed to be most effective when viewed from a particular angle, typically the camera's perspective.

During this experiment, at the request of the make-up artist, the target person served as a physical model throughout the attack creation process; however, this is not essential, as it is possible to use images of the target person without them being present.

The make-up process focuses on different areas of the impostor's face; from top to bottom.

- The eyes: The regions around the impostor's eyes such as the eyebrows and the bags under the eyes, are made-up to look like the target's eyes. The made-up eyebrows take the corporal heat of the impostor (see Figure 2A).
- The nose. A material similar to plasticine, called soft putty is used to enlarge the nose of the attacker, as his nose is narrower and less long than the target. Soft putty is an easily modeled, soft wax preparation with especially good adhesion characteristics, for the alteration of characteristic facial forms. Soft putty is applied over the skin and shaped with a palette knife [44]. The soft putty is made up after its application. If the target's nose were shorter than the attacker's nose, the attacker's nose would be reduced in appearance by creating shadows with make-up. Thermal imaging can identify a region in the nose area that does not have the right temperature. The large amount of soft putty located in the nose region cannot acquire a similar temperature to the rest of the face (see Figure 2B).
- The mouth. The impostor's lips are reduced with the make-up because the impostor's lips are wider than the target's. The made-up lips do not show any disruption at the thermal level (see Figure 2C).
- The jaw. The same methodology is used for nose make-up. This region is divided into two subregions, the right side and the left side of the jaw. The impostor's jaw is enlarged using soft putty to impersonate the target. Make-up can then be applied to the soft putty, enabling the simulation of a beard to the point of painting the individual hairs. For the jaw region, a much smaller amount of soft putty was used compared to the nose region. This smaller amount of soft putty correctly acquires the temperature of the impostor's face (see Figure 2D).
- Complete make-up. Finally, the target's skin colors are warmer than the attacker's and the application of general make-up is necessary to create a skin pattern with a uniform color similar to that of the target. In this step, skin moles are also removed. With the exception of the nose, the attack matches the right temperature (see Figure 2E).

This attack was created by Lewis Amarante [2], a professional make-up artist, and it took eight uninterrupted hours to complete the whole process.

B. PROSTHETIC MASK ATTACK

In this attack, the collaboration of the target is necessary because a mold of their face is required. To perform this attack, it is necessary to divide it into two sessions. The aim of the first session is to obtain molds of the target's and impostor's faces. In the case of this paper, the artists worked for an entire month to create the prosthetic mask from such molds. In the second session, the prosthetic mask is placed over the attacker's face.

This attack was created by Lewis Amarante [2], a professional make-up artist, and Raquel Pintado Rosa [3], a professional FX make-up artist.

1) OBTAINING THE FACIAL MOLDS

This process is carried out twice, and it is mandatory to obtain the attacker's and the target's facial molds. The acquisition of facial molds involves three steps:

- Application of the plastic layer. A layer of petroleum jelly is administered to the subjects' faces to avoid harming their skin. After applying the petroleum jelly,

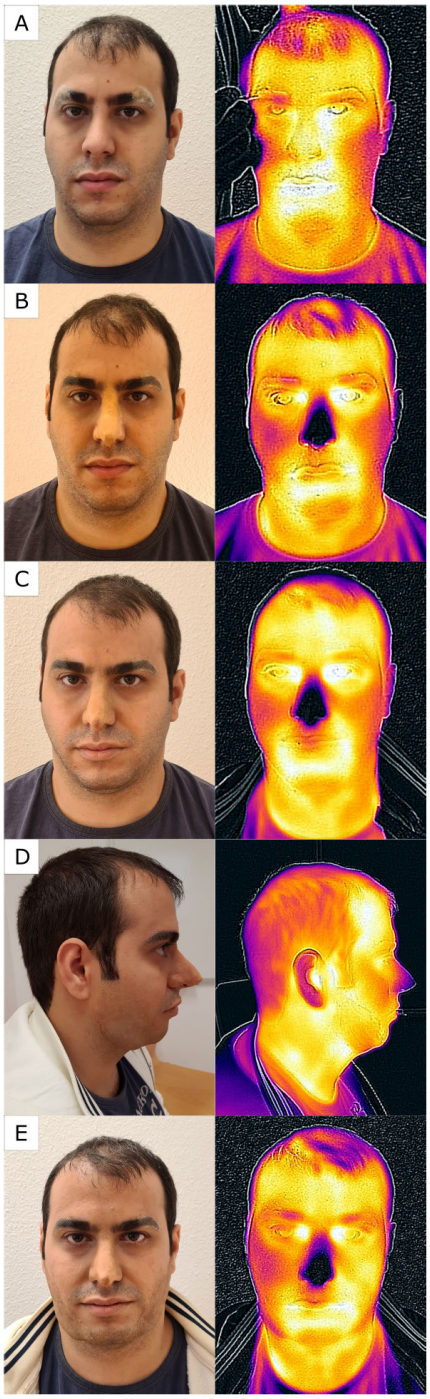

FIGURE 2. Creation of make-up attack, shown step by step in the visible and thermal spectrum. (A) Making up the eyes. (B) Nose construction. (C) Mouth modification. (D) Shaping the jaw.(E) Complete make-up application.

the entire face is covered with a layer of special malleable plastic, respecting the nostrils and allowing the subject to breathe (see Figure 3A).

- Plaster support. Plaster strips are applied on top of the previous layers to form a plaster mask. This mask forces the plastic layer to capture the subject's facial traits (see Figure 3B).

