Reliable Face Anti-Spoofing Using Multispectral SWIR Imaging

Holger Steiner[1], Andreas Kolb[2], Norbert Jung[1]
[1]Bonn-Rhein-Sieg University of Applied Sciences, Sankt Augustin (Germany);
[2]University of Siegen, Siegen (Germany)
holger.steiner@h-brs.de, andreas.kolb@uni-siegen.de, norbert.jung@h-brs.de,

Abstract

Recent studies point out that spoofing attacks using facial masks still are a severe problem for current biometric face recognition (FR) systems. As such systems are becoming more frequently used, for example, for automated border crossing or access control to critical infrastructure, advanced anti-spoofing techniques are necessary to counter these attacks. This work presents a novel, cross-modal approach that enhances existing solutions for face verification and uses multispectral short wave infrared (SWIR) imaging to ensure the authenticity of a face even in the presence of partial disguises and masks. It is evaluated on a dataset containing 137 subjects and a variety of spoofing attacks. Using a commercial FR system, it successfully rejects all attempts to counterfeit a foreign face with a false acceptance rate $FAR_{cf} = 0\%$ and most attempts to disguise the own identity with $FAR_{dg} = 1\%$ at a false rejection rate of $FRR < 5\%$ using SWIR images for verification.

1. Introduction

Biometric face recognition (FR) has been and still is an active research topic within the past decades [15]. Under controlled conditions, current state of the art FR algorithms can achieve even better results than human recognition. Compared to other biometric traits, the face has the advantage that it can be captured easily and non-intrusively. However, in unconstrained environments, automated FR still faces problems handling varying illumination, facial expressions or poses. Especially, determining whether a recognized face is authentic or "fake", *i.e.*, a printed picture or a facial disguise, is an open issue of FR systems [5].

There are several reasons for attacking an FR system using so called *spoofs*, such as to counterfeit the face of an authorized person at access control points or to disguise the own identity when entering a football stadium although being banned [18]. Spoofing attacks range from printed photos over recorded video displayed, for example, on a mobile device, to facial disguises and masks, which might cover the face partially or completely. Recent studies clearly point out that this kind of attack is still a severe problem for current anti-spoofing techniques [5, 7, 14].

Due to the widespread availability of 3D scanners and printers, the creation of facial masks has become much easier in recent years [7]. These masks can be produced using different materials, such as plastics, resin, silicon, rubber or latex. Applying paint or makeup makes the visual appearance and texture of a mask nearly identical to a real face, thus the authentication of a face is very difficult using only the visual (VIS) light spectrum [20].

Different approaches to address spoofing attacks using additional modalities have been proposed in recent work. Such approaches include the combination of depth and texture information [13], the usage of the thermal infrared spectrum [4], as well as multispectral short wave infrared (SWIR) imaging [20, 21, 25]. Multispectral SWIR imaging is a very appealing approach, as in this spectral range human skin can be authenticated via its characteristic remission properties, which are widely independent of a person's age, gender or skin type [8].

Rather than building new multimodal FR systems, it is preferable to enhance existing VIS based systems using new modalities. This way, already existing face image databases can still be used for face verification. Different researchers, *e.g.*, Bourlai *et al.* [2] or Klare and Jain [10], have achieved promising results when using SWIR images to verify faces that have been *enrolled* using VIS images with both commercial and scientific state of the art FR software. However, SWIR-based spoofing detection in conjunction with FR has not been addressed so far.

In this paper, we propose fundamental approaches to combine the skin detection method presented by Steiner *et al.* [21] with existing FR systems, including already acquired face databases. The FR systems are treated as "black boxes" and are merely responsible of recognizing authentic faces. Thus, their performance has an influence only on the false rejection rate. The contributions of our work are:

- A cross-modal approach to detect spoofing attacks even in the presence of (partial) disguises and masks that enhances existing VIS-based solutions. It ensures the authenticity of a face captured with a multispectral SWIR camera and verified against a known face given by a VIS image in a cooperative user scenario.

- An anti-spoofing method that masks out non-skin areas at pixel level in a preprocessing step prior to FR. This requires a given FR system to be able to handle SWIR images as input.
- An alternative anti-spoofing method that verifies the authenticity of a face within a generic region of interest. This method ensures high spoof detection performance and does not impose specific constraints on a given FR system.
- To further promote anti-spoofing research, we provide a first database of corresponding multispectral SWIR and RGB color images incorporating various types of masks and facial disguises to the research community.

