EVALUATING THE EFFECTS OF IMAGE COMPRESSION IN MOIRÉ-PATTERN-BASED FACE-SPOOFING DETECTION

Diogo C. Garcia and Ricardo L. de Queiroz

Universidade de Brasilia, Brasil

ABSTRACT

Face-recognition biometric systems have been shown unreliable under the presence of face-spoofing images, creating the need for automatic spoofing detection. In this paper, the effect of image compression degradation on face-spoofing detection is evaluated, based on an algorithm that searches for Moiré patterns due to the overlap of the digital grids, through peak detection in the frequency domain. The proposed spoofing-detection algorithm performance is evaluated subject to H.264/AVC and JPEG image compression for an image database of facial shots under several conditions.

***Index Terms*—** Biometrics, face-spoofing detection, face recognition.

1. INTRODUCTION

Challenges in biometric systems have been thoroughly studied in recent years, in matters such as security evaluation and vulnerability assessment. Researchers and the industry are particularly interested in face recognition systems, as they offer a simple and effective method for human authentication, requiring only regular cameras and specialized software [1].

Such face recognition systems can be easily spoofed by printed photographs and mobile displays, so that several face spoofing-detection methods have been proposed [2]–[11]. Some of the employed approaches include image-quality analysis, motion analysis, texture analysis, or a combination of these.

Among the image-quality approaches, Li *et. al.* detect printed face-spoofing images with a high-frequency descriptor and a lower threshold [2]. Zhang *et. al.* detect printed and displayed face-spoofing images by searching for a lack of high-frequency information using a support vector machine (SVM) [3].

Among the motion analysis approaches, Anjos and Marcel compare features in the detected-face region and the rest of the image of a video sequence, using a multi-layer perceptron classifier [4]. De Marsico *et. al.* exploit geometric invariants with a set of facial points in different frames [5].

Among the texture analysis approaches, Määttä *et. al.* analyse local-binary-pattern codes of the detected face with a SVM [6]. Chingovska *et. al.* build upon the previous work by testing different classifiers [7]. Bharadwaj *et. al.* apply texture analysis to motion-magnified sequences [8].

Among the combination approaches, Schwartz *et. al.* analyse diverse spatial and temporal features, such as the histogram of oriented gradients, color frequency, gray level co-occurrence matrix, and histograms of shearlet coefficients, and integrate these features with a weighting scheme based on partial least squares [9]. Pereira *et. al.* employ two previous methods in order to detect face-spoofing images and videos [4],[7],[10].

These works obtain great success in face-spoofing detection, but generally rely on highly empirical methods, making it difficult to replicate them under different circumstances. SVMs, for instance, require a large training database suited for the conditions under which they will work. Furthermore, image degradation due to compression is not accounted for in previous works, which can be very important for non-local biometric systems. A more theoretical approach to 2D face-spoofing detection was previously proposed based on Moiré patterns [11], which can be modeled as the overlap of the digital grids in the face-spoofing display and in the face-recognition camera. This approach is simpler than searching for textures in the spatial domain, as it does not require large training databases for descriptors such as local binary patterns.

In this paper, we quickly review the conditions under which the Moiré patterns arise and the proposed algorithm for the detection of face-spoofing images. Next, the algorithm performance under H.264/AVC and JPEG compression is evaluated for a database of face images shot under several conditions.

2. DIGITAL ARTIFACTS ON FACE-SPOOFING IMAGES

Face-spoofing images of trusted users rely on digital media, such as printed photographs and mobile displays, as opposed to the analog reality of the trusted user. In this manner, there is an overlap between the digital grids of the face-recognition system camera and of the face-spoofing digital media, which generates artifacts such as Moiré patterns [12] [13].

In order to illustrate this, Figure 1(a) shows a portion of

E-mails: diogogarcia@unb.br, queiroz@ieee.org.