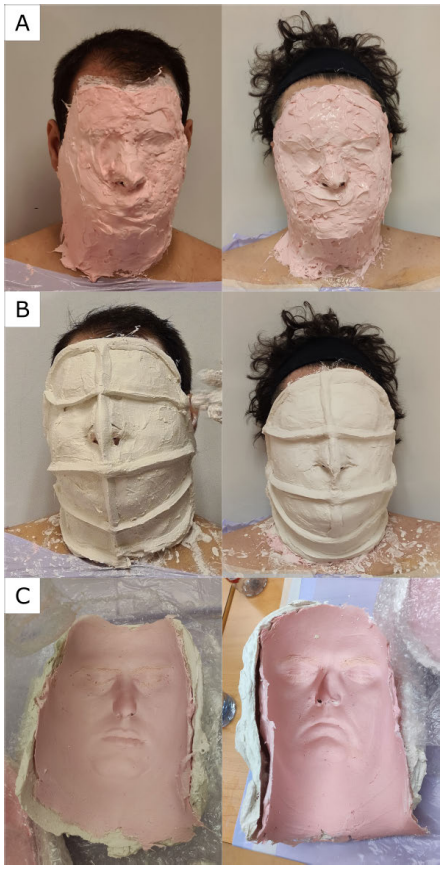

FIGURE 3. Creation of the face molds. (A) Application of the plastic layer. (B) Plaster support for the plastic mold. (C) Acquisition of the mold.

- Mold acquisition. Once the plaster mask is dry, it is removed. The plastic layer will also have dried, producing a texture similar to latex (see Figure 3C).

The creation of each mold takes around one hour. The authors of this research do not recommend this process for someone who suffers from claustrophobia.

2) CREATION OF THE PROSTHETIC MASK ATTACK

The second session takes place one month later after the construction of the facial molds. During this month, the artists created the prosthetic mask. New and much more precise plaster face molds are created from the plastic ones (see Figure 4A). Using these molds as a reference, it is possible to obtain the facial morphology of the subject, altering or diminishing the physical and structural aspects of the face. The mask is composed of small pieces of a synthetic material similar to human flesh (see Fig 4B). The prosthetic mask represents what needs to be added to the impostor's face to make it morphological accurate to the target's (see Fig 4C). A complete facial construction can be seen in Fig 4D.

The process of fitting the mask can be summarised in the following steps.

- Putting on the mask. Each piece of the mask has a specific position on the impostor's face where it must be placed. Depending on the facial morphology of the

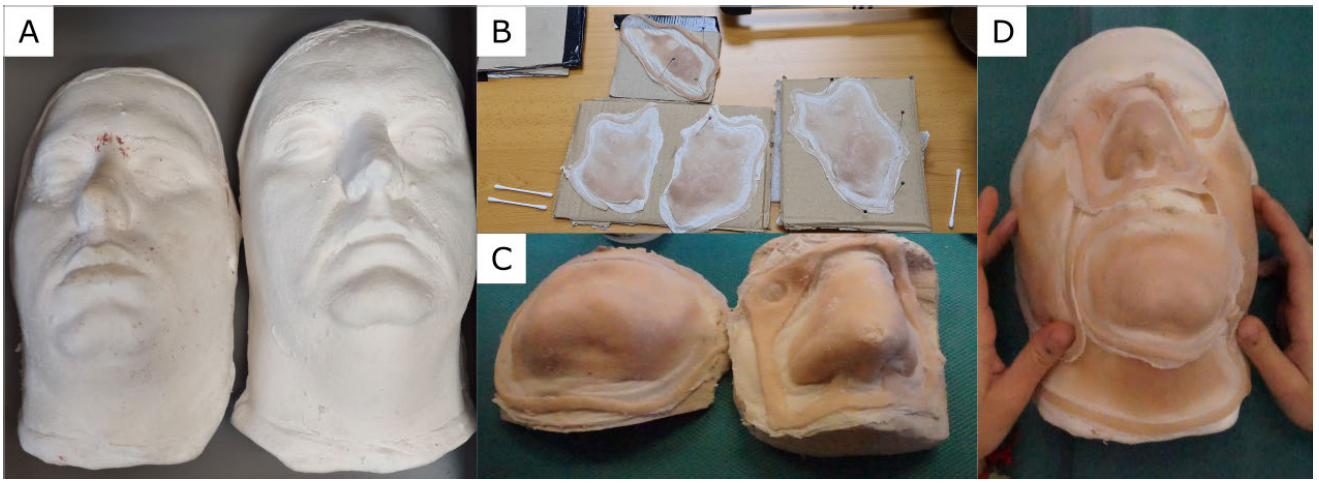

FIGURE 4. Construction of the prosthesis. (A) Plaster face molds. (B) Mask pieces. (C) Obtaining the parts of the face mask. (D) Facial construction using the mask.

person being impersonated, some parts may overlap with others. The mask is assembled piece by piece like a jigsaw puzzle and glued onto the attacker's face. The pieces have a thicker border to make it easier for the artists to handle them; these borders are removed once they are placed on the impostor's face. Once all the pieces have been fitted, make-up is applied to conceal the connections between them. Analyzing the thermal images once the mask is completely assembled, it can be observed that the nose and chin areas do not acquire the temperature that would be expected from genuine facial features. This happens because the mask is particularly thick in these regions (see Figure 5A).

- Applying make-up to the eyes. Make-up is then applied, around the impostor's eyes, to regions such as eyebrows and the bags under the eyes. At this point in the experiment, there was a problem with the adhesion of one region of the mask to the face and it was necessary to add a patch to properly grip and stick the former to the latter. The patch is invisible to human eyes, but not to a thermal camera (see Figure 5B).
- Complete mask attack. General make-up is finally applied to create a uniform skin colour pattern similar to the target's skin. Although the mask acquires the temperature of the face, there is a loss of approximately two degrees when thermal images are analyzed. The nose and chin have higher losses. This means that, if the system is equipped with a thermal camera, the presence of a mask could potentially be detected simply by properly thresholding the thermal image data (see Figure 5B).