2. Related Work

Anti-Spoofing in the Visual Spectrum

In the past few years, several researchers have addressed the problem of spoofing attacks on face recognition systems. Using motion based approaches, *e.g.* detecting motion patterns [1] or tracking facial features to analyze the 3D structure [11, 24]), spoofing attacks using printed photos can be detected. Potential solutions for video replay attacks have also been proposed, including 3D / depth image acquisition or interactive challenge-response methods [18], analysis of the texture [16, 17], image quality assessment [6] and detection of artifacts or distortion [3, 19, 26], as well as combinations of these methods [12, 27]. However, these approaches have not sufficiently addressed the problem of detecting (three-dimensional) facial masks.

Anti-Spoofing Using Different Modalities

The detection of spoofing attacks with masks and facial disguises is not easily possible using the visible spectrum only. Different modalities have been proposed in prior work: Dhamecha *et al.* [4] proposed the combination of images acquired in the visible and thermal infrared (TIR) spectra to detect spoofing attacks. They define patches on a detected face, classify each patch as authentic or disguised and use only the authentic patches for recognition. Kose and Dugelay [13] presented an approach that combines the texture analysis of 2D facial images from [16] with 3D depth images to detect spoofing attacks with masks.

The most promising results so far have been achieved using multispectral SWIR imagery. Pavlidis and Symosek [20] described an approach for skin and disguise detection using two co-registered SWIR cameras with a sensitivity range of $800 \leq \lambda_1 \leq 1400nm$ and $1400 \leq \lambda_2 \leq 2200nm$, respectively, fused the images using weighted differences and applied a threshold to distinguish skin from other materials. Zhang *et al.* [29] presented a scanning sensor with $850nm$ and $1450nm$ wavebands as addition to an RGB camera, which distinguishes real skin from disguises at one single point in front of the camera. Wang *et al.* [25] described a multispectral method using $420nm$ and $800nm$ wavebands that divides the image of a face into blocks and creates feature vectors for each block that are compared to those acquired during enrollment, which has to be done using the same system. Yi *et al.* [28] proposed a multispectral VIS and near-infrared (NIR) camera system, which was shown to reliably detect attacks with printed photos. However, they do not report tests with facial masks or subjects with varying skin types. As their system only uses a single NIR waveband at $780nm$, it must be expected that it will not be able to distinguish real skin from skin-like material under all circumstances. Steiner *et al.* [21] presented a multispectral imaging system with 4 distinct wavebands between $900nm$ and $1550nm$ that requires only one SWIR camera. Their classification approach is capable of distinguishing authentic human skin from masks and facial disguises at pixel level with very high accuracy. Due to active frontal illumination that is invisible to the user, it is ideally suited for face recognition and verification.

A robust solution on matching the spoofing detection to specific facial features has not been introduced by any of these approaches, though.

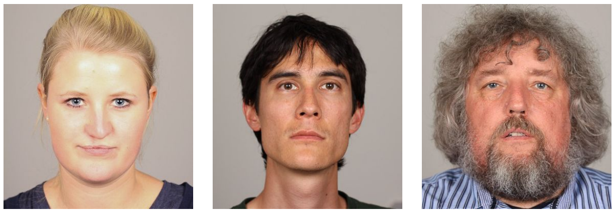


Figure 1: Portraits of different persons showing different amounts of skin in the facial region.

3. Combining Face Verification and Skin Detection

Classical biometric face recognition is limited in spoofing detection, as solely imagery in the visible spectrum is used. Methods using alternative modalities are more successful in the authentication of skin and faces as such, but often require to set up new databases for face recognition. Our approach, therefore, aims at a scheme integrating multispectral SWIR skin authentication into existing face verification systems. We will show that this approach achieves unprecedented anti-spoofing performance even in the presence of partial disguises or facial hair.

As described in Sec. 2, multispectral SWIR imaging allows for a reliable classification of material as “skin” or “non-skin” at pixel level. Even material similar to skin, such

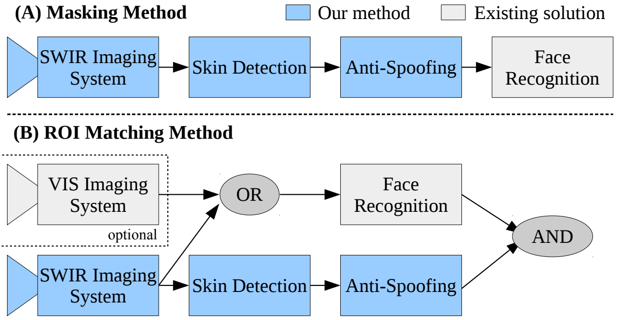


Figure 2: Components of the proposed anti-spoofing methods: (a) masking of non-skin regions; (b) ROI matching.

as silicon specifically designed to model human limbs, can be distinguished from authentic human skin with high accuracy [21]. The challenge is, how these classification results can be used for face verification, as skin regions naturally vary strongly across different individuals (see Fig. 1) and spoofs may also address very different regions and amounts of a person's face (see Fig. 3).