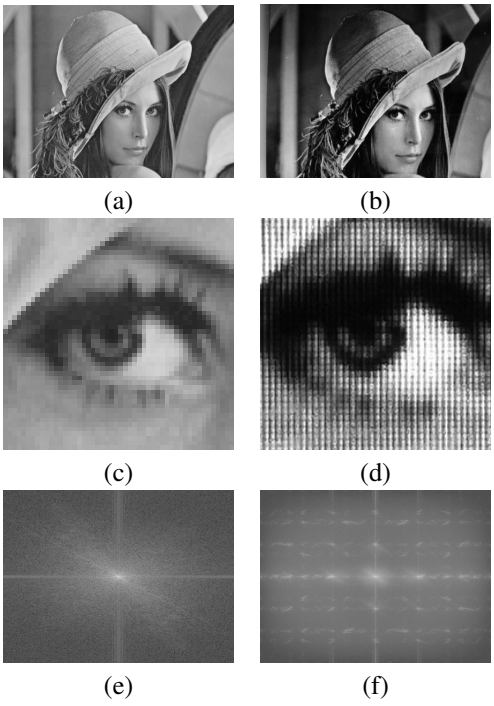

Fig. 1. Example of Moiré patterns due to the overlapping of digital grids. (a) Portion of the *Lena* test image. (b) Photograph of (a) on a 13-inch Macbook Pro screen and shot by an iPhone 4 camera without any compression artifacts. (c)-(d) Details of (a)-(b), respectively. (e)-(f) Absolute values of the discrete Fourier transforms of (a)-(b), respectively, after a logarithmic scaling for viewing purposes.

test image *Lena*, and Fig. 1(b) is a photograph of (a), captured from a 13-inch display of a Macbook Pro using an iPhone 4 camera, without any compression artifacts. Figures 1(c) and (d) show details of Figs. 1(a) and (b), respectively, illustrating the patterns that occur after an image is recaptured from a screen.

There is no *a priori* method in the spatial domain to distinguish Moiré patterns from any other, but in the frequency domain the analysis can be further simplified. Figures 1(e) and (f) show the absolute values of the discrete Fourier transforms (DFT) of Figs. 1(a) and (b), respectively, after a logarithmic scaling for viewing purposes. Figure 1(f) shows very distinctive peaks on mid and high frequencies, due to the overlapping of pixel grids between the camera and the screen.

The emergence of Moiré patterns can be more easily explained in the one-dimensional case [12] [13]. Given a continuous-space low-pass function $f(t)$, sampling it with period T_1 renders $f_s(nT_1)$, with respective Fourier transforms $F(\omega)$ and $F_s(\omega) = \sum_k F(\omega - 2\pi k/T_1)$. Displaying $f_s(nT_1)$ on a screen renders $f_{sd}(t)$, which is equivalent to the convolution of $f_s(nT_1)$ with a boxcar function, or to the multiplication of $F_s(\omega)$ with a sinc function. In that manner, $f_{sd}(t)$ presents decaying spectral repetitions of $F(\omega)$ at frequencies $1/T_1$, $2/T_1$ and so on.

After recapturing $f_{sd}(t)$ with a digital camera with sampling interval T_2, Moiré patterns will emerge if the sampling frequency $1/T_2$ on the digital camera is larger than the screen sampling frequency $1/T_1$, or $T_1 > T_2$ [13]. Otherwise, the spectral repetitions of $f_{sd}(t)$ at frequencies $1/T_1$, $2/T_1$ and so on will fall out of the frequency range of the recaptured image. Note that these spectral repetitions may be attenuated by low-pass filtering from motion blur, lens defocus, diffraction and pixel response, among others, reducing the emergence of Moiré patterns.

Although the relation $T_1 > T_2$ is crucial for the emergence and detection of Moiré patterns, it is very hard to directly measure it. The sampling interval ratio $SR = T_1/T_2$, however, can be approximated by the pixel ratio $PR = N_2/N_1$, where N_1 and N_2 represent the pixel lengths of a given feature on the screen and on the camera, respectively. This feature could be a face size, an eyes' distance and so on.