It took five uninterrupted hours to complete this session.

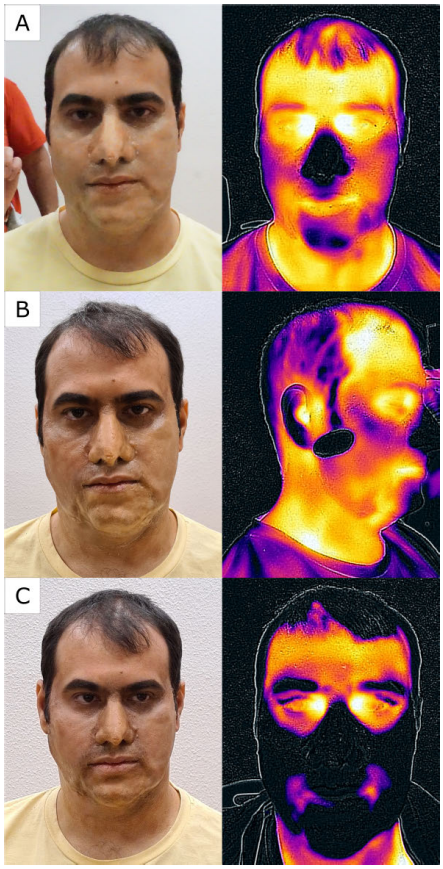

FIGURE 5. Creation of the prosthetic mask attack. (A) Donning the mask and concealing its connections. (B) Make-up applied to the regions around the eyes. (C) Complete make-up result.

C. HYPER-REALISTIC LATEX MASK ATTACK

For the creation of the latex mask, it is necessary to obtain front and profile photographs of both, the person whose mask is to be created and the person who will wear it. Additionally, a set of head measurements of both subjects is also required to obtain a better resemblance.

The collaboration of the target may not be necessary. For example, the photographs could be obtained from social networks, and one could use head measurements taken only from the impostor. Resemblance to the target would be

TABLE 1. Analysis of the scores generated by different FRS.

	OpenFace			FaceNet			ArcFace		
	Minimum	Maximum	Mean	Minimum	Maximum	Mean	Minimum	Maximum	Mean
Bonafide	0.107	0.338	0.224	0.139	0.398	0.259	0.068	0.150	0.105
Impostor	0.560	0.761	0.673	0.580	0.867	0.738	0.805	0.961	0.884
Make-up eyes	0.287	0.508	0.341	0.510	0.755	0.630	0.682	0.865	0.758
Make-up nose	0.219	0.468	0.342	0.532	0.636	0.592	0.666	0.861	0.756
Make-up mouth	0.292	0.540	0.379	0.465	0.646	0.556	0.615	0.847	0.737
Make-up jaw	0.392	0.504	0.465	0.516	0.758	0.628	0.673	0.815	0.746
Make-up complete	0.346	0.477	0.407	0.553	0.770	0.661	0.738	0.827	0.776
Prosthetic	0.433	0.491	0.459	0.689	0.772	0.726	0.782	0.824	0.802
Prosthetic & make-up eyes	0.413	0.591	0.496	0.688	0.759	0.709	0.752	0.804	0.776
Prosthetic mask complete	0.446	0.531	0.493	0.707	0.765	0.721	0.707	0.754	0.732
Latex mask	0.292	0.315	0.302	0.370	0.397	0.383	0.592	0.627	0.607

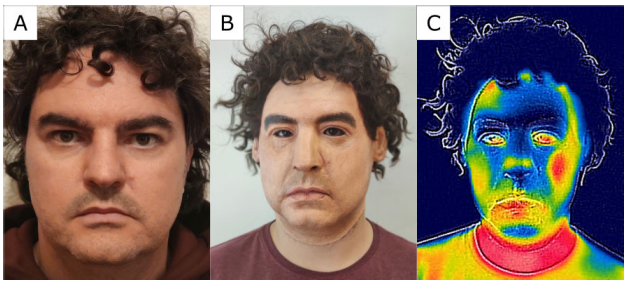

FIGURE 6. Latex mask attack. (A) Target. (B) Impostor wearing the mask. (C) Thermal analysis of the mask.

degraded, but this would enable carrying out some degree of impersonation without the target's cooperation.

The latex mask created for this paper was entirely hand-crafted by artisans, highlighting details such as expression lines or birthmarks. The mask has a hole for the eyes (cropped-eyes), allowing the wearer to see, and a practically imperceptible junction between the lips to facilitate breathing for the wearer (see Fig. 6). Thanks to the eye holes, the mask would avoid a portion of the liveness detectors found in the literature [15], [45].

Although the mask fits perfectly, it does not acquire the same temperature as the wearer's face. The eyes are the warmest point on the face, as there is no mask covering that region. It should be noted that the mask does not reach the same temperature as the wearer, with a noticeable difference from the temperature of the neck.

This attack was created by Crea Fx Special Effects [4], a laboratory specialized in the creation of special make-up effects and it took two months to create this mask.

