RASH:RAdon Soft Hash algorithm

Frédéric Lefèbvre, Benoit Macq and Jean-Didier Legat
Laboratoire de Télécommunications et Télédetection
Université catholique de Louvain
Batiment Stevin - 2, place du Levant
B-1348 Louvain La Neuve, Belgium
E-mail:{lefebvre,macq}@tele.ucl.ac.be,legat@dice.ucl.ac.be

ABSTRACT

In this paper, we present a high compression and collision resistant algorithm for images either suitable to extract an indexing pattern of the image and to detect deformations applied to original image. Some transforms are extracting characteristics invariant against geometrical deformations (rotation and scalling). Among them, the Radon transform, largely used in magnetic resonance imaging, is also robust against image processing basic attacks (like compression, filtering, blurring, etc...) and strong attacks (Stirmark). This transformation allows to caracterize easily features of geometrical transforms. It permits also an easy extraction of an indexing vector of the image.

keywords: hash function, pattern recognition, radon transformation, digital signature, watermarking.

1 Overview

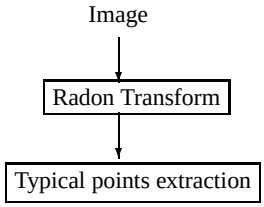
Two types of hash functions exist : Keyed Hash functions and No-Keyed Hash functions. In our case, only the second one is interesting. No-Keyed Hash functions are well known for computing bits sequences for password, document signature. These type of functions are collision resistant. For example, MD5 [1], SHA1 [2] are customized compression function in cryptographic process. To be cryptographically secure, the two important hash functions properties are:

- This hash function provides a unique output called message digest for each input. In other word, if some bits of the input are modified, the digital signature provided by hash function will differ from the original signature. It is desirable to have as few collisions as possible.
- It must be computationally infeasible to reverse the process. With the digital signature, it must be impossible to find the message.

For image application [3, 4], the second property is relevant but the first point need to be corrected in Two different images must have two different message digests. Two images are different if and only if image contents are different. The message digest must be resistant and robust, so remaining the same before and after attacks [5], if these attacks do not modify visual contents. The design of a hash algorithm is focussed on specific imaging attacks : blur, sharpening, compression, noise insertion, rotation, scaling lead to requirements which are quite different from those that are required for text document.

The Radon transformation largely used in medical image processing [6] provides a good basis for our algorithm. In fact, this transformation is robust against image processing such as sharpening, blurring, adding noise, compression, and has some invariant properties with regards to geometrical transformations such as rotation and scaling.

The amount of elements in transform domain is almost the same than the pixel domain when perfect reconstruction is required. It is however possible to reduce further the amount of transform coefficients to realize a real soft hash function. From Radon transformation, some robust and almost invariant elements can be extracted.



In the following sections, we describe our robust and invariant hash function for images with more details.

2 Radon Transform

The Radon transform is largely used in medical image processing. In tomography, when a bundle of X-Rays goes through an organ, its attenuation depends on content of organ, distance, and direction or angle of this projection.

This set of projections is called Radon transform.

In two dimensions, we can illustrate it by

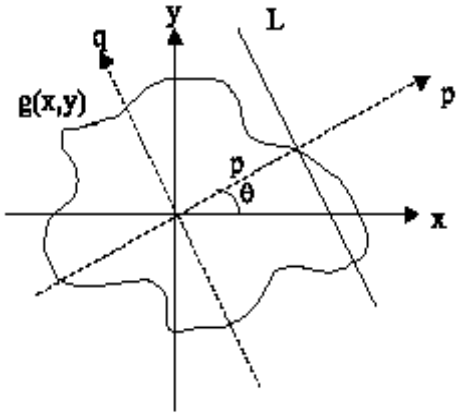


Figure 1: Projections

The figure 1 can be explained by:

$$\mathcal{R}\mathrm{g}(\mathrm{x},\mathrm{y}) = \int_{\mathrm{L}} \mathrm{g}(\mathrm{x},\mathrm{y})\,\mathrm{dl} \tag{1}$$

Where L is given by:

$$p = x.cos\theta + y.sin\theta \tag{2}$$

So each projection is an estimation of line integral of g(x,y) of θ and p. To express this integral in an other way, we can simply use a change of variable :

$$x = p.cos\theta - q.sin\theta \tag{3}$$

$$y = p.sin\theta + q.cos\theta \tag{4}$$

This new representation is:

