

Ridgelet Signature for Image Authentication

Zhen Yao, *Student Member, IEEE* and Nasir Rajpoot, *Member, IEEE*

Abstract—In this paper, we describe a novel content-based image signature for authentication using the ridgelet transform. The signature is extracted from the Radon domain and entropy coded after a 1D wavelet transform, which is essentially the so-called “ridgelet transform”. Unlike traditional authentication signatures, it has the ability to localise tampering at a high resolution, also the robustness to content-preserving manipulations such as compression and allows a progressive authentication.

Index Terms—Authentication, signature, ridgelet transform, Radon transform, watermarking

I. INTRODUCTION

TRADITIONAL data authentication and integrity verification are done by appending a hashed signature of the file, usually encrypted with a secret key. The signature is practically “unique” and distributed with the file. However, the proliferation of multimedia data over the Internet poses some new authentication requirements, such as localising tampering and semi-fragility. Unfortunately these are the realms that traditional signature-based system fails and alternative approaches such as authentication watermarks [1], and content-based robust signatures [2], [3] have become popular in the research community.

A watermark, usually involves some form of steganography, is a code embedded into a host image. The authenticity of the image can be verified by checking the integrity of the watermark. Since attacks on the host image also destroy the watermark correspondingly on the same position, tampering localisation can be achieved. However there is a fundamental trade-off between security and localisation. One must establish a neighbourhood dependency in the watermark otherwise it is vulnerable to counterfeiting attacks [4]. Moreover, since the process of watermarking itself introduces distortion on the host data, it is sometimes not desirable in some applications such as with medical images. Although a few reversible watermarks have been proposed [5], their localisation abilities are however constrained by the data hiding capacity.

It has been pointed out by Shannon [6] that for a perfect secrecy system, the key K , must be at least as long as the message M , more precisely, that $H(K) \geq H(M)$, where $H(\cdot)$ denotes the entropy function. Intuitively, this says that in order to achieve perfect security, the key has to be long enough to describe the message. This is true in a case when authentication is checked with a signature, a perfectly secure signature is essentially a compressed form of the image. For example, many content-based signatures are extracted from domains such as DCT (Discrete Cosine Transform) and DWT

(Discrete Wavelet Transform) domain which are also popular choices for compression [7]. Such ideas were exploited in the watermarking world in the form of self-embedding, where a redundant lower-resolution copy of the image is embedded in order to detect and recover tampering. Despite the extra communication cost, the advantage of signature-based authentication is apparent: First, it does not introduce distortion on the original image. Second, it can solve the dilemma of security-localisation uncertainty, if the signature is considered as the lossy-coded version of the image, since a longer signature can offer better security as well as localisation resolution. Third, a compact signature can be combined into a watermarking system just as many watermarking schemes do employ such label-embedding approach.

Recently, motivated by the need for finding better representations for nature images, several geometric wavelets (eg. ridgelet [8] and curvelet [9]) have been proposed. The underlying Radon transform plays an essential role in providing such non-separable, directional properties. Although Radon-based signatures have been previously proposed [10], which take the advantage of invariant features of the transform to provide robustness functionality, but few address the problem of localisation, which is the key motivation of this work.

The rest of the paper is organised as follows. In the next section, a brief review of Radon and ridgelet transforms is presented. Next we discuss how authentication and localisation can be achieved by a number of Radon vectors and how to generate a compact signature using the ridgelet transform. Next we show the signature is able to provide a robustness measure on images, based on the work in [10]. Some experimental results are presented and the paper concludes with comments on the proposal and future directions of research.

II. RADON AND RIDGELET TRANSFORMS

The Radon transform, which has been mainly used in tomography reconstruction, is now gaining popularity in image processing as a general tool. Mathematically the continuous Radon transform of an integrable bivariate function $f(x, y)$ is defined by

$$R_f(\theta, t) = \int_{\mathbb{R}^2} f(x, y) \delta(x \cos \theta + y \sin \theta - t) dx dy \quad (1)$$

One important theorem for the Radon transform is the Fourier slice theorem:

Theorem 1: (Fourier Slice Theorem). *The 1D Fourier transform with respect to t of the projection $Rf(t, \theta)$ is equal to a central slice, at angle θ , of the 2D Fourier transform of the function $f(x, y)$, that is,*

$$\hat{R}f(\theta, t) = \hat{f}(\xi \cos \theta, \xi \sin \theta). \quad (2)$$

Z. Yao is with the Computer Science Department, University of Warwick, CV4 7AL UK. E-mail: yaozhen@ieee.org

N. Rajpoot is with the Computer Science Department, University of Warwick, CV4 7AL UK. E-mail: nasir@dcs.warwick.ac.uk

where

$$\hat{f}(\xi_1, \xi_2) = \int \int f(x, y) e^{-2\pi i(x\xi_1 + y\xi_2)} dx dy.$$

is the 2D Fourier transform of $f(x, y)$.