IV. RESULTS AND DISCUSSION

This chapter explores the possibility of impersonating another person using different attack methods. Additionally, it analyzes the attacks by examining the scores at each step of the attack creation process. The reason for dividing the attacks into stages is to study how the attacker gradually resembles the victim as the presentation attack progresses. For these purposes, the analysis is carried out with different deep face recognition systems (FRS), the open-source OpenFace [46], the well-known FaceNet [47] implemented through [48], and the recent ArcFace [49] system. The experiments involve ten images, with different models, in all the stages of the attacks' construction. The score values represent the resemblance between two faces calculated by the FRS. A closer value to 0 indicates a higher level of similarity. A database of one hundred users is used to standardize the score values. This methodology was repeated for each FRS (see Fig. 7) and all its values are collected in the Table 1. The used metrics have been selected for compatibility with other authors. Exact thresholds could be adapted to the specific conditions of the border control. In some situations (i.e. flights arriving from low-risk countries) false rejection rate (FRR) could be lower, although the false acceptance rate (FAR) was higher. In the case of high-risk countries, the FRR could be higher since the FAR could be kept to a lower threshold. The operative thresholds could be selected depending on these conditions and could not be a fixed parameter.

A. POSSIBILITY OF IMPERSONATION

The scores generated by different images of the target are categorized as bonafide and the scores generated by comparing the target with the attacker are referred to as impostors. These scores are analyzed and compared to the results obtained from the final stages of each attack to verify the possibility of identity theft using these methods. The scenarios evaluated include bonafide, impostors, the complete make-up attack, the complete prosthetic mask attack and the latex mask attack (see Fig. 7A).

Openface shows several problems with these attacks. The scores generated from different bonafide images (the target) have a range between 0.107 and 0.338, whereas the impostor has a range of 0.560 to 0.761. The three attacks obtain a similarity score closer to bonafide scores. The make-up attack achieves remarkable range scores between 0.346 and 0.477, similar to those that have been assigned to a genuine user. The prosthetic mask also obtains fairly good results with a range of 0.446-0.530, while the latex mask achieves the best ones, surpassing even better results than the make-up attack with results ranging 0.292-0.315.

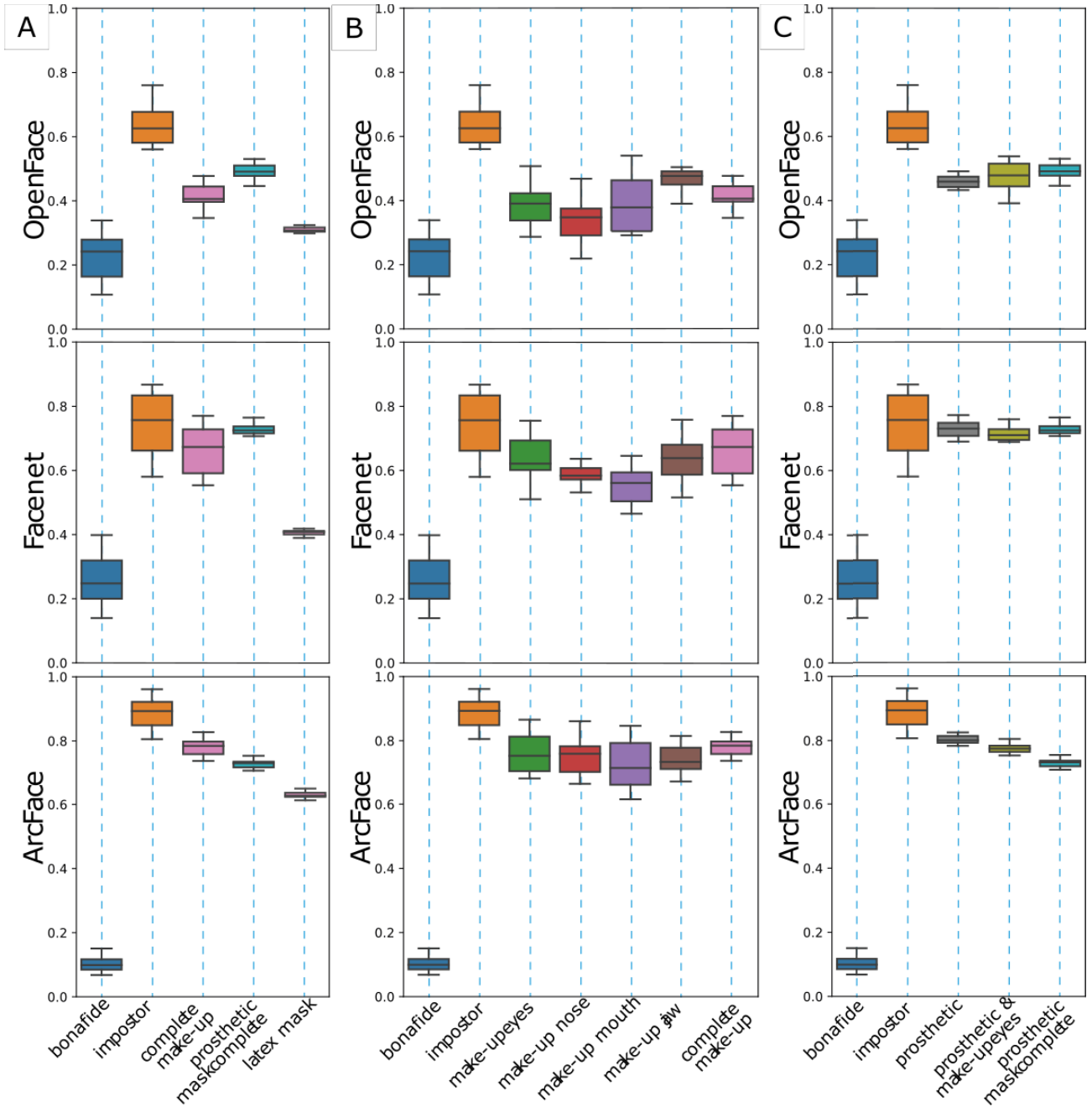

FIGURE 7. Comparison scores. (A) Final stages of attacks. (B) Stages of the make-up attack. (C) Stages of the prosthetic mask attack.

