A ROBUST SOFT HASH ALGORITHM FOR DIGITAL IMAGE SIGNATURE

F. Lefebvre, J. Czyz and B. Macq

Laboratoire de Télécommunications et Télédétection
Université catholique de Louvain
Bâtiment Stévin, place du Levant - 2
B-1348 Louvain-la-Neuve, Belgium

ABSTRACT

Watermarking is largely used for copyright protection and fast search of images in databases. Another method for securely identifying images is to use hash functions. Digital Signature Standard, used in cryptosystem to dispute authentication documents, is based on hash functions. A digital signature is a bit stream dependent on key and content of document. For each document, the digital signature algorithm provides a unique output bit stream. In order to be efficient in images, the digital signature should be different if and only if the image content, and not the input bit stream, is different. Our new method is a one-way function for images. Using the Radon transform and Principal Component Analysis, we extract characteristics robust against geometrical transformation (rotation and scaling) and image processing attacks (compression, filtering, blurring).

1. INTRODUCTION

The digital signature scheme was introduced by Goldwasser, Micali and Rivest[1]. This authentication scheme asserts that an adversary cannot compute the same signature with two different messages. In cryptosystems, this type of process is largely used to ensure data integrity, data origin authentication and non repudiation. The digital signature is based on a hash function (or a one way function) and an encryption algorithm [2]. In this paper, only the case of one way functions will be treated. One-way functions and cryptographics hash functions are computed by cryptographic primitives without key. For example, MD5 [3], SHA1 [4] are customised hash function in cryptographic process. A typical hash function requires the following properties:

1. **Easily computable**: A one-way function or cryptographic or hash function f has to be easily computable.
2. **Short Bit length**: A hash function f maps an input x of arbitrary bit length to an output h(x) of fixed bit length.
3. **Preimage resistant**: given an output y, for which there exists an x such as $f(x) = y$, it is computationally infeasible to compute any preimage x' such as $f(x') = y$.
4. **Collision resistant**: given any preimage x , it is computationally infeasible to find a second preimage $x' \neq x$ with $f(x) = f(x')$.

The classical signature, or message digest, is unique for any document. Given two documents, the message digests will be different if and only if the document bit streams are different. The content of a picture stored in a JPEG file and in a JPEG2000 file can be strictly identical, the classical hash function leads to different message digests, due to the different bit stream JPEG and JPEG2000 standards. Clearly, the classical definition, ”two documents are different if and only if their bit stream are different” is not applicable for digital image signature.

Fridrich [5] and Venkatesan *et al.* [6] proposed a visual hash as an alternative to watermarking based on tile division of the image. In [7], a new definition of hash functions for image applications is introduced: ”two images are different if and only if image contents are different”. Image manipulations, that do not change the content, must not affect the output of the hash function, called message digest. To fulfill the above criteria, we present in this paper a specific hash function for images based on the Radon Transform [8]. The design of the hash algorithm is focused on resistance against specific geometric image transformations: rotation and scaling, and also image processing attacks: blur, sharpening, compression. Thanks to Radon Transform invariance properties, the robustness against image rotation and scaling is intrinsically achieved. Furthermore, by extracting the second order statiscal properties of the Radon transform of the image, the message digest is sensitive to the image content but not to minor pixel modifications that arise from blurring and compression operations. Our experimental results on typical images show that the developed hash algorithm extracts different message digests for images with different contents. At the same time, the same message digest is extracted for images with the same content. The paper is organised as follows. In the next section, we describe the proposed hash algorithm and the digital signature computation. In section 3, experiment results are given and conclusions are drawn in the last section.

2. HASH ALGORITHM DESCRIPTION

The hash algorithm is based on the Radon transform. This transform is classically used in medical image processing. In tomography, X-Rays are largely used to define an organ. In fact, the bundle provided by X-Rays goes through an organ, and its attenuation depends on the content of the organ. For a specific distance and direction (or angle), this attenuation is measured and gives a projection of the organ in this direction. Each angle leads to a projection and the set of all projections is called Radon transform. Mathematically, the Radon transform $\mathcal{R}$ of a continuous function $g(x, y)$ is defined by

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

The continuous Radon transform has useful properties, some of them are listed below.