As it is not feasible to individually re-engineer any potentially given FR system in order to analyze its "facial regions of interest" and to apply skin verification there, we propose two fundamentally different methods to integrate SWIR-based skin detection into existing FR systems that are widely independent of the actual recognition algorithm:

(A) Masking Out Non-Skin Pixels: This method requires the given FR system to be able to handle SWIR images as input for face recognition. Here, we only acquire SWIR images, apply skin classification, and mask out non-skin regions prior to FR in a preprocessing step.

(B) Generic Regions of Interest (ROI): This method can be applied to any given FR system. In addition to the SWIR image required for anti-spoofing, a VIS image of the face can (optionally) be acquired and used for FR instead of the SWIR image. The two cameras do not need to be co-registered as long as they have a similar field of view. We apply skin classification on the SWIR image and perform anti-spoofing based on a generic ROI in a post-processing step.

In both methods, we expect that the FR systems database has been created using VIS images of all subjects. Both methods consist of the following components; see Fig. 2:

A multispectral SWIR image source with four wavebands around $935nm$, $1060nm$, $1300nm$ and $1550nm$. In this work, the BRSU Skin/Face Database [21] is used, but the presented approach can be applied to other image sources as well.

A face recognition and verification module that is considered as a black box and can be implemented using academic state of the art or commercial off the shelf software. For this work, the commercial Cognitec FaceVACS software is used in version 8.9.

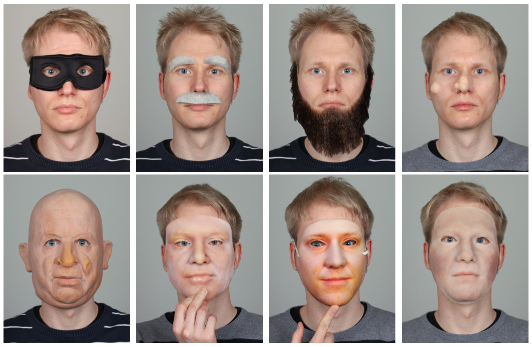


Figure 3: Examples of evaluated spoofing attacks.

An accurate SVM-based skin classifier trained on authentic skin samples, as well as new material samples recorded in the context of this work, which include different types of makeup and materials that might be used for spoofing attacks.

An innovative anti-spoofing module that detects spoofing attacks reliably without rejecting authentic faces due to facial hair or uncritical occlusion of skin. This module has two modes of operation (see above): *masking out non-skin regions* as a preprocessing to FR systems that can work on SWIR imagery as input, or *region of interest matching* as post-processing of the FR systems verification result.

In the following sections, the skin classifier and the data used for its training, as well as both methods for spatially resolved face anti-spoofing are described in detail.

4. SVM-based Skin Classifier

Steiner *et al.* [21] have shown that a highly accurate skin detection can be achieved on multispectral SWIR images by using a Support Vector Machine (SVM) classifier. They achieved a per-pixel classification accuracy of 99.968%. The skin samples that were used to train the classifier are available in the BRSU Skin/Face Database, which serves as a basis for this work. To extend the database and add training data of material used to create spoofs, new multispectral images of different masks and facial disguises have been acquired, including makeup and (fake) facial hair. This new data is provided to the research community on our website to further promote anti-spoofing research. Fig. 3 shows a selection of the considered spoofing attacks.

Similar to [21], skin classification is performed for each pixel individually by extracting its spectral signature $\vec{s}$:

$$\vec{s}(x, y) = (i_1, .., i_{n-1}), \qquad (1)$$

with $i_w, 1 \leq w < n$ being the intensity value of pixel (x, y)

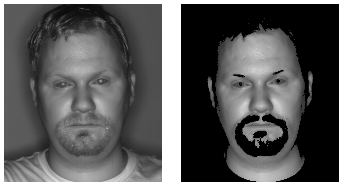


Figure 4: SWIR image before (left) and after (right) masking out all non-skin pixels.

for waveband w, normalizing it and feeding it to the classification algorithm.

Normalized spectral signatures have been extracted from all skin and material samples of the extended database described above. In total, 404 face images and 102 spoof images were used. Using the libSVM library, a new SVM classifier was trained on this data, which has been annotated by hand as “skin” or “non-skin”, respectively. As makeup, facial cream or tattoos should not be rejected as a spoofing attack per se, no such samples were used for training. Optimal parameters for the SVM learner were experimentally found by testing the resulting SVM model using cross-validation.