Facenet generated bonafide range scores of 0.139-0.398, and the impostor's scores achieved a range of 0.581-0.867. The make-up attacks also seem to be quite effective against this FRS with a score range of 0.554-0.770. The prosthetic mask obtains worse results regarding the similarity, getting a range score 0.707-0.756. Indeed, the hyper-realistic latex mask again achieves excellent results, obtaining a range of 0.371-0.389, similar to a genuine user.

The Arcface system accomplished a bonafide score range of 0.068-0.150 and 0.805-0.961 in the impostor category. Although discrimination with Arcface is considerably better, the attacks also provide similarity scores that are closer to those of genuine users. The make-up attack realizes a score range 0.738-0.827 and the prosthetic mask 0.707-0.754. The best attack scores are again generated by the latex mask, achieving a score range of 0.592-0.627. Notice that Arcface is the only system in which the prosthetic mask attack achieves better results than the make-up attack. Nonetheless, the similarity scores of all these attacks are far behind the score generated by a genuine user.

It can be observed that all three systems excel notably in distinguishing between bonafide and impostor users. The

latex mask reaches the highest similarities to the target in all scenarios among all the attacks.

B. INSIDE THE MAKE-UP ATTACK

The scores generated by each stage of the make-up attack are compared (see Fig. 7B). The make-up and prosthetic mask attacks are divided into incremental phases, meaning that the second phase involves the first one, the third phase includes the first two, and so on. The make-up attack is divided into the following phases: make-up eyes, make-up nose, make-up mouth, make-up jaw, and complete make-up.

The score ranges for those scenarios are as follows. Concerning Openface, the values obtained about make-up are 0.287-0.508 (eyes), 0.219-0.468 (nose), 0.292-0.540 (mouth), 0.392-0.504 (jaw) and 0.346-0.477 (complete). Analogously, regarding FaceNet, the values attained about make-up are 0.510-0.755 (eyes), 0.532-0.636 (nose), 0.465-0.646 (mouth), 0.516-0.758 (jaw) and 0.553-0.770 (complete). Finally, the outcomes of ArcFace are 0.682-0.865 (eyes), 0.666-0.861 (nose), 0.615-0.847 (mouth), 0.673-0.815 (jaw) and 0.738-0.827 (complete).

The different stages of the make-up attack have a similar progression in the three scenarios. As the make-up process progresses, the similarity to a genuine user gradually increases up to a specific point, before the make-up process is fully completed, and the similarity decreases as the score increases. The key point of the make-up attack is that the eyes, nose and mouth are made up are the most distinctive features of these systems. Applying make-up to the jawline not only proves to be unnecessary but also counterproductive, worsening the previous results. The final stage, the complete make-up phase, does not appear to contribute much to the final result. This attack can achieve, or closely approach, the similarity score generated by a genuine user when the best result for each FRS is analyzed, even improving the scores previously achieved by the latex mask

C. INSIDE THE PROSTHETIC MASK ATTACK

With the make-up attack, the prosthetic mask attack is also divided into incremental stages and each stage is analyzed (see Fig. 7C). The prosthetic mask attack is divided into the prosthetic mask, the prosthetic mask with eye make-up and the complete prosthetic mask. The score ranges for those scenarios explain as follows. About Openface, the results accomplished are 0.433-0.491 (prosthetic), 0.413-0.591 (prosthetic and make-up eyes) and 0.446-0.531 (prosthetic and mask complete). Concerning the FaceNet, the scores achieved are 0.689-0.772 (prosthetic), 0.688-0.759 (prosthetic and make-up eyes) and 0.707-0.765 (prosthetic and mask complete). Finally, regarding ArcFace, the outcomes attained are 0.782-0.824 (prosthetic), 0.863-0.824 (prosthetic and make-up eyes) and 0.707-0.754 (prosthetic and mask complete).

The results obtained from the stages of the prosthetic mask do not exhibit the pattern followed in the case of the make-up attack, as the process of progressively incorporating the prosthetic mask, so as to gradually resemble the target person, does not seem to affect the performance of the verification systems. In fact, in the Openface and Facenet systems, there are little variations in the similarity scores and, in the case of Facenet, they approach the similarity scores generated by a genuine user.

Depending on the system, the prosthetic mask can approach the similarity scores generated by a genuine user.

V. CONCLUSION

This research presents the step-by-step construction of different presentation attacks inspired by the world of cinema, namely the make-up attack, the prosthetic mask attack and the latex mask attack. The effectiveness of these attacks was tested against different facial recognition systems using different individuals.

The purpose of this paper is to demonstrate that these attacks can allow an impostor to simulate the facial features of a genuine user to the point of enabling impersonation. Whether or not these attacks can breach the security of FRS depends on where the threshold is set. It is easier to breach systems that are configured to be more friendly.

The best results were achieved by the latex mask attack, but all the attacks presented could be used for impersonation depending on the system used for evaluation. International Civil Aviation Organisation (ICAO) categorizes systems in the following levels, ordered from lower to higher vulnerability: a system that performs a cursory examination at the border control point, a system that acts as an examination using simple equipment, and a system that employs forensic techniques. These attacks should not have difficulties bypassing systems at levels one or two [50]. More examples of such attacks are needed to ensure that these attacks are sufficient to breach the security of these systems. The obtained data suggest that older systems are much more vulnerable to such attacks than newer ones. Using similar models and objects such as contact lenses, wigs, or earrings could also lead to better results.