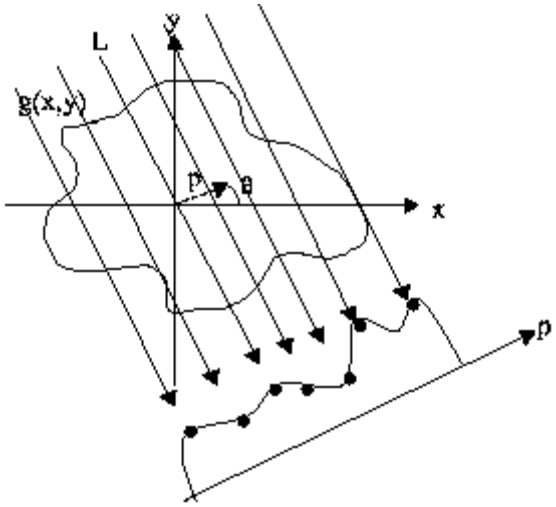


Figure 2: line integral of Radon

Mathematical equation of this transformation becomes:

$$\mathcal{R}\mathrm{g}(p,\theta) = \int_{-\infty}^{\infty} g(p.cos\theta - q.sin\theta, p.sin\theta + q.cos\theta)\,dq \tag{5}$$

Figure(3) depicts the Radon transform of Lena:

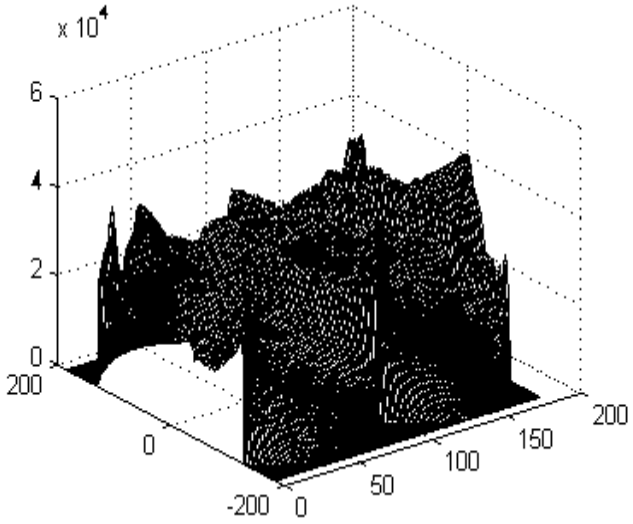


Figure 3: Radon transform

The mathematical expression of Radon transform leads to some very useful properties.

- If a set (images) g is shifted by (x_0, y_0), the Radon transform is

$$g(x - x_0, y - y_0) \longleftrightarrow \mathcal{R}\mathrm{g}(p - x_0.cos\theta - y_0.sin\theta, \theta) \tag{6}$$

- If a set (images) g is rotated by ϕ, the Radon transform is

$$g(x.cos\phi - y.sin\phi, x.sin\phi + y.cos\phi) \longleftrightarrow \mathcal{R}\mathrm{g}(p, \theta + \phi) \tag{7}$$

- If a set (images) g is scaled by a factor α, the Radon transform is

$$g(\alpha.x, \alpha.y) \longleftrightarrow \frac{1}{|\alpha|}.\mathcal{R}\mathrm{g}(\alpha.p, \theta) \tag{8}$$

- There is energy conservation in the Radon transform and in the space domain

$$\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} g(x,y)\,dx\,dy \longleftrightarrow \int_{-\infty}^{\infty} \mathcal{R}\mathrm{g}(p,\theta)\,dp \tag{9}$$

The sinograms (projections taken along the angular direction) of Lena and Lena rotated show us the rotation property of Radon Transform

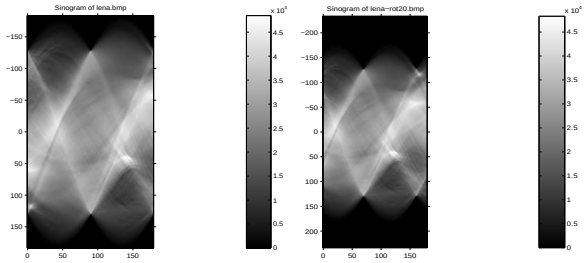


Figure 4: Sinograms of Lena and Lena rotation of 20^o

These projections give a unique representation for each image. But this set has the same cardinality than the image in space domain. Rotation and scaling spread the signal. In the Radon transform domain, we need to find some invariant points included in a set of fixed length element.

