Face Anti-Spoofing Based on Radon Transform

Razvan D. Albu, *Member, IEEE*

Abstract—**In this paper I will present a technique to generate a digital signature for an image, which will uniquely identify it, using Radon transform. Even if Radon based approaches are broadly applicable to tomography (the construction of an image from the projection data related with cross-sectional scans of it), in this research work I will show how it can be successfully utilized to classify images and detect face spoof attacks. This increased popularity of face recognition system has raised disquiets about biometric attacks, where a photo of an authorized person's face could be used by unauthorized individuals to access diverse services. The presented results prove this method offers similar performances to the state of the art and they were obtained using MATLAB 2013 environment and NUAA Photograph Imposter Database.**

Index Terms—**Radon transform, classification, spoof attacks, security, digital signature**

I. Introduction

Radon transform has numerous applications in image processing, most of them related to tomographic images reconstruction. However, in this paper I will present a new applicability of Radon transform in image classification and detection of spoof attacks.

For a given function *f*, whose domain is the plane, the Radon transform of *f* is defined, for each pair of real numbers (t,θ), by:

$$Rf(t,\theta) = \int_{s=-\infty}^{\infty} f(t*cos(\theta) - s*\sin(\theta), t*\sin(\theta) + s*\cos(\theta))ds \qquad (1)$$

The inverse Radon transform relates to the rebuilding of the function from the projections. Reformulating Radon transform it can be easily applied for shape detection in images.

$$R_{c(p)}\{I\}(p) = \int_{x\ on\ c(p)} I(x)dx = \int_{\mathbb{R}^D} I(x)\delta(c(x;p))dx \ (2)$$

Assuming Radon transform offers a mapping from image space to a parameter space p, shape detection could be reduced to the unpretentious problem of peak detection. The function formed in this parameter space, *P(p)*, comprises peaks for those p for which the equivalent shape *c(p)*exists in the image. The digital signature generated for a given image using the method presented in this research work will contain information about both basic image parameters, like luminosity and contrast, and also its shapes.

Among numerous consistent biometric approaches, face is a very popular one mainly because of its accessibility. Unfortunately, this advantage can also be expletive in spiteful circumstances, allowing aggressors to easily create copies of images with authorized faces and spoof face recognition systems. The challenge of detecting face spoofing attacks has lately earned a richly deserved attractiveness.

II. Related Works

A. Radon based approaches

In [1] the Radon transform is used to approximate camera shake by examining edges in an image. Taeg Sang Cho along with an Adobe Systems team incorporate the Radon transform within the MAP (maximum a posteriori) estimation framework to jointly estimate the kernel and the image. They experimentally show that their algorithms attain similar results with classical approaches and produce superior outputs on man-made scenes and photos degraded by a small kernel.

In [3] authors present an image reconstruction method for X-ray tomography, based on Radon transform and a set of discrete orthogonal Tchebichef polynomials. Radon Transform was also applied in recognition tasks. For example, in [4] Mirosław Miciak presented a new technique of handwritten characters recognition. The proposed algorithm is based on Radon transform and Principal Component Analysis, and it is applied to classify post mails based on zip code.

B. Recent anti -spoofing researches

Since anti-spoofing rises researchers interest, numerous methods and approaches were proposed, especially in last years. Unfortunately, none of them can claim can solve this problem and a realistic and practical solution seems to be a combinations of different methods. In [3] a very low degree of complexity method is presented. Authors claimed it is appropriate for real-time applications, using 14 image quality features extracted from one image to distinguish between legitimate and impostor samples.

For a reproducible analysis of several approaches and available public databases, researchers can study [5].A survey on anti-spoofing systems for fingerprint recognition systems is described in [6]. Useful mathematical support and results can also be found in [7] and [8].

This paper is organized as follows: after a short introduction where I introduce Radon transform and present some related research studies about anti-spoofing, I will describe the

Submision date of this paper is 30 April 2015.

Albu Răzvan-Daniel is with the University of Oradea, Department of Electronics and Telecommunications, Bihor, România (e-mail: ralbu@ uoradea.ro).