Increasing the distance from the camera to the screen reduces the capture resolution, increasing T_2 and decreasing SR. The pixel length N_2 of the given feature on the camera will decrease proportionally, and so will PR. Since it is necessary that $T_1 > T_2$ for the Moiré patterns to emerge, and assuming $SR \approx PR$, it immediately follows that:

$$PR > 1. \tag{1}$$

If this condition is met, distinctive mid- and high-frequency peaks such as those in Fig. 1(f) will appear on the DFT of the captured face.

3. FACE-SPOOFING DETECTION BY MOIRÉ-PATTERN ANALYSIS

Based on this Fourier analysis of Moiré patterns, face-spoofing detection is performed by searching for unusual peaks at frequencies other than the baseband. There is no easy way to know how much of the baseband needs to be ignored, since Moiré patterns emerge for any value of T_2 as long as $T_1 > T_2$. So, the peaks of interest may be at different frequency bands.

In essence, the algorithm works as follows. Given an image $\mathbf{I}$ of a detected face, distinct band-pass-filtered versions of this image are generated, and a peak detector is applied to the absolute value of the DFT of each of these filtered versions. If any strong peak is detected, the image is considered a face-spoofing image.

Each band-pass-filtered version of $\mathbf{I}$ ($\mathbf{I}_{BP}$) is obtained through convolution of $\mathbf{I}$ with a difference-of-Gaussians (DoG) filter [14]:

$$\mathbf{D}(\sigma, k) = \mathbf{G}(0, \sigma^2) - \mathbf{G}(0, k\sigma^2), \tag{2}$$

where $\mathbf{G}(0, \sigma^2)$ is a 2D-Gaussian function with zero mean and standard deviation σ. The width and the center of the frequency band are defined by k and σ, respectively. In the proposed algorithm, several DoG filters are tested, with σ varying from σ_0 to σ_{max} in increments of Δ.

Band-pass filtering of $\mathbf{I}$ is followed by peak detection in the frequency domain. The peak-detector algorithm is based on maximum-correlation thresholding [15], which works as follows: given any image $\mathbf{A}$, its thresholded version $\mathbf{B} = \mathcal{T}\{\mathbf{A}\}$ is defined as

$$B(u,v) = \mathcal{T}\{A(u,v)\} = \begin{cases} 1, & A(u,v) > t \\ 0, & A(u,v) \leq t \end{cases}, \qquad (3)$$

where t maximizes the correlation $\rho_{\mathbf{AB}}$ between $\mathbf{A}$ and $\mathbf{B} = \mathcal{T}\{\mathbf{A}\}$.

Maximum-correlation thresholding of $|\mathcal{F}\{\mathbf{I}_{BP}\}|$ (the absolute values of the DFT of any of the band-pass-filtered versions of $\mathbf{I}$) will emphasize peaks, if any of them is present, and very few of its pixels will have a higher value than the threshold t. If $|\mathcal{F}\{\mathbf{I}_{BP}\}|$ does not contain peaks, more of its pixels will have a higher value than t. The peak-detector algorithm consists in thresholding $|\mathcal{F}\{\mathbf{I}_{BP}\}|$ and counting the percentage p of pixels with a higher value than the threshold t:

$$p = \frac{1}{WL} \sum_{u=1}^{W} \sum_{v=1}^{L} \mathcal{T}\{|\mathcal{F}\{\mathbf{I}_{BP}\}|\}, \qquad (4)$$

where W is the image's width and L its height.

If $p < p_{min}$, $\mathbf{I}$ is considered a face-spoofing image. The value p_{min} is a simple percentage of the whole image, and it is supposed to be very small when peaks are present in $|\mathcal{F}\{\mathbf{I}_{BP}\}|$. The algorithm is repeated for different values of σ, and if no peak is found for all band-pass versions of $\mathbf{I}$, it is considered a non-face-spoofing image. The proposed algorithm is summarized in Figure 2.