In need, such property is widely used in implementing discrete Radon transforms. However, strictly speaking, this continuum approach could be problematic since it is not naturally defined on Cartesian digital data while the radial slices typically requires interpolation. In order to guarantee invertibility. Therefore discretisation has been a major difficulty in applying Radon transform to general image processing, especially coding. The simplest form of discrete Radon transform is to select finite number on the angular variable of projection, then take the summation on the discrete image along the projection line. Some authors [11], [12], [13] have attempted to exploit two-scale relations, which say that if one knows the Radon transform over four dyadic subsquares of a dyadic square, these can be combined to obtain the Radon transform over the larger square. This suggests a recursive algorithm, in which the problem is broken up to the problem of computing Radon transforms over squares of smaller sizes which are then recombined. The finite Radon transform [14], which is used in Do and Vetterli's ridgelets [15] uses a combinatorial approach and is defined on an algebraic finite group. Averbuch et al. [16] proposed a notion of discrete Radon transform called *Fast Slant Stack* which is algebraically exact, geometrically faithful and invertible, but introduces a fixed amount of redundancy at rate of 4.

The Radon transform is a linear transform and like the Fourier transform, has several useful properties.

Property 1: If the function $f(x, y)$ is translated, its Radon transform is

$$f(x - x_0, y - y_0) \Leftrightarrow R_f(\theta, t - x_0 \cos \theta - y_0 \sin \theta) \quad (3)$$

Property 2: If the function $f(x, y)$ is rotated by ϕ , it corresponds to a shift translation in the Radon transform.

$$f(x \cos \phi - y \sin \phi, x \sin \phi + y \cos \phi) \Leftrightarrow R_f(\theta + \phi, t) \quad (4)$$

Property 3: If the function $f(x, y)$ is rescaled by a factor of a , its Radon transform is

$$f(ax, ay) \Leftrightarrow \frac{1}{|a|} R_f(\theta, at) \quad (5)$$

The ridgelet transform, introduced in [8], has the continuous form of

$$CRT_f(a, b, \theta) = \int_{\mathbb{R}^2} \psi_{a,b,\theta}(x, y) f(x, y) dx dy \quad (6)$$

where the ridgelet $\psi_{a,b,\theta}(x, y)$ in 2-D are defined from a wavelet-type function in 1-D $\psi(x)$ as

$$\psi_{a,b,\theta}(x, y) = \frac{1}{\sqrt{a}} \psi \left(\frac{x \cos \theta + y \sin \theta - b}{a} \right) \quad (7)$$

Since Radon transform projects a linear-singularity into a point-singularity, the wavelet and ridgelet transforms are linked via the Radon transform. More precisely, the definition in equation (6) can be re-written as

$$CRT_f(a, b, \theta) = \int_{\mathbb{R}} \psi_{a,b}(t) R_f(\theta, t) dt \quad (8)$$

where $\psi_{a,b}(t) = a^{-1/2} \psi((t - b)/a)$ is a 1-D wavelet.

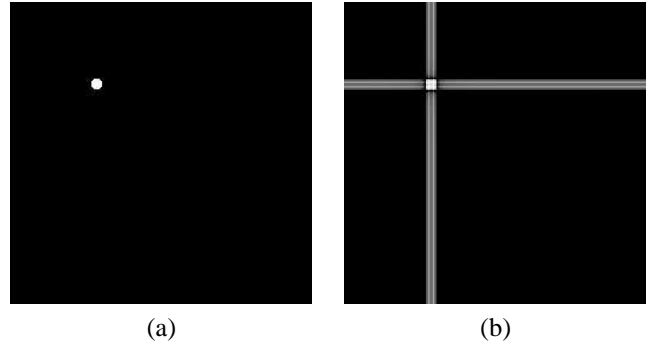


Fig. 1. (a) A point-wise singularity and (b) its back-projected reconstruction from two Radon vectors at orthogonal angles.