Another idea extracted from this study is that the point of the closest similarity to the target may not be the final stage of the attack construction (see Fig. 7). In the make-up attack, the point of highest similarity was achieved only when the eyes, nose, and mouth had make-up. This specific point can become the point of highest similarity among all the analyzed attacks and phases. The reason why jawline make-up generated worse results may be due to several factors: it could be that modifying this region significantly alters the shadows and contours of the face, confusing the system, or be simply due to the inherent degradation of the first layers of make-up over time, which can affect the most characteristic facial features and make it more difficult to maintain the impersonation. In the prosthetic mask attacks, there is no clear relationship between how the progression of the attack affects the improvement of the similarity, as the similarity scores barely varied.

However, several disadvantages have been found in carrying out these attacks. It is necessary to hire and coordinate various artists. The creation of the prosthetic mask requires a month, and the creation of the latex mask requires two months of the artist's work. Aside from the economic cost, this makes it very difficult to mass-produce them in order to generate a database. For the creation of the prosthetic mask, the cooperation of the person who is going to be impersonated is strictly necessary. Once the make-up is removed, it cannot be reused, and to remove the prosthetic mask, it must be destroyed, making these attacks single-use. After several hours, the first areas where make-up has been applied will deteriorate due to perspiration and sweating of the skin, causing attacks involving make-up to lose quality over time. This fact negatively affects its performance because it makes it more obvious to human eyes and also causes it to perform worse with face recognition systems.

Analyzing the attacks in the visible, the make-up attack and the prosthetic mask attack can be sufficiently discreet, but the latex mask attack cannot. Make-up goes unnoticed among people because we are familiar with it. Furthermore, there are no clear limits on the maximum amount of wearable make-up that is allowed. Concerning thermal analysis, in the make-up attack, the temperature of the nose stands out, while the rest of the face shows nothing out of the ordinary. In the prosthetic mask attack, the mask has a temperature loss of approximately two degrees. Despite the fact that the latex mask varies in temperature, it achieves an average of five degrees less than the temperature of an actual user, generating human atypical temperature values and creating a sharp contrast with the neck. However, this issue could be addressed by increasing the size of the latex mask to cover the neck as well. Nonetheless, it could be possible to create a PAD that easily detects these attacks using thermal cameras using these and other guidelines that could be inferred given a sufficient database.

REFERENCES

[1] B. Calleja. *Pasaportes Falsos Y Disfraces: Así Traficaba Una Red Malagueña Con Refugiados Iraníes*. Accessed: May 24, 2023. [Online]. Available: https://www.epe.es/es/espana/ 20230208/red-trafico-personas-ilegal-iran-82633612

[2] L. Amarante. *Lewis Amarante*. Accessed: May 24, 2023. [Online]. Available: https://www.lewisamarante.es/

[3] *Raquel Pintado Rosa. Raquel Pintado Rosa*. Accessed: May 24, 2023. [Online]. Available: https://www.instagram.com/accounts/login/?next=/raquel_pintado_rosa/

[4] CreaFX. *Creafx Special Make-Up Effects*. Accessed: May 24, 2023. [Online]. Available: https://www.creafx.com/

[5] S. Cimato, M. Gamassi, V. Piuri, R. Sassi, and F. Scotti, "Privacy-aware biometrics: Design and implementation of a multimodal verification system," in *Proc. Annu. Comput. Secur. Appl. Conf. (ACSAC)*, Dec. 2008, pp. 130–139.

[6] E. Marasco and A. Ross, "A survey on antispoofing schemes for fingerprint recognition systems," *ACM Comput. Surv.*, vol. 47, no. 2, pp. 1–36, Jan. 2015.

[7] C. Sousedik and C. Busch, "Presentation attack detection methods for fingerprint recognition systems: A survey," *IET Biometrics*, vol. 3, no. 4, pp. 219–233, Dec. 2014.

[8] M. Ferrara, R. Cappelli, and D. Maltoni, "On the feasibility of creating double-identity fingerprints," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 4, pp. 892–900, Apr. 2017.

[9] M. Espinoza, C. Champod, and P. Margot, "Vulnerabilities of fingerprint reader to fake fingerprints attacks," *Forensic Sci. Int.*, vol. 204, nos. 1–3, pp. 41–49, Jan. 2011.

[10] J. Daugman, "How iris recognition works," in *The Essential Guide to Image Processing*. Amsterdam, The Netherlands: Elsevier, 2009, pp. 715–739.

[11] C.-T. Chou, S.-W. Shih, W.-S. Chen, V. W. Cheng, and D.-Y. Chen, "Non-orthogonal view iris recognition system," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 20, no. 3, pp. 417–430, Mar. 2010.

[12] K. B. Raja, R. Raghavendra, and C. Busch, "Color adaptive quantized patterns for presentation attack detection in ocular biometric systems," in *Proc. 9th Int. Conf. Secur. Inf. Netw.*, Jul. 2016, pp. 9–15.

[13] A. Anjos and S. Marcel, "Counter-measures to photo attacks in face recognition: A public database and a baseline," in *Proc. Int. Joint Conf. Biometrics (IJCB)*, Oct. 2011, pp. 1–7.

[14] D. O. del Campo, C. Conde, Á. Serrano, I. M. de Diego, and E. Cabello, "Face recognition-based presentation attack detection in a two-step segregated automated border control e-gate," Secrypt, Madrid, Spain, Tech. Rep., 2017, vol. 4.

[15] G. Pan, L. Sun, Z. Wu, and S. Lao, "Eyeblink-based anti-spoofing in face recognition from a generic webcamera," in *Proc. IEEE 11th Int. Conf. Comput. Vis.*, Oct. 2007, pp. 1–8.