The next section develops the hash function and explains how to find these invariant and robust points.

3 Hash Function

Due to mathematical properties, rotation and scaling spread the signal. If we extract some points from each projection from each angle, it is very difficult to retrieve these points as shown in figure (5), figure (6) and figure(7).

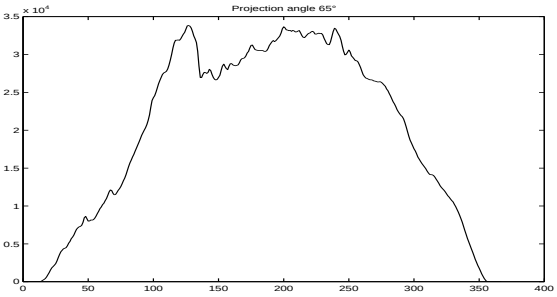


Figure 5: Projection with $\theta = 65^o$ for original image of Lena

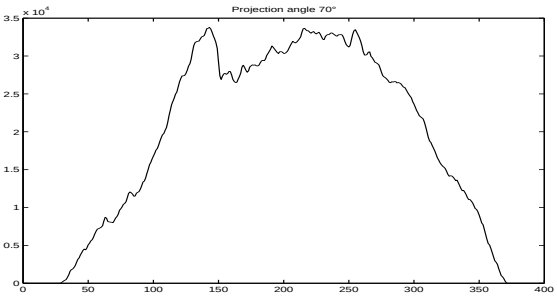


Figure 6: Projection with $\theta = 70^o$ for Lena rotation of 5^o

The X and Y ranges are never the same, they depend on the

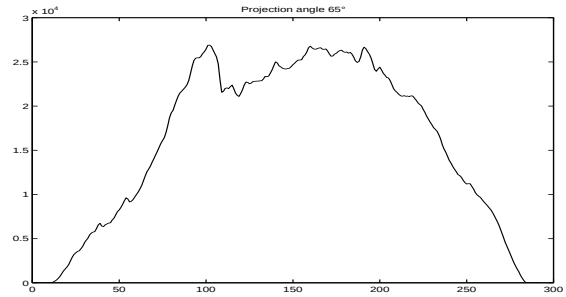


Figure 7: Projection with $\theta = 65^o$ for Lena scaling of 0.8

rotation angle and the scaling factor. To realize an efficient hash function, typical points must not be sensitive to spread range. Only one type of points are invariant: the medium points of each projection of each angle. These medium points keep all Radon transform properties as explained by figure (8). This medium points are evaluated by:

$$p_{middle} \approx \frac{\sqrt{width^2 + hight^2}}{2} \tag{10}$$

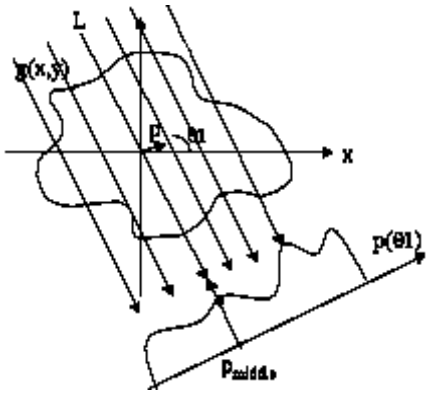


Figure 8: Typical Points extraction

Applying this extraction on all angles discretized with 1^0 sampling angle, the output set contains 180 elements, i.e one element per angle. In fact, Radon transform is symetric over 180^0 angle projection, so we only need the first 180 projections to complete our transform and to have all typical points of our image figure (9).

Mathematical properties of the Radon transform focus on an line integral in the continus domain or a summation in discrete domain. So, any attacks in space domain such as blurring, sharpenning, or stirmark modify these typical points. Furthermore, for large images, the image processing manipulations are not visible and without influence for output soft hash function. Some tests about attacks will be described in the next section.