III. SIGNATURE GENERATION

Although the ridgelet enjoys some elegant mathematical properties, and it does in fact exploit the fact that nature images exhibit linear regularity along contours and edges. The success of its application in image representation has been limited to geometrically regular objects [15]. However, for tampering detection, a decent representation for the image is less important than representing the tampered location and a key characteristic of malicious attacks is that they are usually locally singular. Naturally, the Radon transform is capable of capturing the location of such singularity due to its directionality in projections.

In the simplest case, consider an image with a point-wise singularity (see figure 1). Two Radon vectors (i.e. the discrete angular projection) at orthogonal angles are sufficient to determine its location. Of course, it is not sufficient when there is more than one singularity, which rises ambiguity, nor can it determine the exact geometrical shape of such singularity. However, the resolution increases as more number of Radon vectors are used in reconstruction. This motivates us to use Radon vectors as the signature of the image, but the eventual signature is ridgelet transformed, since wavelet can provide a sparse representation in a multi-resolution framework which is useful for compression.

The signature generation algorithm can be described as follows.

- 1) For a set of angles $\Theta = \{\theta_1, \theta_2, \dots, \theta_n\}$, where $\theta_i \in [0, \pi]$, preferably evenly spaced, typically with $n > 20$, compute the normalised Radon vectors at these angles as follows.

$$\mathcal{R}_i(\theta_i) = \frac{1}{N_{\theta_i}} \sum_j f(i \cos \theta_i - j \sin \theta_i, i \sin \theta_i + j \cos \theta_i).$$

- 2) Apply an L -level DWT on the Radon vectors $\{\mathcal{R}_i\}$ to obtain the ridgelet representation, denoted as $\{\mathbf{w}_i\}$.
- 3) Entropy code the ridgelet coefficients with traditional entropy coders such as arithmetic code.
- 4) The signature is stored/transmitted with low-pass band first, then from smaller bands to larger bands progressively in encrypted form.

It should be noted that since Radon transform takes a summation over the image support, the Radon vectors can be considered as *global* information. There is an inherent

directional *neighbourhood dependency* in the projected vectors and they are also correlated. Therefore it is not possible to perform the counterfeiting attack on the image.

The verification process is simply as follows. Once we have retrieved the image \hat{f} and the signature, we apply the ridgelet transform on \hat{f} as described before but without the entropy coding to obtain $\{\hat{\mathbf{w}}_i\}$, while $\{\mathbf{w}_i\}$ can be decoded from the signature. If the image is original, $\{\hat{\mathbf{w}}_i\}$ and $\{\mathbf{w}_i\}$ should be identical. If not, their reconstructions should exhibit the difference between the tampered image \hat{f} and the original copy f . Since Radon and wavelet transforms are both linear, $\{\mathbf{w}_i - \hat{\mathbf{w}}_i\}$ is the (undercomplete) ridgelet representation of $f - \hat{f}$. We take the inverse ridgelet transform on $\{\mathbf{w}_i - \hat{\mathbf{w}}_i\}$ to observe the difference.

IV. ROBUSTNESS MEASURE ON THE SIGNATURE

The invariance of the Radon transform can be used to provide a robustness measure on the image. This problem was studied in [10] by performing the Principle Component Analysis (PCA) on Radon vectors. First, they obtain a finite number of Radon projected slices, typically 180 of them, then calculate the covariance matrix V and its eigenvalues with corresponding eigenvectors. The principle component, or the major axis in the point-cloud by the covariance matrix V is the corresponding eigenvector to the biggest eigenvalue. In [10], they take the largest and second largest eigenvector as the signature. Since they correspond to the major two orthogonal axes with largest variances, they are robust under several attacks. Some of them are briefly listed here:

- **Lowpass filtering.** Since the principle component in the dataset represents the most correlated element, it essentially is the lowpass of the signal, obvious is invariant to lowpass filtering.
- **Noise.** Generally speaking, noises are uniform uncertainties. Since a lowpass filtering is a common technique to remove noises, the signature should resist noises as well.
- **Compression.** A lossy compression procedure can be viewed as approximation using a set of basis functions. It discards mostly high frequency content therefore similar to the case of lowpass filter.
- **Rotation.** A rotation in the spatial domain corresponds to a cyclic shift in the Radon domain, resulting the same shift in the eigenvectors.
- **Scaling.** The scaling in the spatial domain corresponds to a scaling in Radon slices, which in a statistical sense can be regarded as sub/over-sampling. This has subtle impact on the principle components.