[16] K. Patel, H. Han, and A. K. Jain, "Secure face unlock: Spoof detection on smartphones," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 10, pp. 2268–2283, Oct. 2016.

[17] A. Dantcheva, C. Chen, and A. Ross, "Can facial cosmetics affect the matching accuracy of face recognition systems?" in *Proc. IEEE 5th Int. Conf. Biometrics, Theory, Appl. Syst. (BTAS)*, Sep. 2012, pp. 391–398.

[18] S. Ueda and T. Koyama, "Influence of make-up on facial recognition," *Perception*, vol. 39, no. 2, pp. 260–264, Feb. 2010.

[19] M.-L. Eckert, N. Kose, and J.-L. Dugelay, "Facial cosmetics database and impact analysis on automatic face recognition," in *Proc. IEEE 15th Int. Workshop Multimedia Signal Process. (MMSP)*, Sep. 2013, pp. 434–439.

[20] T. Y. Wang and A. Kumar, "Recognizing human faces under disguise and makeup," in *Proc. IEEE Int. Conf. Identity, Secur. Behav. Anal. (ISBA)*, Feb. 2016, pp. 1–7.

[21] H. Chang, J. Lu, F. Yu, and A. Finkelstein, "PairedCycleGAN: Asymmetric style transfer for applying and removing makeup," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit.*, Jun. 2018, pp. 40–48.

[22] C. Rathgeb, A. Dantcheva, and C. Busch, "Impact and detection of facial beautification in face recognition: An overview," *IEEE Access*, vol. 7, pp. 152667–152678, 2019.

[23] C. Rathgeb, P. Drozdowski, and C. Busch, "Detection of makeup presentation attacks based on deep face representations," in *Proc. 25th Int. Conf. Pattern Recognit. (ICPR)*, Jan. 2021, pp. 3443–3450.

[24] C. Chen, A. Dantcheva, and A. Ross, "Automatic facial makeup detection with application in face recognition," in *Proc. Int. Conf. Biometrics (ICB)*, Jun. 2013, pp. 1–8.

[25] S. Wang and Y. Fu, "Face behind makeup," in *Proc. 13th AAAI Conf. Artif. Intell.*, 2016, pp. 58–64.

[26] C. Chen, A. Dantcheva, and A. Ross, "An ensemble of patch-based subspaces for makeup-robust face recognition," *Inf. Fusion*, vol. 32, pp. 80–92, Nov. 2016.

[27] C. Chen, A. Dantcheva, T. Swearingen, and A. Ross, "Spoofing faces using makeup: An investigative study," in *Proc. IEEE Int. Conf. Identity, Secur. Behav. Anal. (ISBA)*, Feb. 2017, pp. 1–8.

[28] Z.-A. Zhu, Y.-Z. Lu, and C.-K. Chiang, "Generating adversarial examples by makeup attacks on face recognition," in *Proc. IEEE Int. Conf. Image Process. (ICIP)*, Sep. 2019, pp. 2516–2520.

[29] Y. Li, L. Song, X. Wu, R. He, and T. Tan, "Anti-makeup: Learning a bi-level adversarial network for makeup-invariant face verification," in *Proc. AAAI Conf. Artif. Intell.*, vol. 32, 2018, pp. 7057–7064.

[30] Y. Sun, L. Ren, Z. Wei, B. Liu, Y. Zhai, and S. Liu, "A weakly supervised method for makeup-invariant face verification," *Pattern Recognit.*, vol. 66, pp. 153–159, Jun. 2017.

[31] N. Erdogmus and S. Marcel, "Spoofing in 2D face recognition with 3D masks and anti-spoofing with Kinect," in *Proc. IEEE 6th Int. Conf. Biometrics, Theory, Appl. Syst. (BTAS)*, Sep. 2013, pp. 1–6.

[32] S. Liu, P. C. Yuen, S. Zhang, and G. Zhao, "3D mask face anti-spoofing with remote photoplethysmography," in *Proc. Eur. Conf. Comput. Vis.* Amsterdam, The Netherlands: Springer, Oct. 2016, pp. 85–100.