978-1-4799-7650-8/15/$31.00 ©2015 IEEE

process I have used to generate a digital signature for a given image using Radon transform, and I will present how those signature look like for both real and fake images. In this article, a real image is an image of a real human while a fake image is an impostor image, an image of another image or any other kind of pretender image (paper image, image on a screen, etc.). Then, I will present the performed experiments and some thought-provoking results. The article ends with pertinent conclusions and future working plans.

III. DIGITAL IMAGE SIGNATURE GENERATION

As I have exposed in the introduction, the goal of the presented method is to generate a digital signature that will act as a unique identifier for each image, storing also important information about contrast, luminosity and shapes.

A. The proposed method

The proposed technique to generate a digital signature of an image is presented in (Fig. 1).

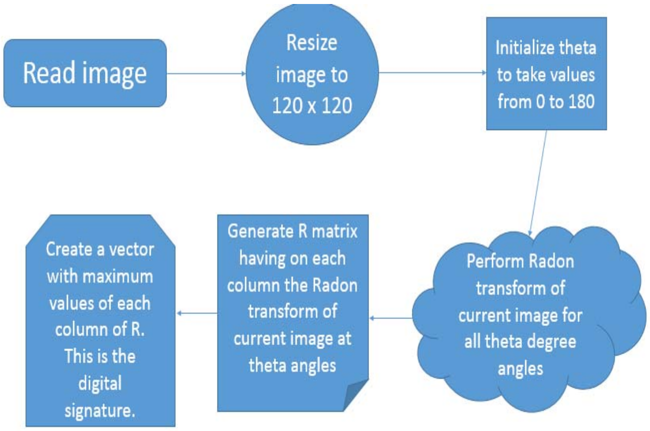
Read image
Resize image to 120 x 120
Initialize theta to take values from 0 to 180
Perform Radon transform of current image for all theta degree angles
Generate R matrix having on each column the Radon transform of current image at theta angles
Create a vector with maximum values of each column of R. This is the digital signature.

Figure 1. The process of digital image signature generation

First, I have read a color image into a MATLAB variable, determine its size, and resize it to 120 x 120 pixels. This resizing is important in order to have the same conditions of signature generation for all images. 120x120 is the value that in my experiments provided best results. The second step is to create a vector with angles for which the Radon transform will be performed. The Radon transform is the projection of the current image along a radial line sloping at each angle defined in this vector, called theta in the above diagram. As we can observe, for high accuracy and better performances, I have used values from 0 to 180 with a step of 0.1, as angles inside theta vector. Consequently, the size of theta vector is 1800. Next, the Radon transform for each angle defined in theta is performed and the R matrix is generated. Since we have 1800 angles, R will have 1800 columns, each column containing the Radon transform of current image at a particular angle. The final step is to extract from each column of R the maximum values and create a new vector with all maximums. This new vector is the digital signature I have used to identify and classify images.

The Radon transform algorithm calculates the Radon transform of an image as the sum of Radon transform of each pixels. The Radon algorithm implemented in MATLAB divides pixels into 4 sub-pixels and project each one separately. Sub-pixels contribution are also split proportionally into the two nearest bins. If the sub-pixel projection hits the center of the bin, than the bin gets the full value of the sub-pixel otherwise if the projection hits the border between two bins, the subpixel value will be evenly split between neighbor bins.

In MATLAB Radon transform of *f(x, y)* is implemented based on the following formula:

$$R_{\theta}(x^{\ddagger}) = \int_{-\infty}^{\infty} f(x^{\ddagger}cos\vartheta - y^{\ddagger}sin\vartheta, \qquad x^{\ddagger}sin\vartheta + y^{\ddagger}cos\theta)dy^{\ddagger}$$

Where:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} cos\theta & sin\theta \\ -sin\theta & cos\theta \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \qquad (3)$$

IV. ANALYZING REAL AND IMPOSTOR IMAGES

Analyzing the results obtained computing Radon signature presented above, on real and fake images, I observed few interesting aspects.