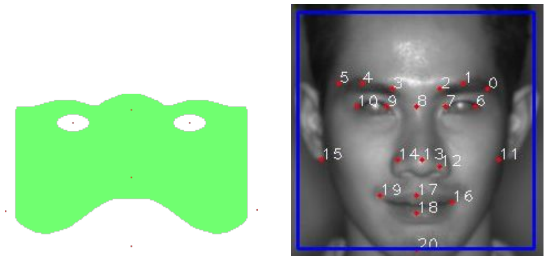
5. Masking Out Non-Skin Regions

This first method, (A), see Fig. 2, to integrate SWIR-based skin detection into existing FR systems removes, or masks out, all pixels classified as “non-skin” in the input images as a preprocessing step before the SWIR image is analyzed by the FR algorithm. As the subjects have been enrolled using VIS images, this method requires that the FR module is capable of matching these with the SWIR face images acquired for the query. The masking method is comparable to the approach described by Dhamecha *et al.* [4], but much more fine-grained, as the decision whether or not to use a certain facial area for the recognition is made for each pixel individually instead of larger patches. This ensures that no fake information will be contained in the image used for recognition. Fig. 4 shows a face image before and after masking.

6. Region of Interest Matching

Our alternative approach, (B), to masking non-skin regions verifies the authenticity of a face in a post-processing step using a generic region of interest (ROI). This method does not impose specific constraints on the FR module as such. Especially, the FR system can be fed with either SWIR or VIS query images, whatever the system requires.

As shown in Fig. 2, the anti-spoofing module uses the SWIR face image to check the authenticity of a face presented to the system. In post-processing, this information is combined with the result of the face recognition module. If a face has been verified by both the face recognition and the anti-spoofing module, it is accepted by the system.



(a) Template of the central face area.

(b) Example of a facial landmarking result.

Figure 5: Components of the ROI matching method.

6.1. Template Design

A simple approach to detect spoofing in the SWIR image would be to measure the total amount of skin in the complete image or facial region. However, this approach is too simple to distinguish spoofing attacks with partial disguises from occlusions by facial hair, as shown in Fig. 1 and 3. Furthermore, it potentially opens up new possibilities to attack the FR system.

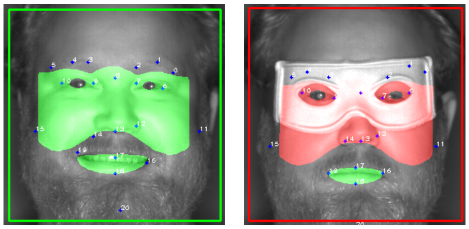
Our approach is to restrict the skin verification to regions in the human face that are commonly not occluded by facial hair: the central area around the nose and eyes, as well as the mouth. As biometric face verification systems are usually robust against changing hair styles or beards, our hypothesis is that these regions are most significant to be checked for skin authenticity.

We deduced a generic template of the central facial area, which includes only those areas that can be expected to show uncovered skin for every subject; see Fig. 5a. The template’s shape and dimension has been experimentally optimized using the BRSU Skin/Face Database, which includes several persons wearing a full beard.

6.2. Template Matching

In order to match the template to a captured image, our method uses the openCV library to detect faces and applies the facial landmark detector presented by Uricar *et al.* [22] to locate facial features. Using a previously trained model, this approach is capable of detecting a set of 20 landmarks, as shown in Fig. 5b. The algorithm is robust against (moderate) rotation and changes in perspective and allows to estimate the orientation and pose of a face with high accuracy.

After extracting the facial features, three points are derived from them: the center positions of both eyes and the mouth. These points have shown to be most stable under motion and changing illumination. Based on these points, an affine transformation matrix is calculated and applied on the template. Then, its width is adjusted to the width of the face. In addition, the features marking the outer edges of



(a) Face without mask (b) Face with partial mask

Figure 6: Results of the ROI matching method (B). *Green:* successful verification; *red:* spoof detected.

		Predicted Class	
		Skin	**No Skin**
Actual	**Skin**	99.86%	0.14%
Class	**No Skin**	1.29%	98.71%

Table 1: Pixel-level classification results on the test data.

the mouth are used to calculate form and position of the lips and the outlined area is added as a second template.

Finally, the amount of authentic skin pixels is calculated for both ROIs. As the template matching process suffers from slight inaccuracies of the landmarking algorithm, the matching is not always perfect. Therefore, the threshold for the verification has been set to 90% of the pixels in the central face area and to 50% of the pixels in the mouth area. This setting works for all faces in the database and should still be sensitive enough to detect spoofing attacks. Fig. 6 shows an example of the successful template matching.

7. Experimental Evaluation

To evaluate the performance of the proposed anti-spoofing approach, the accuracy of the skin classifier is analyzed in the first step. Then, both the masking and ROI matching methods are tested on face images with and without spoofing attacks.