Such approach seems reasonable to be applied with wavelet transformed Radon vectors as well, since a norm-preserving linear transform should not change the outcome of PCA. However, the rotational invariance is almost lost in our approach, since relatively a few (usually less than 20) Radon slices are being used. It could accept rotated versions directly at some specific angles, or otherwise rotate the received image in a full range of angles to see if any angle could be accepted. But it is by no means efficient and not practically useful.

In our scheme, the PCA is performed on the signature $\{\mathbf{w}_i\}$ and $\{\hat{\mathbf{w}}_i\}$ from the received image \hat{f} , and we obtain the robust

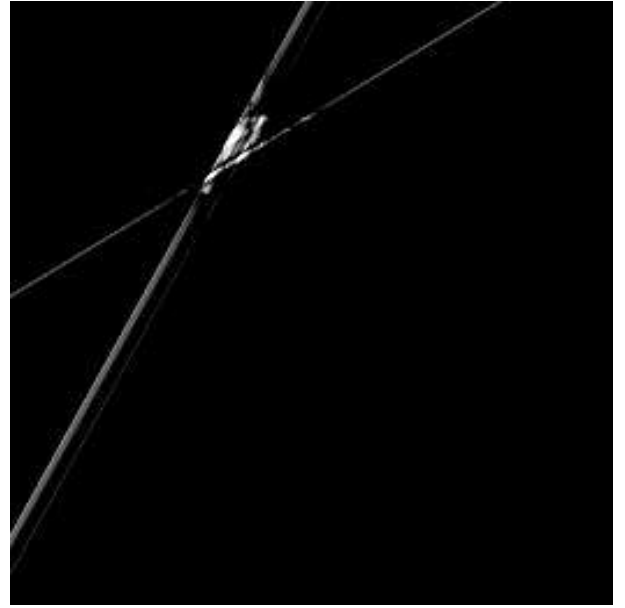


Fig. 6. Thresholded difference map constructed by the lowpass subband at resolution 256×256 (6 projections).

components \mathbf{e} and $\hat{\mathbf{e}}$ accordingly by performing the PCA and selecting the top two principle components. The measure is based on MSE, defined as follows:

$$\mathcal{M}(\mathbf{e}, \hat{\mathbf{e}}) = \log \left(\frac{\sum_{i=1}^n (\mathbf{e}_i - \hat{\mathbf{e}}_i)^2}{n} \right). \quad (9)$$

V. EXPERIMENTAL RESULTS

We have performed our experiments over a range of natural images, although the tampering detection ability of our proposed approach is image-independent. We chose the *barbara* and *lena* (512×512) to present our results in this paper. Typical attacks are simulated both for authentication and robustness evaluation.

Figures 2, 4 and 5 suggest that robustness against content-preserving manipulations is possible just from observations on the difference maps, since it is a reconstruction of $\{\mathbf{w}_i - \hat{\mathbf{w}}_i\}$. If f and \hat{f} are visually identical, the most energy of $\|f - \hat{f}\|$ should be nearly zero. The contrast enhanced version of the difference, on the other hand, may be useful in determining the nature of such manipulation. Notably, in the case of changing brightness, the amount of brightness can be easily estimated by the mean of the difference map.

Figure 3 demonstrate the tampering localisation ability of the signature. The tampered area is accurately detected by the intersection of “ridges”. The difference map can be further enhanced by a soft thresholding on the constructed difference map, in order to suppress some undesired linear artifact of under-complete projection. Such artifact is completely removed in with 12 angles of projections, where the bird-shaped region is clearly formed.

Due to the inherent multi-resolution property of the wavelet transform, the signature also allows a progressive authentication without losing its capability of tampering localisation.