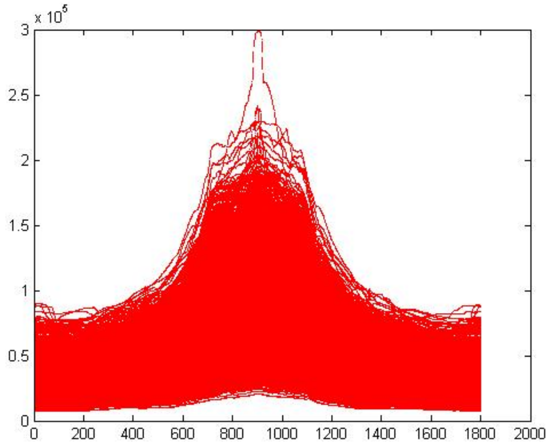

Figure 2. Radon signature of FAKE images

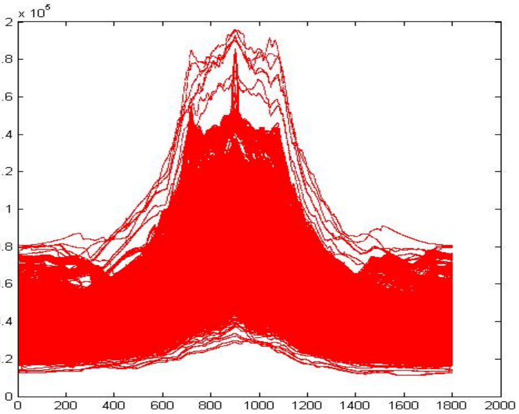

Figure 3. Radon signature of REAL images

Figure 2 illustrates the Radon signatures obtained over a dataset with more than 9000 fake images, most of them collected from NUUA impostor's database [9]. Similarly, in figure 3 are shown more than 6000 signatures of a collection of real images, obtained with various devices (smart phones and tablets). NUAA Photograph Imposter Database was created using several generic cheap webcams. They have built this database during three sessions having approximatively 2 weeks interval between them. However, the place and illumination conditions of each session were changed as well. A total of 15 subjects were invited to join this effort.

As we can observe, fake images tend to provide smoother and sharper plots than real images. We can also observe the plots for fake and real images have different shapes, amplitudes and number of spikes. Both set of plots have on OX the number of theta angles used to compute Radon transform (1800 with a step of 0.1), while on OY are Radon transform values. Withal, both sets of images (real and fakes) contain images of same persons. Since the computation of those Radon signatures plots, for almost 16000 images, could take days on a usual computer, I utilized a powerful Ultrabook, Asus G750j [10], having 32 GB of DDR3L 1600 MHz SDRAM and Intel Core™ i7 4700HQ Processor.

V. EXPERIMENTS AND RESULTS

A. *Learning only fake images*

In my first experiment, I have implemented a MATLAB script to learn fake images from a folder and then try to classify all 16000+ images, as real or fake. The main idea in this experiment is that, knowing a set of Radon signatures of fake images to try to find images that will have similar signatures. If an image will have a similar signature, it will be classified as fake otherwise will be real by default. The results of this experiment are summarized in table 1. As we can observe, a lower value of theta step (high number of angles) will not necessary provide a better classification accuracy. However, increasing the number of learned images, will provide better classification results.

TABLE I
FIRST EXPERIMENT SUMMARY

Number of learned images	Theta step	Classification accuracy
1 of 10	0.1	88.5%
1 of 5	0.1	84.2/%
1 of 3	0.1	80.8%
1 of 10	2	88.2%
1 of 5	2	83.9%
1 of 3	2	80.4%
1 of 10	21	82.9%
1 of 5	21	81.3%
1 of 3	21	89%[4]

Learning only fake images.

B. *Learning only real images*

The second experiment is similar with the first one, but, in this case, I have implemented a MATLAB script that will learn signatures of only real images, and will try to classify all images from my database. The results of this experiment are summarized in table 2.

TABLE 2
SECOND EXPERIMENT SUMMARY

Number of learned images	Theta step	Classification accuracy
1 of 10	0.1	87.5%
1 of 5	0.1	82.4/%
1 of 3	0.1	80.5%
1 of 10	2	87.2%
1 of 5	2	82.9%
1 of 3	2	81.4%
1 of 10	21	80.9%
1 of 5	21	80.6%
1 of 3	21	88.2%[4]

Learning only real images.

As we can see, again, the best accuracy is obtained using a theta step of 21 and as the number of learned images increases, (every image of 3 images with the same person is learned), the accuracy increases.