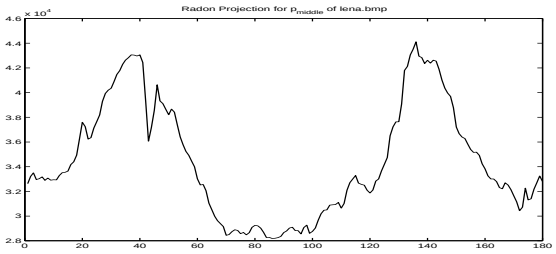


Figure 9: Radon projection for p_{middle} of lena

4 Experiments and geometrical detection

Scaling and rotation operation are separable in Radon Domain figure (10). Each modification can be detected with some signal processing tools.

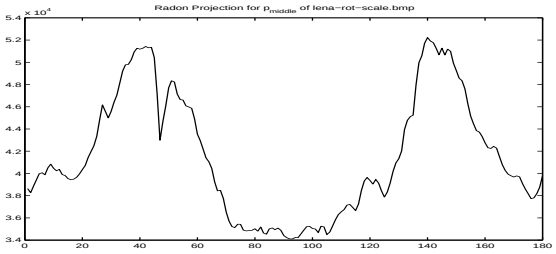


Figure 10: Radon projection for p_{middle} of Lena rotated and scaled

Energy modification is due to scaling, and shifting is due rotation. To detect geometrical attacks, we can:

- calculate the ratio between the energy of soft hash from original image and the energy of soft image scaling

$$\alpha = \sqrt{\frac{Energy(hash_{original})}{Energy(hash_{scaled})}} \tag{11}$$

- calculate and detect the top of cross covariance between original and rotated image.

$$\phi = 180 - argmax_m(R_{xy}(m)) \tag{12}$$

$$R_{xy}(m) = \sum_{n=0}^{N-m-1} \left(x_n - \frac{1}{N}.\sum_{i=0}^{N-1} x_i \right). \left(y_{n+m} - \frac{1}{N}.\sum_{i=0}^{N-1} y_i \right)$$

The following tests demonstrate the Robust and Invariant Soft hash function for Images. MSE describes the Mean Square Error:

$$MSE = \frac{\sum_{i=0}^{N-1} (x_i - y_i)^2}{N} \tag{13}$$

Ref:Lena	$max(R_{xy})$	$argmax(R_{xy})$	MSE
Lena-scale(0.8)	0.99	180	$7.4.10^{-4}$
Lena-sharpen*2	0.99	180	$1.9.10^{-3}$
Lena-blur*2	0.99	180	$7.8.10^{-4}$
Lena-stirmark	0.99	180	$4.4.10^{-3}$
baboon	0.6	181	0.8
barbara	0.65	187	0.82
fishingboat	0.45	265	1.19
houses	0.7	183	0.4
peppers	0.6	181	0.8

Figure 11: Collision and detection tests

After normalization, if the input did not come from the referenced image Lena, all message digests are different. Showing that, the soft hash function for images is robust, invariant and efficient.

5 Conclusion

We developed a new soft hash function for images. This function provides a unique message digest for each different image contents. Thanks to the mathematical properties of the Radon transform and the robustness against image processing attacks, RASH could be used in pattern recognition to retrieve an image in a database, and in watermarking process as a synchronization block to detect and rectify geometrical deformations such as rotation and scaling. The length and the non collision property of the message digest (180 values x 8 bits for quantization) is also a possible solution to sign an image.

References

[1] Ronald RIVEST "RFC 1321: The MD5 Message-Digest Algorithm." RSA Data Security Inc., April 1992.

[2] National Institute of Standards and Technology (NIST), "Announcement of Weakness in the Secure Hash Standard", 1994.

[3] Jiri FRIDRICH and Miroslav GOLJAN, "Robust Hash Functions for Digital Watermarking", ITCC 2000, Las Vegas, March 27-29, 2000, Nevada, USA

[4] C.L. SABHARWAL and S.K. BHATIA. "Perfect Hash Table Algorithm for Image Databases Using Negative Associated Values." Pattern Recognition. 28:7. pp. 1091-1101. July 1995.

[5] F.A.P. PETITCOLAS, R.J. ANDERSON and M.G. KUHN, "Attacks on copyright marking systems", in Information Hiding:2nd Workshop, vol.1525, D. Aucsmith, Ed. Berlin, Germany:Springer-Verlag, 1998.

[6] Zhi-Pei LIANG and Paul C. LAUTERBUR, "Principles of Magnetic Resonance Imaging, A Signal Processing Perspective", IEEE Press Series in Biomedical Engineering, Metin Akay, Series Editor.