7.1. Skin Classification Accuracy

The SVM classifier is evaluated on a data set of spectral signatures from skin and material samples. These samples have been extracted from images of all analyzed spoofs that have not been used for training. The confusion matrix for the full data set is shown in Tab. 1. The classifier achieves a pixel-level accuracy of 99.283% on the test data set and most spoof materials listed in Tab. 3 and Tab. 5 are distinguished from skin perfectly. The only material that is hard to distinguish from skin is artificial blood applied on a fake scar, probably due to its high water content. However, due to its liquid character, this material is difficult to be applied for spoofing attacks.

404 images in total	**(A) Masking**	**(B) ROI**
Rank-1 Identification	100 %	100 %
Above Verification Threshold	95.79 %	95.05 %
False Rejection Rate (FRR)	4.21 %	4.95 %

Table 2: False rejection rate and face verification performance of both methods using FaceVACS (trained on VIS images, queried with SWIR images).

7.2. False Rejection Rate

To evaluate the false rejection rate (FRR) of the proposed anti-spoofing methods, they are tested on the full data set of authentic (not disguised) faces. For this purpose, 137 subjects from the BRSU database have been enrolled in FaceVACS using three VIS images with varying facial expressions for each subject. The database covers subjects between 18 and 59 years of all skin types; demographic details can be found in [21], Sec. 6.2. With a few exceptions, there are also three multispectral SWIR face images available for each subject, which have been captured in the same session. From all 404 SWIR images, only the 1060nm waveband has been used for this test. As we expect a cooperative scenario, the influence of glasses has not been tested. Facial hair had no noticeable influence on the results.

As shown in Tab. 2 and Tab. 4, the performance surpasses that presented in prior work with a rank-1 identification rate of 100%. However, for some images, the *matching score* is slightly below FaceVACS' internal threshold for a successful verification result. Surprisingly, the matching score and, thus, the true positive rate is even slightly higher for the masking method than for the ROI method, which uses the unmasked image for recognition. Please note that the ROI method allows to use VIS images as input for the FR system as well, which might reduce the FRR significantly, especially under good lighting conditions. As the ROI template and acceptance threshold has been designed to accept all of these faces, see Sec. 5, no face images were falsely rejected due to an incorrect spoofing detection.

7.3. Spoof Detection and False Acceptance Rate

To evaluate the anti-spoofing performance of both methods, two attack scenarios are considered: disguise of the own identity and counterfeiting of a foreign identity. Both scenarios were evaluated using 5 subjects in total. ROC curves for both scenarios are shown in Fig. 7. It has to be noted that the printed 2D attacks and hard resin masks achieve recognition scores similar to real faces, while all other masks achieve far lower scores. Thus, the ROC curves of standard FR appear as a step function.

Counterfeiting

In this scenario, an attacker tries to counterfeit the identity

Description / no. of images		**Std. FR**	**(A)**	**(B)**
Full and partial 2D attacks	21	21	0	0
Full mask 1, silicon	3	0	0	0
Full mask 2, silicon *	3	0	0	0
Full mask 3, silicon *	3	0	0	0
Full mask 4, plastic	3	0	0	0
Full mask 5, hard resin	3	3	0	0
Full mask 6, hard resin	3	3	0	0
Sum / FAR$_{cf}$	**39**	***69.2%***	***0.0%***	***0.0%***

Table 3: Evaluated spoofing attacks for the counterfeiting scenario with number of false acceptances and total false acceptance rate (FAR) using standard FR and both anti-spoofing methods (A) and (B). 2D attacks include prints and images shown on mobile devices. * = *with makeup*.

of a specific person, for example in order to pass an automated border control gate using a fake passport. Here, a *false acceptance* occurs if the attacker is falsely verified as the person he claims to be using a spoofing attack, without the attack being detected by our anti-spoofing module. Tab. 3 presents a list of spoofing attacks from our test data set that could be used to counterfeit another person's face. For each spoof, multiple images have been captured showing variations of the attack or different attackers. Without additional anti-spoofing, all 2D attacks and hard resin masks achieve scores similar to or even higher than real faces using FaceVACS, but both proposed anti-spoofing methods successfully reject all evaluated attacks. With regard to this scenario, both achieve an FAR$_{\text{cf}}$ $= 0\%$. An example of the multispectral SWIR image of a silicon mask and its classification result compared to the corresponding RGB color image is shown in Fig. 8. Tab. 4 shows a qualitative comparison of our results to prior work.

Disguise Scenario

This scenario focuses on situations in which an attacker does not need to counterfeit a specific person's identity, but simply tries to disguise his own, for example, because his face is known and "blacklisted". Therefore, for this scenario, a *false acceptance* occurs if the attacker can hide his identity without the spoof being detected.