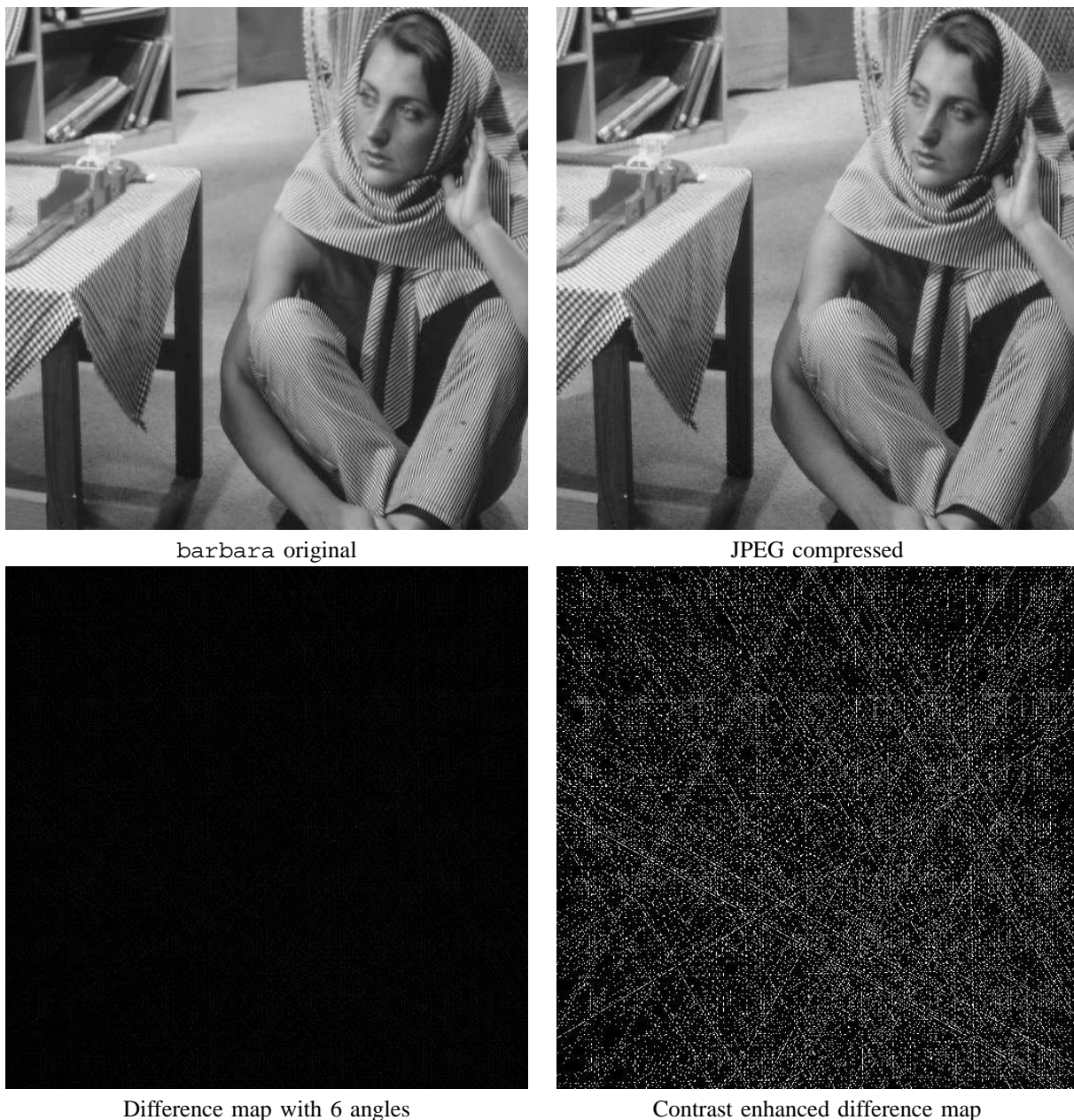


Fig. 2. Authentication Results from JPEG compression

Figure 6 illustrates an instance when the authentication is verified with lowpass subband of the signature, which is only half of the total ridgelet coefficients. The tampering localisation is effectively identical to its counterpart in figure 3.