Property 1. If an image g is rotated by ϕ, its Radon transform is

$$g(x.\cos\phi - y.\sin\phi, x.\sin\phi + y.\cos\phi) \longleftrightarrow \mathcal{R}\mathrm{g}(p, \theta + \phi). \quad (1)$$

Property 2. If an image g is scaled by a factor α, its Radon transform is

$$g(\alpha.x, \alpha.y) \longleftrightarrow \frac{1}{|\alpha|}.\mathcal{R}\mathrm{g}(\alpha.p, \theta). \quad (2)$$

Basically, the first property states that the Radon transform of a rotated image is simply translated by the corresponding angle. The second property shows that when an image is scaled, its Radon transform is scaled by the same factor and the magnitude is simply divided by the scale factor. We applied the Radon transform principle to digital images. Given an image, the luminance of image pixels $g(i, j)$ are summed up along a set of directions (see fig.(1)). This operation is repeated for 180 directions uniformally distributed on a half circle and defines 180 projections of the image. Formally, for $\theta = 0, 1, ...179$, we compute 180 projections

$$p_i(\theta) = \frac{1}{N_{i\theta}} \sum_j g(i\cos\theta - j\sin\theta, i\sin\theta + j\cos\theta)$$

where $N_{i\theta}$ is the pixel number along direction θ. The projection $p_\theta(i)$ is therefore the average luminance of the image in direction θ. The purpose of the normalisation is to keep the magnitude of p_θ between 0 and 255. The image content is better described by the *variation* of the projections rather than the projection themselves, which depend on the average luminance value of the image. To achieve robustness against average luminance changes, we use the projection angular increment $w_\theta(i) = p_\theta(i) - p_{\theta-1}(i)$ to generate the image signature. We introduce a set of N 180-dimensional vectors $v_i(\theta)$, that we call Radon vectors, by taking the ith value of of the angular increment $w_\theta(i)$ for the 180 directions. The number N depends on the size of the image. For a square image with size n, we have $N = \lfloor\sqrt{2}n\rfloor$. Although the two properties cited above are not valid for discrete functions, a good approximation of the Radon transform of rotated and scaled images can be found using a discrete version of equations (1) and (2).

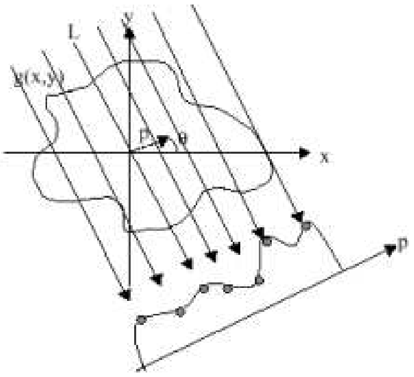

Fig. 1. Line integral of the Radon transform

Let v_i^ϕ and v_i^α correspond to Radon vectors of an image rotated by ϕ and scaled by a factor α respectively. It can be shown that

$$\begin{aligned} v_i^\phi(\theta) &\approx v_i(\theta + \phi) && \text{for } \theta + \phi \leq N \\ v_i^\phi(\theta) &\approx v_i(N + \theta - \phi) && \text{for } \theta + \phi > N. \end{aligned}$$

In other words, the Radon vectors undergo a cyclic shift during a rotation.