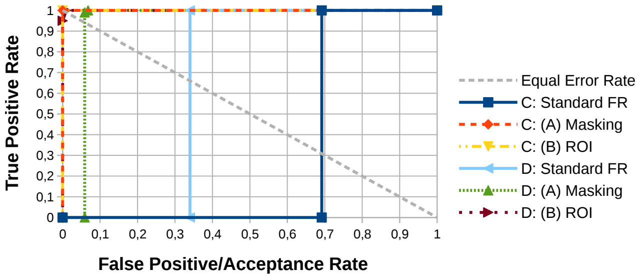
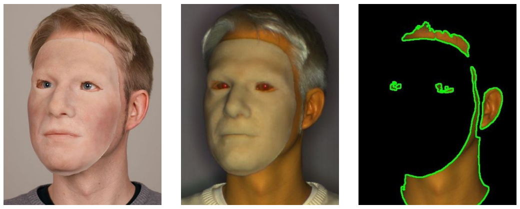


Figure 7: Receiver operating characteristic (ROC) curves for the counterfeit (C) and disguise (D) scenario.



(a) RGB image. (b) SWIR image. (c) Classification.

Figure 8: RGB color image, SWIR false-color image and classification result of a face with a silicon mask.

Method	**FPR**	**FRR**
(A) Masking	0.0	4.21 / 0.0*
(B) ROI	0.0	4.95 / 0.0*
Buciu *et al.* [3]**	2.5	6.2
Kose *et al.* [13]	14.0 / 9.1	9.8 / 18.8
Wang *et al.* [25]	3.0	3.3
Yi *et al.* [28]**	0.0	6.0

Table 4: Qualitative comparison to reported results of existing approaches on different datasets.
* = Based on Rank-1-Identification; ** = only 2D attacks

Obviously, the attacks evaluated in the counterfeiting scenario also allow an attacker to disguise his identity. Additionally, we tested several partial disguises and alterations to a face, which are listed in Tab. 5. For each spoof, the table lists the number of correct identifications (*i.e.* the attacker did not succeed with hiding his identity) and false acceptances using the standard FR system without anti-spoofing, as well as both anti-spoofing methods. For the latter, the number of detected spoofing attempts is given as well.

Without any anti-spoofing module, the FR software is easily tricked by all full face attacks, but does perform well on the partial attacks: in all but two cases, it identifies the attacker in spite of them. However, by combining several of these attacks, a successful disguise might still be possible. In total, standard FR achieves an FAR$_{\text{dg}}$ $\approx 34\%$.

Method (A) can detect spoofing attacks only by comparing face detection results before and after masking out non-skin areas. Therefore, the detection of partial disguises is not reliably possible with this method. At the same time, the disguises are more successful on SWIR images than on the VIS images used for standard FR. In combination, the attacker managed to disguise his true identity in FAR$_{\text{dg}}$ $\approx 7\%$ of the query images without the attack being detected.

Method (B) detects most of the partial disguises and misses only those that are too small or out of the specified regions, which is uncritical as these attacks are unlikely to successfully disguise the identity. Only in one image of a face with fake eyebrows and mustache, the attack is not de-

Description / number of images		**Standard FR**		**(A) Masking Method**			**(B) ROI Method**		
		Attacker ident.	False Acc.	Attacker ident.	Spoof det.	False Acc.	Attacker ident.	Spoof det.	False Acc.
Full face counterfeiting attacks *	27	0	27	0	27	0	0	27	0
Full face masks, latex	6	0	6	0	6	0	0	6	0
Partial face 2D attacks	12	12	0	6	6	0	0	12	0
Partial mask 1, unknown mat.	3	3	0	0	3	0	0	3	0
Partial mask 2, cotton on plastic	3	3	0	2	0	1	0	3	0
Partial mask 3, cotton on plastic	3	3	0	0	0	3	1	3	0
Fake nose 1, foam plastic	3	3	0	2	1	1	2	3	0
Fake nose 2, rubber latex	3	3	0	3	0	0	3	3	0
Soft nose putty (1) **	3	3	0	3	0	0	3	3	0
Soft nose putty (2) **	3	3	0	3	0	0	3	3	0
Liquid rubber latex **	2	2	0	2	0	0	2	0	0
Fake scar, latex ** / ***	3	3	0	3	0	0	3	0	0
Fake mustache, blond	2	2	0	2	0	0	2	0	0
Fake eyebrows / mustache, gray	3	3	0	1	1	1	1	2	1
Fake full beard, black	3	3	0	3	0	0	3	0	0
Fake glasses / nose / eyebrows	3	2	1	0	2	1	0	3	0
Headscarf	2	1	1	1	1	0	1	1	0
Makeup / facial cream / tattoos	18	18	0	15	3	0	18	3	0
Total	**102**	**65.7%**	**34.3%**	**45.1%**	**49.0%**	**6.8%**	**41.2%**	**73.5%**	**1.0%**

Table 5: Evaluated spoofing attacks for the disguise scenario, number of correct identifications, detected spoofs and false acceptances for standard FR without anti-spoofing (using RGB images for query), as well as both anti-spoofing methods (using SWIR images for query). ** = see Tab. 3, ** = with and without makeup, *** = with and without artificial blood.*

tected and the attacker is not identified correctly. By using a VIS image as input for the FR software instead of the SWIR image, which is optionally possible with this method, the attacker is identified correctly in this case, though. In total, the ROI method achieves an $\text{FAR}_{\text{dg}} = 1\%$.