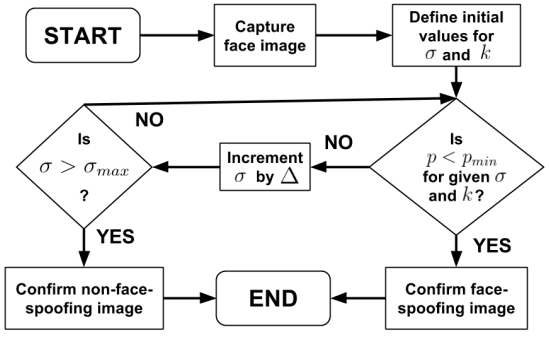

Fig. 2. Face-spoofing detection algorithm based on Moiré-pattern analysis.

4. EXPERIMENTAL RESULTS

Here, we assess the effect of H.264/AVC and JPEG compression on the algorithm performance. Since the proposed algorithm searches for peaks in the frequency domain, it will be affected by the image degradation due to quantization in the compression process. We evaluate how much compression is allowed before the algorithm offers different results as compared to the uncompressed cases.

The proposed algorithm was previously validated with a large face-spoofing database, using images of 50 individuals under 13 conditions, in a total of 650 images [11]. The face-spoofing database consists of 50 images of individuals shot under several conditions: (i) displayed on a 13-inch Macbook Pro screen and captured by an iPhone 4 camera; (ii) displayed on a 13-inch Macbook Pro screen and captured by an iPad mini camera; (iii) displayed on an iPad Mini screen and captured by an iPhone 4 camera; and (iv) displayed on an iPhone 4 screen and captured by an iPad Mini camera. In all of these conditions, images were taken at different distances from the displays. By changing the camera resolution and the distance from the displays, several pixel ratio (PR) values were obtained, In all of the aforementioned conditions, images were captured as uncompressed TIFF files [16]. Table 1 summarizes all tested conditions. The full database can be found at the url given by: http://image.unb.br/queiroz/moiredatabase.

Table 1. Tested conditions for the face-spoofing image database (L = Macbook Pro, P = iPhone 4, T = iPad mini).

Condition	**Display**	**Capture**	**Distance**	**Avg.** PR
0	Original image			
1	L	P	$\approx$ 20cm	3.88
2	L	P	$\approx$ 30cm	2.53
3	L	P	$\approx$ 40cm	1.85
4	L	T	$\approx$ 20cm	3.9
5	L	T	$\approx$ 30cm	2.61
6	L	T	$\approx$ 40cm	1.93
7	T	P	$\approx$ 15cm	3.09
8	T	P	$\approx$ 20cm	2.26
9	T	P	$\approx$ 25cm	1.98
10	P	T	$\approx$ 10cm	1.95
11	P	T	$\approx$ 15cm	1.29
12	P	T	$\approx$ 20cm	0.97

Figure 3 presents results for the false spoof rate as a function of the average pixel ratio PR, using the settings previously defined in [11]. PR is measured as the ratio of the widths of the detected faces on the capturing system (N_2) and on the face-spoofing screen (N_1). Condition 0 is not depicted, as the pixel ratio cannot be defined in this case. Under condition 0, no false positives were detected, so that the false living rate was null. Figure 3 shows that the condition in Eq. 1 holds true, and that the algorithm becomes more reliable as the pixel

ratio increases.

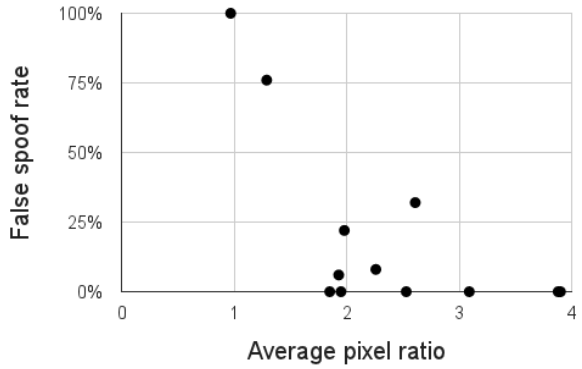

Fig. 3. False spoof rate for the proposed algorithm as a function of the average pixel ratio. The data was computed under conditions 1-12 in Table 1. Condition 0 represents non-face-spoofing images, for which the false living rate was found null.