In order to fulfill the digital signature requirements cited in the introduction, we must extract a short and fixed length bit string from the Radon vectors of an image, that characterises as well as possible this image. To achieve this, we extract two vectors from the Radon vectors using a method inspired by Principal Component Analysis (PCA) [9]. PCA is a data analysis tool that relies on second-order statistics and extracts the most “important” part of a signal. Here, we have N vectors that we want to characterise using a small set of numbers. From the N Radon vectors v_i corresponding to an image, we estimate the covariance matrix of the v_i

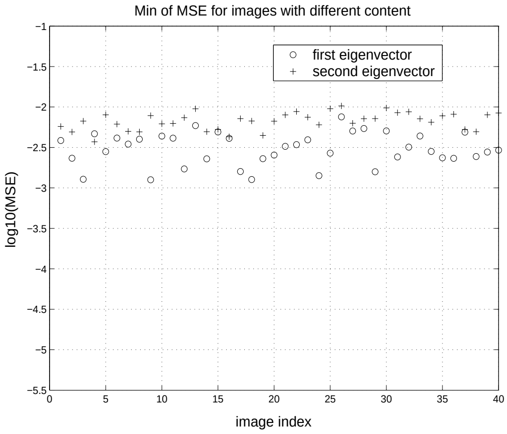

Fig. 2. Minimum MSE for signature matching between images with different content.

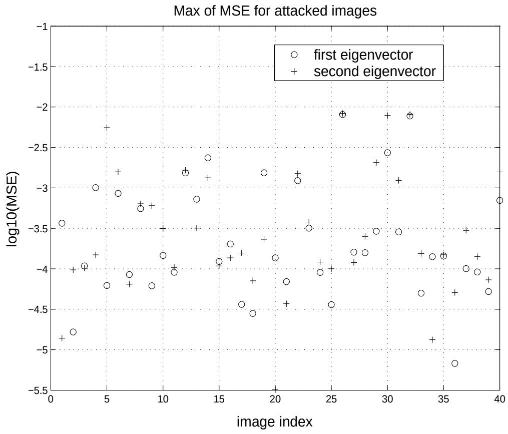

Fig. 3. Maximum MSE for signature matchings between images with the same content.

by

$$\Sigma = \sum_{i}^{N}(v_i - \mu)(v_i - \mu)^T$$

where μ is the v_i mean, i.e. $\mu = \frac{1}{N}\sum_{i}^{N} v_i$. We extract the eigenvectors of Σ corresponding to two largest eigenvalues, and these vectors form the digital signature of the image. This process has a geometrical interpretation: the set of N Radon vectors that characterises a given image can be seen as a set of N points, forming a cloud in a 180-dimensional space. The eigenvector with maximum eigenvalue of the covariance matrix corresponds to the direction where the cloud has maximum variance. This direction is therefore a global statistical property of the points that will be little affected by small changes in the points resulting from small changes in the image. In contrast, the global configuration of the points will change when the image content is different, hence the direction with largest variance will change as well. If the image is rotated, its Radon vectors are cyclically shifted. It can be shown that the eigenvectors of the Radon vector covariance matrix are shifted in the same way. If the image is scaled, the same signal is resampled more densely or more sparsely depending on whether the size increases or decreases. The same resampling happens for the Radon vectors. In fact, the number of points forming the cloud changes but its global configuration remains the same, leading hence to the same direction with largest variance as the original image.

When two signatures x and y of two images have to be matched in order to determine whether the two images have the same or different contents, we compute the cross-correlation R_{xy} between the two signatures

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

where d is the length of the signature. Since cross-correlation compares the two signals at different values of shifting, when the two signatures come from images with the same content, $R_{xy}(m)$ will be close to 1 for a certain m^*. In fact, m^* corresponds to the angle between the images in the case of two rotated version of the same images. In our implementation, the two signatures are re-synchronised using m^* and the Mean Square Error (MSE) between them is computed using

$$MSE = \frac{\sum_{i=0}^{d-1}(x_i - y_i)^2}{d}.$$

The MSE determines if the signatures come from images with the same content.

3. EXPERIMENTS

In order to evaluate the robustness and the collision resistance of the proposed algorithm, we performed experiments on real images taken from the USC-SIPI database [10]. The USC-SIPI image database is a collection of digitised images which are free of copyrights if used in image processing research. The miscellaneous sub-set consists of 40 images like baboon, Lena and peppers, of various sizes such as 256x256 pixels, 512x512 pixels, or 1024x1024 pixels. All colour images are transformed into 8 bits/pixel gray level images.