[33] I. Manjani, S. Tariyal, M. Vatsa, R. Singh, and A. Majumdar, "Detecting silicone mask-based presentation attack via deep dictionary learning," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 7, pp. 1713–1723, Jul. 2017.
[34] A. Agarwal, D. Yadav, N. Kohli, R. Singh, M. Vatsa, and A. Noore, "Face presentation attack with latex masks in multispectral videos," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW)*, Jul. 2017, pp. 275–283.
[35] S. Bhattacharjee and S. Marcel, "What you can't see can help you–extended-range imaging for 3D-mask presentation attack detection," in *Proc. Int. Conf. Biometrics Special Interest Group (BIOSIG)*, Sep. 2017, pp. 1–7.
[36] A. Ali, N. Alsufyani, S. Hoque, and F. Deravi, "Biometric counter-spoofing for mobile devices using gaze information," in *Proc. Int. Conf. Pattern Recognit. Mach. Intell.* Kolkata, India: Springer, Dec. 2017, pp. 11–18.
[37] C. Yao, S. Wang, J. Zhang, W. He, H. Du, J. Ren, R. Bai, and J. Liu, "RPPG-based spoofing detection for face mask attack using efficientnet on weighted spatial–temporal representation," in *Proc. IEEE Int. Conf. Image Process. (ICIP)*, Sep. 2021, pp. 3872–3876.
[38] M. Kowalski, "A study on presentation attack detection in thermal infrared," *Sensors*, vol. 20, no. 14, p. 3988, Jul. 2020.
[39] S. Bhattacharjee, A. Mohammadi, A. Anjos, and S. Marcel, "Recent advances in face presentation attack detection," in *Handbook Biometric Anti-Spoofing*. Cham, Switzerland: Springer, 2019, pp. 207–228.
[40] N. Damer and K. Dimitrov, "Practical view on face presentation attack detection," in *Proc. Brit. Mach. Vis. Conf.*, 2016, pp. 1–11.
[41] H. Wei, L. Chen, and J. Ferryman, "Biometrics in abc: Counter-spoofing research," in *Proc. FRONTEX 2nd Global Conf. Future Develop. Automated Border Control*, vol. 2, Warsaw, Poland, 2013.
[42] C. Busch, "Standards for biometric presentation attack detection," in *Handbook Biometric Anti-Spoofing*. Cham, Switzerland: Springer, 2019, pp. 503–514.
[43] R. Ramachandra, S. Venkatesh, K. Raja, and C. Busch, "Towards making morphing attack detection robust using hybrid scale-space colour texture features," in *Proc. IEEE 5th Int. Conf. Identity, Secur., Behav. Anal. (ISBA)*, Jan. 2019, pp. 1–8.
[44] Kryolan. *Soft Putty*. Accessed: May 24, 2023. [Online]. Available: https://global.kryolan.com/product/soft-putty
[45] G. Pan, L. Sun, Z. Wu, and Y. Wang, "Monocular camera-based face liveness detection by combining eyeblink and scene context," *Telecommun. Syst.*, vol. 47, nos. 3–4, pp. 215–225, Aug. 2011.
[46] T. Baltrušaitis, P. Robinson, and L.-P. Morency, "OpenFace: An open source facial behavior analysis toolkit," in *Proc. IEEE Winter Conf. Appl. Comput. Vis. (WACV)*, Mar. 2016, pp. 1–10.
[47] F. Schroff, D. Kalenichenko, and J. Philbin, "FaceNet: A unified embedding for face recognition and clustering," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jun. 2015, pp. 815–823.
[48] D. Sandberg. *Face Recognition Using Tensorflow*. Accessed: May 24, 2023. [Online]. Available: https://github.com/davidsandberg/facenet
[49] J. Deng, J. Guo, N. Xue, and S. Zafeiriou, "ArcFace: Additive angular margin loss for deep face recognition," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jun. 2019, pp. 4685–4694.
[50] *Machine Readable Travel Documents*, ICAO, Montreal, QC, Canada, 2021.

ROBERTO GALLARDO-CAVA was born in Madrid, Spain. He received the B.Eng. degree in software engineering and the M.Sc. degree in computer vision from Universidad Rey Juan Carlos (URJC), in 2019 and 2020, respectively, where he is currently pursuing the Ph.D. degree in computer science. His research interests include the development of several neural network approaches, morphing image processes, pattern recognition, explainable artificial intelligence, counterfactuals, biometrics, and security. He is also a member of the Face Recognition and Artificial Vision Group (FRAV).

DAVID ORTEGA-DELCAMPO was born in Madrid, Spain. He received the B.S. degree in computer engineering and the master's degree in computer vision from Universidad Rey Juan Carlos (URJC), in 2002 and 2015, respectively, and the Ph.D. degree in computer science. Before the Ph.D. degree, he was an engineer in a private company for 14 years, and he has been a Contracted Professor with URJC for six years. His research interests include the development of various neural network approaches, morphing and de-morphing processes, pattern recognition, machine learning, image processing, biometrics, and security. He is currently a member of the Face Recognition and Computer Vision Group.

JULIO GUILLEN-GARCIA received the B.S. degree in computer science from Universidad Nacional de Educacin a Distancia (UNED), in 2012, and the M.S. degree in computer vision from Universidad Rey Juan Carlos (URJC), Madrid, Spain, in 2014, where he is currently pursuing the Ph.D. degree in information and communication technologies. He is also an Assistant Professor with URJC. Prior to joining academia, he was a Consultant in the private sector and a Researcher in public sector projects with URJC and the Universidad Pública de Navarra (UPN). He is also a member of the Face Recognition and Artificial Vision (FRAV) Research Group, URJC. His current research interests include bioinspired systems, dendritic computation, multiplayer environments, artificial intelligence, and video games.

DANIEL PALACIOS-ALONSO was born in Madrid, Spain. He received the B.S. and M.S. degrees in computer science and the Ph.D. degree in advanced computation from Universidad Politnica de Madrid (UPM), in 2009 and 2017, respectively. He was a team leader in a technological consulting firm for five years. Since 2013, he has been a member of the Neuromorphic Speech Processing Laboratory, Center for Biomedical Technology (CTB). He is currently an Associate Professor with Universidad Rey Juan Carlos (URJC). In addition, he is also the Head of the Bioinspired Systems and Applications Research Group (SABIO). His research interests include three approaches, such as the biomedical area, such as stress and emotional states and neurodegenerative diseases, biometrics (XAI, pattern recognition, security, and crime), and based on teaching innovation. He is a reviewer of national and international journals. He was a recipient of several awards, such as the Doctoral Consortium Award of the Spanish Association of Artificial Intelligence, in 2013, two best paper awards, in 2016 and 2019, and the Innovative Teachers Award, in 2020.

CRISTINA CONDE received the B.S. degree in physics (electronics) from the Complutense University of Madrid, in 1999, and the Ph.D. degree from University Rey Juan Carlos (URJC), Madrid, in 2006. She was worked several years in the private sector, and in 2001, she joined URJC as an Assistant Professor. For seven years, she was the Vice-Dean of Studies with the Computer Science School. Her research interests include image and video analysis, pattern recognition, and machine learning in both, classical and biologically inspires computation. She has coordinated several national and European projects.