In order to assess the effect of image compression on the algorithm performance, the images in the database were encoded and decoded with the H.264/AVC [17] and JPEG [18] standards at several rates before running the algorithm, until results different from those in Fig. 3 were obtained. Figures 4(a) and (b) show limit and average values for quantization parameters in both standards (QP for H.264/AVC, Quality for JPEG) in order to mantain the algorithm performance shown in Fig. 3, as a function of average pixel ratio.

In the H.264/AVC and JPEG standards, the amount of quantization applied to the image is determined by the parameters QP and Quality, respectively. QP ranges from 0 to 51, where 0 offers the least amount of quantization, and Quality ranges from 0 to 100, where 100 offers the least amount of quantization. Figures 4(a) and (b) show that for $PR > 1$, greater levels of quantization are allowed as PR increases. For instance, under Condition 2, $PR = 2.53$ and a limit QP value of 29 was found; that is, for all images under that corresponding condition, the algorithm performance was maintained whenever QP was lower than 30. On average, however, a more relaxed QP value of 49 was acceptable. A similar analysis can be made for JPEG compression, where the highest and average Quality values were 28 and 2, respectively, under the same condition.

Figures 3 and 4 suggest that in order to detect face-spoofing images, the proposed algorithm requires not only control over the pixel ratio, but also a limit quantization level due to compression. Pixel ratio control can be achieved by requiring a minimum size for the detected face, which controls the distance to the camera, and a minimum resolution for the capturing system. After defining the minimum acceptable pixel ratio, a limit quantization level can be defined, such as the QP value in the H.264/AVC standard and the Quality value in the JPEG standard.

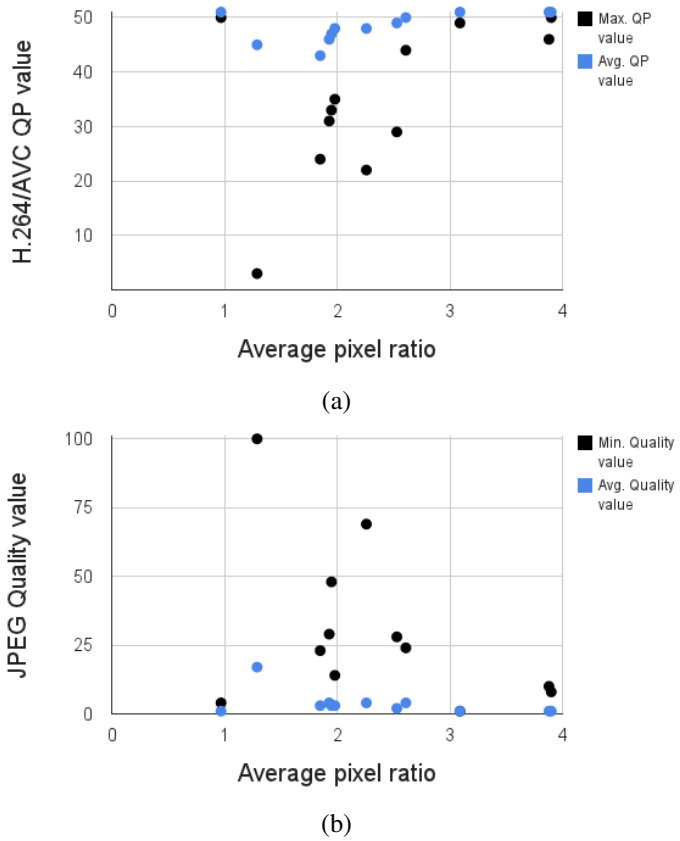

Fig. 4. Limit and average quantization parameter values used to mantain the algorithm performance (Fig. 3) as a function of average pixel ratio: (a) H.264/AVC; (b) JPEG.