For each image, we performed a series of 8 image processing attacks:

- **Filtering**: 3x3 Gaussian filtering with standard deviation of 0.5 and 3x3 averaging filtering.
- **Compression**: JPEG compression 25%, JPEG compression 15%,
- **Geometric**: scaling with scaling factor α = 1.2 and 0.8, 2 degree rotation and 1 degree rotation with cropping.

Cross-correlation and MSE are computed (after re-synchronisation) between the original and the modified image signatures. Hence 320 matchings are done between images with the same content, we call them intra-image matchings. For comparisons between images with different contents (inter-image matchings), we matched each image signature from the database against the 39 remaining image signatures. This gives 40x39/2 = 780 inter-image matchings. For the 40 images in the database, figure 2 shows the minimum MSE from these 39 matchings, that is, the MSE between the two closest signatures when the image contents are different. Circles are plotted when the first eigenvector is used as signature, while crosses are plotted when the second eigenvector is used. Figure 3 shows the maximum MSE for each image signature matched with the 8 corresponding attacked image signatures. Hence only $\frac{1}{8}$ of the intra-image matchings is shown. From this figure, it appears most of the MSE's are below 10^{-3} for intra-image matchings, only 8 attacked images (on 320) lead to MSE's greater than 10^{-3}. For inter-image matchings there is no MSE under 10^{-3}. Using the MSE, we can therefore determine with a certain confidence if two signatures come from the same image or from two different images. It appears that the images leading to high intra-image MSE contain a lot of high frequency textures. This suggests that the signature is not well adapted to these kind of images. It is likely that the first eigenvector characterising the Radon vectors is not well defined in case of texture.

4. CONCLUSIONS

We presented a soft hash function algorithm for digital images. Using a modified definition of digital signature for images, the algorithm outputs a short bit string (180 real numbers) that depends on the image content rather than the image bit stream. This signature can be used for copyright purposes or fast searches in image databases. In the algorithm development, care has been taken for robustness to rotation and scaling by designing a method based on Radon transform and Principal Component Analysis. Our experimental results show that the digital signature is quite robust to popular image processing attacks, such as JPEG compression. Future work will be devoted to study resistance to other attacks, like stirmark [11] and to increase robustness for texture images.

5. REFERENCES

[1] O. Goldreich, "Two remarks concerning the Goldwasser-Micali-Rivest signature scheme," Tech. Rep., MIT Laboratory for Computer Science, September 1986.

[2] National Institute of Standards and Technology (NIST), "Digital siganture standard (dss)," Tech. Rep., FIPS PUB 186-2, 2000.

[3] Ronald Rivest, "Rfc 1321: The md5 message-digest algorithm," Tech. Rep., RSA Data Security Inc., 1992.

[4] National Institute of Standards and Technology (NIST), "Announcement of weakness in the secure hash standard," Tech. Rep., 1994.

[5] F.Fridrich, "Robust bit extraction from images," in *Proc. of the IEEE ICMCS, Italy*, 1999.

[6] R. Venkatesan, S.-M. Koon, M. H. Jakubowski, and P. Moulin, "Robust image hashing," in *Proc. of the IEEE International Conference on Image Processing*, 2000.

[7] F.Lefebvre, B.Macq, and J.-D.Legat, "RASH: Radon soft hash algorithm," in *Proc. of the European Signal processing Conference EUSIPCO2002*, 2002.

[8] Zhi-Pei Liang and Paul C. Lauterbur, *Principles of Magnetic Resonance Imaging, A Signal Processing Perspective*, IEEE Press Series in Biomedical Engineering, 1999.

[9] K. Fukunaga, *An Introduction to Statistical Pattern Recognition*, Academic Press, 1990.

[10] "USC-SIPI image database," available at http://sipi.usc.edu/services/database/Database.html.

[11] F.A.P. PetitColas, R.J. Anderson, and M.G. Kuhn, "Attacks on copyright marking systems," in *in Proceedings of the 2nd Workshop on Information Hiding*, D. Aucsmith, Ed. 1998, vol. 1525, Springer-Verlag.