It was further found that different skin types or (ambient) illumination conditions have no influence on the results. The same applies to most types of makeup have no influence on the SWIR images at all, except for heavy theater makeup. Eyeliner and eye shadow (both black and white), although absorbing in the SWIR and mostly being classified as "non-skin", do not influence the FR performance. If eye shadow is applied to large areas, however, it might lead to a rejection of the face. Several thick layers of powder or large amounts of facial cream that have not yet vanished can also lead to rejections, but appear to be uncritical in practice.

8. Conclusion

Nowadays, three-dimensional facial masks and disguises that defeat state of the art anti-spoofing approaches can be created without much effort. Improved methods based on multispectral images or other modalities are necessary to address this problem, as face recognition (FR) systems using the visual spectrum alone can be fooled easily.

This work presents a novel, robust and cross-modal approach that enhances existing FR solutions and ensures the authenticity of a face even in the presence of such spoofing attacks. Based on multispectral SWIR imaging, we propose an anti-spoofing method with two modes of operation: masking out non-skin pixels as preprocessing step to FR systems that can handle SWIR imagery as input or verification of a generic region of interest (ROI) as postprocessing of the FR results. Both modes are evaluated on a new database of corresponding RGB and SWIR images showing different spoofing attacks. This database is available to other researchers on our website[1] to further promote research on face anti-spoofing.

We show that both methods successfully reject all attempts to counterfeit a foreign identity with $\text{FAR}_{\text{cf}} = 0\%$. The masking method is slightly in favor with $\text{FRR}_{\text{M}} = 4.21\%$ compared to $\text{FRR}_{\text{ROI}} = 4.95\%$. Attempts to disguise the attacker's identity can be detected in most cases by the ROI method with a total $\text{FAR}_{\text{dg}} = 1\%$.

As our approach works with existing or future FR solutions and does not require an additional enrollment process, it can also be used in conjunction with template protection methods, such as fuzzy vault, which might become increasingly important for biometric systems in the near future in order to increase data protection and privacy for users [9].

In future work, training the facial landmarking algorithm with images in the $1060nm$ band could increase the reliability of the template matching in order to lower the acceptance threshold of the ROI method. Different technology,

[1] http://isf.h-brs.de/en/skin-db/

such as vein and blood vessel detection [23], could further increase the anti-spoofing performance in the presence of masks manufactured using surface materials that are very similar to skin in the SWIR spectrum.

Acknowledgments

This work was funded by the German Federal Ministry of Education and Research as part of the program FHprofUnt (FKZ: 03FH044PX3) and supported by the German Research Foundation (DFG) as part of the research training group GRK 1564 Imaging New Modalities. We also thankfully acknowledge the support of the German Federal Office for Information Security (BSI), as well as the Cognitec GmbH for providing an evaluation copy of FaceVACS.

References

[1] 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)*, pages 1–7, 2011.

[2] T. Bourlai, N. Kalka, A. Ross, B. Cukic, and L. Hornak. Cross-spectral face verification in the short wave infrared (swir) band. In *Proc. Int. Conf. Pattern Recognition (ICPR)*, pages 1343–1347, 2010.

[3] I. Buciu and S. Goldenberg. Oscillating patterns based face antispoofing approach against video replay. In *Proc. Int. IEEE Conf. Automatic Face and Gesture Recognition (FG)*, volume 02, pages 1–6, 2015.

[4] T. Dhamecha, A. Nigam, R. Singh, and M. Vatsa. Disguise detection and face recognition in visible and thermal spectrums. In *Proc. Int. Conf. Biometrics (ICB)*, pages 1–8, 2013.

[5] N. Erdogmus and S. Marcel. Spoofing face recognition with 3d masks. *IEEE Trans. Information Forensics and Security*, 9(7):1084–1097, 2014.

[6] J. Galbally, S. Marcel, and J. Fierrez. Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition. *IEEE Trans. Image Processing*, 23(2):710–724, Feb 2014.

[7] J. Galbally and R. Satta. Three-dimensional and two-and-a-half-dimensional face recognition spoofing using three-dimensional printed models. *IET Biometrics*, 2015.

[8] J. Jacquez, J. Huss, W. McKeehan, J. Dimitroff, and H. Kuppenheim. Spectral reflectance of human skin in the region 0.7-2.6m. *J. Applied Physiology*, 8(3):297, 1955.