Results show that for $PR > 3$ the false spoof rate can be made quite low, and the compression requirements can be greatly relaxed. These values of PR correspond to Conditions 1, 4 and 7, where the camera was disposed at an approximate distance of 15-20cm from the target.

5. CONCLUSION

In this paper, the effect of H.264/AVC and JPEG compression was evaluated for a face-spoofing-detection algorithm based on Moiré patterns. The conditions under which these patterns arise were described and experimentally verified on a database of face images shot under several conditions. Results show that face-spoofing detection depends not only on the pixel resolution of the capturing system, but also on the distance of the subject to the capturing system and on the amount of compression applied to the image prior to evaluating face spoofing. A maximum distance of 15-20cm was empirically determined for reliable face-spoofing detection, under which image compression no longer poses a problem.

6. REFERENCES

[1] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition: Security and privacy concerns," *IEEE Security Privacy*, vol. 1, no. 2, pp. 3342, Mar./Apr. 2003.

[2] J. Li, Y. Wang, T. Tan and A. Jain, "Live face detection based on the analysis of Fourier spectra," *Biometric Technology for Human Identification*, pp. 296–303, 2004.

[3] Z. Zhang, J. Yan, S. Liu, Z. Lei; D. Yi, S. Z. Li, "A face antispoofing database with diverse attacks," *IEEE Int. Conf. on Biometrics Compendium*, pp.26–31, Mar. 2012.

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

[5] M. De Marsico, M. Nappi, D. Riccio and J. Dugelay, "Moving face spoofing detection via 3D projective invariants," *IAPR Int. Conf. Biometrics*, pp.73–78, Mar. 2012.

[6] J. Määttä, A. Hadid and M. Pietikäinen, "Face spoofing detection from single images using micro-texture analysis," *Int. Joint Conf. on Biometrics*, pp.1–7, Oct. 2011.

[7] I. Chingovska, A. Anjos, S. Marcel, "On the effectiveness of local binary patterns in face anti-spoofing," *Proc. Int. Conf. Biometrics Special Interest Group*, pp.1–7, Sept. 2012.

[8] S. Bharadwaj, T. I. Dhamecha, M. Vatsa and R. Singh, "Computationally efficient face spoofing detection with motion magnification," *IEEE Conf. Comput. Vision and Pattern Recognition Workshops*, pp.105–110, June 2013.

[9] W. R. Schwartz, A. Rocha and H. Pedrini, "Face spoofing detection through partial least squares and low-level descriptors," *IEEE Int. Conf. on Biometrics Compendium*, pp.1–8, Oct. 2011.

[10] T. Pereira, A. Anjos, J. M. De Martino and S. Marcel, "Can face anti-spoofing countermeasures work in a real world scenario?," *IEEE Int. Conf. on Biometrics Compendium*, pp.1–8, June 2013.

[11] D. C. Garcia and R. L. de Queiroz, "Face-Spoofing 2D-Detection Based on Moiré-Pattern Analysis," *IEEE Trans. Inf. Forens. Security*, vol. 10, no. 4, pp. 778–786, April 2015.

[12] I. Amidror, "The theory of the moiré phenomenon, volume I: periodic layers," Springer, 2nd edition, 2009.

[13] J. Krumm and S. Shafer, "Sampled-grating and crossed-grating models of moire patterns form digital imaging," *Optical Engineering*, vol. 30, no. 2, pp. 195–206, 1991.

[14] J. Crowley and R. Stern, "Fast computation of the difference of low-pass transform," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol.PAMI-6, no.2, pp.212–222, March 1984.

[15] A. Brink, "Grey–level thresholding of images using a correlation criterion," *Pattern Recognition Lett.*, vol. 9, issue 5, pp. 335–341, June 1989.

[16] 645 Pro Mk II iOS app, in *http://jag.gr/645pro/*.

[17] "JM H.264 reference software version 18.0," in *http://iphome.hhi.de/suehring/tml/*.

[18] "ImageMagick software version 6.9.0-0," in *http://www.imagemagick.org/script/download.php*