C. *Learning both fake and real images*

In the last experiment, I have performed a balanced training, creating two learning sets containing both real and fake images. Now, the MATLAB script that tests the classification capabilities of this system is changed, for each image I will compute a similarity score. If the highest similarity score is provided by a fake image signature, than the tested image is classified as fake. If the highest similarity score is provided by the Radon based signature of a real image, it will be classified as real accordingly. Table 3 summarizes the results of this experiment.

You can notice that a balanced approach, learning both real and fake signatures, provide the best results. The first experiment confirms that the optimum number of theta steps is 21 and the highest classification accuracy (97.2%) is obtained when I have trained the system to learn every image of 3 images with the same person.

TABLE 3
THIRD EXPERIMENT SUMMARY

Number of learned images	Theta step	Classification accuracy
1 of 10	0.1	92.7%
1 of 5	0.1	91.8/%
1 of 3	0.1	93.5%
1 of 10	2	93.2%
1 of 5	2	94.9%
1 of 3	2	95.4%
1 of 10	21	94.9%
1 of 5	21	95.6%
1 of 3	21	97.2%[4]

Balanced learning

VI. CONCLUSIONS AND FUTURE DIRECTIONS

In this research, I have described a new method of face anti-spoofing. The proposed method is based on Radon transform and consists of an algorithm to generate a digital signature for a given image. The presented results prove that this method can offer similar performances with current state-of-art. The key characteristics of this method are:

1) This method provides best results when it is used to learn both real and fake images.
2) The optimal number of theta steps utilized by Radon transform is 21. A lower number of theta steps means more angles at which Radon projection are computed, but this will not provide a higher classification accuracy. However, learning more images will increase the classification accuracy.
3) Learning all images of testing database will offer obviously 100% accuracy over the same database. As the number of theta steps is lower, the computation time increases, but the probability to have two images with the same signature decreases.

As future researches, I planned to compare the Radon based signature method described in this article with a similar techniques that uses Hough transform instead.

REFERENCES

[1] Taeg Sang Cho, Sylvain Paris, William T. Freeman, Berthold Horn, “Blur Kernel Estimation using the Radon Transform,” presented at IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2011.

[2] X.B. Dai, H.Z.Shu, L.M.Luo, G.N.Han, J.L.Coatrieux, “Reconstruction of tomographic images from limited range projections using discrete Radon transform and Tchebichef moments”, Pattern Recognition, vol. 43, 2010, pp. 1152—1164.

[3] Galbally, J. Marcel, S., “Face Anti-spoofing Based on General Image Quality Assessment”, [1] International Conference on Pattern Recognition (ICPR), 24-28 Aug. 2014, Stockholm, pp. 1173 – 1178, ISSN 1051-4651.

[4] Mirosław Miciak, ”Radon Transformation and Principal Component Analysis Method Applied In Postal Address Recognition Task”, International Journal of Computer Science and Applications, Technomathematics Research Foundation, Vol. 7 No. 3, pp. 33 - 44, 2010.

[5] A. Anjos and S. Marcel. ”Counter-measures to photo attacks in face recognition: A public database and a baseline” In International Joint Conference on Biometrics, pages 1 –7, October 2011.

[6] Emanuela Marasco, Arun Ross,”A Survey on Anti-Spoofing Schemes for Fingerprint Recognition”, ACM Computing Surveys, Vol. 47, No. 2, Article A, Publication date: September 2014.

[7] D. Nuzillard, S. Curilă, M. Curilă, “Blind Separation in low frequencies using Wavelet analysis, Application to artificial vision“, Fourth International Symposium on Independent Component Analysis and Blind Signal Separation, pp. 77 - 82, Avril 1-4, 2003, Nara, Japan, ISBN 4-9901531-1-1, ICA2003 Proceedings.

[8] Sorin Curilă, Cornelia E. Gordan and Mircea Curilă, “Tracking of polyhedral objects in image sequences”, 2008 IEEE 4th International Conference on Intelligent Computer Communication and Processing (ICCP 2008), August 28-30, 2008, Cluj-Napoca, Romania, Page(s):61 – 66, ISBN: 978-1-4244-2673-7.

[9] NUUA impostors database: http://parnec.nuaa.edu.cn/xtan/data/nuaaimposterdb.html (14.05.2015)

[10] Asus G750 Ultrabook: http://www.asus.com/Notebooks_Ultrabooks/ASUS_ROG_G750JX/specifications/ (14.05.2015)