[9] A. Juels and M. Sudan. A fuzzy vault scheme. *Designs, Codes and Cryptography*, 38(2):237–257, 2006.

[10] B. Klare and A. Jain. Heterogeneous face recognition: Matching nir to visible light images. In *Proc. Int. Conf. Pattern Recognition (ICPR)*, pages 1513–1516, 2010.

[11] K. Kollreider, H. Fronthaler, and J. Bigun. Non-intrusive liveness detection by face images. *Image and Vision Computing*, 27(3):233 – 244, 2009.

[12] J. Komulainen, A. Hadid, M. Pietikainen, A. Anjos, and S. Marcel. Complementary countermeasures for detecting scenic face spoofing attacks. In *Proc. Int. Conf. Biometrics (ICB)*, pages 1–7, 2013.

[13] N. Kose and J.-L. Dugelay. Countermeasure for the protection of face recognition systems against mask attacks. In *Proc. IEEE Int. Conf. Automatic Face and Gesture Recognition (FG)*, pages 1–6, 2013.

[14] N. Kose and J.-L. Dugelay. On the vulnerability of face recognition systems to spoofing mask attacks. In *Proc. IEEE Int. Conf. Acoustics, Speech and Signal Processing (ICASSP)*, pages 2357–2361, 2013.

[15] S. Z. Li and A. K. Jain. *Handbook of Face Recognition*. Springer, 2nd edition edition, 2011.

[16] J. Maatta, A. Hadid, and M. Pietikainen. Face spoofing detection from single images using micro-texture analysis. In *Proc. Int. Conf. Biometrics (IJCB)*, pages 1–7, 2011.

[17] L. Mei, D. Yang, Z. Feng, and J. Lai. Wld-top based algorithm against face spoofing attacks. In *Biometric Recognition*, volume 9428 of *Springer LNCS*, pages 135–142. 2015.

[18] K. A. Nixon, V. Aimale, and R. K. Rowe. Spoof detection schemes. In A. K. Jain, P. Flynn, and A. A. Ross, editors, *Handbook of Biometrics*, pages 403–423. Springer, 2008.

[19] K. Patel, H. Han, A. Jain, and G. Ott. Live face video vs. spoof face video: Use of moir patterns to detect replay video attacks. In *Proc. Int. Conf. Biometrics (ICB)*, pages 98–105, 2015.

[20] I. Pavlidis and P. Symosek. The imaging issue in an automatic face/disguise detection system. *Proc. IEEE Workshop Computer Vision Beyond the Visible Spectrum*, 0:15, 2000.

[21] H. Steiner, S. Sporrer, A. Kolb, and N. Jung. Design of an active multispectral SWIR camera system for skin detection and face verification. *J. Sensors*, 2016(1):Article ID 9682453, 2016.

[22] M. Uřičář, V. Franc, D. Thomas, S. Akihiro, and V. Hlaváč. Real-time multi-view facial landmark detector learned by the structured output svm. In *Proc. IEEE Int. Conf. Automatic Face and Gesture Recognition Workshops (BWILD)*, 2015.

[23] L. Wang and G. Leedham. Near- and far- infrared imaging for vein pattern biometrics. In *Proc. IEEE Int. Conf. Video and Signal Based Surveillance (AVSS)*, pages 52–52, 2006.

[24] T. Wang, J. Yang, Z. Lei, S. Liao, and S. Li. Face liveness detection using 3d structure recovered from a single camera. In *Proc. Int. Conf. Biometrics (ICB)*, pages 1–6, 2013.

[25] Y. Wang, X. Hao, Y. Hou, and C. Guo. A new multispectral method for face liveness detection. In *Proc. Int. Conf. Pattern Recognition (ACPR)*, pages 922–926, 2013.

[26] D. Wen, H. Han, and A. K. Jain. Face spoof detection with image distortion analysis. *IEEE Trans. Information Forensics and Security*, 10(4):746–761, April 2015.

[27] J. Yan, Z. Zhang, Z. Lei, D. Yi, and S. Li. Face liveness detection by exploring multiple scenic clues. In *Proc. Int. Conf. Control Automation Robotics Vision (ICARCV)*, pages 188–193, Dec 2012.

[28] D. Yi, Z. Lei, Z. Zhang, and S. Z. Li. *Handbook of Biometric Anti-Spoofing: Trusted Biometrics under Spoofing Attacks*, chapter Face Anti-spoofing: Multi-spectral Approach, pages 83–102. Springer London, London, 2014.

[29] Z. Zhang, D. Yi, Z. Lei, and S. Li. Face liveness detection by learning multispectral reflectance distributions. In *Proc. IEEE Int. Conf. Automatic Face Gesture Recognition (FG)*, pages 436–441, 2011.