Although we selected only a limited number of angles to perform the principle component analysis, the robustness measure results are still very promising. We tested the measure with four typical content-preserving operations:

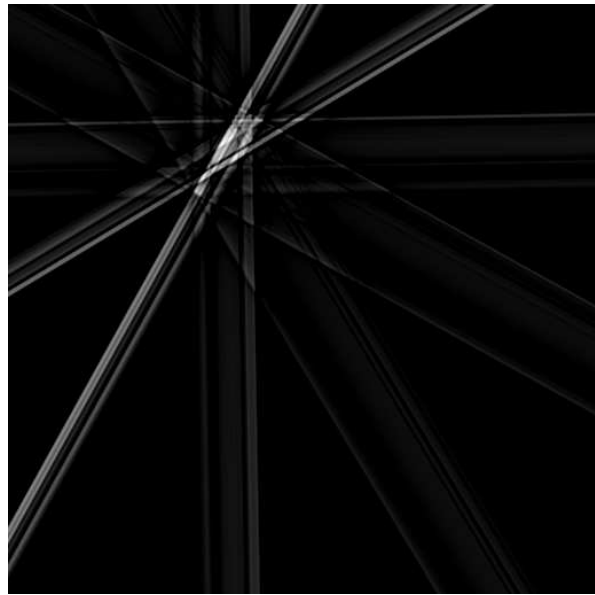
- 1) **Scaling.** The size of the support is reduced by half.
 - 2) **Noise.** Heavy Gaussian white noise with standard deviation at 0 dB.
 - 3) **Lowpass.** A 5×5 Gaussian lowpass filter.
 - 4) **Contrast.** Increasing the contrast by 20% percent.
- Images processed by these operations together with the

intact original are cross-compared using the \mathcal{M} measure we defined in equation (9). It seems clearly, from table I and II, which cross compares the intra-class images, that the measure usually below 0, even in extremely noisy cases. Table III is the inter-class comparison results between barbara and lena. As we expected, the measurements are almost constant, significantly higher than the results from intra-class measures. It is then almost trivial to classify if the content is preserved or not, by looking at the \mathcal{M} value. If the value is negative, it is safe to assume the content is preserved otherwise it has been destroyed or replaced.

There is certainly a degree of flexibility in controlling the signature's length by varying the number of Radon vectors. It is desirable for the signature to be compact while the trade-offs between communication cost and security / localisation



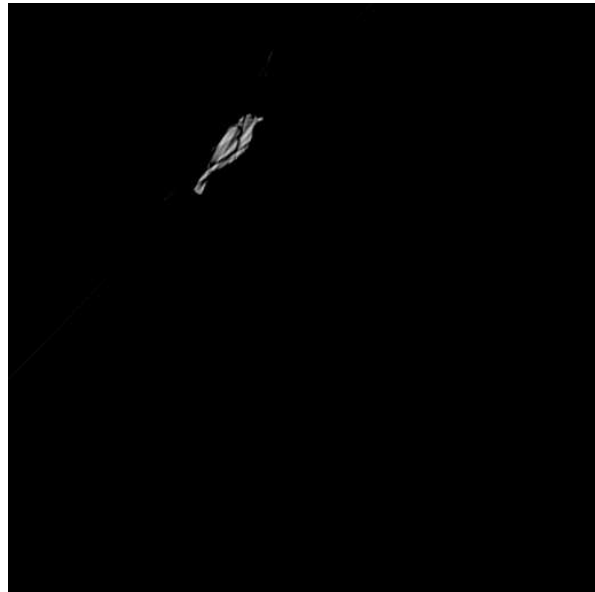
The tampered barbara



The difference map, 6 angles



Thresholded difference map, 6 angles



Thresholded difference map, 12 angles.

Fig. 3. Authentication results from tampered image

TABLE I
ROBUSTNESS MEASURES ON lena

lena	Original	Scaled	Noisy	Lowpass	Contrast
Original	-Inf	-2.2286	-0.5275	-4.7074	-5.3393
Scaled	-2.2286	-Inf	0.1380	-1.8247	-1.9562
Noisy	-0.5275	0.1380	-Inf	-0.7589	-0.5685
Lowpass	-4.7074	-1.8247	-0.7589	-Inf	-4.5097
Contrast	-5.3393	-1.9562	-0.5685	-4.5097	-Inf

always remain. However it is difficult to define exactly the length of the signature in order to be called “compact”. Here we would like to propose that the signature is “compact” as long as it can be embedded obliviously into the host media with some protective redundancy. For a 512×512 image, if we use the spatial LSB bits for data embedding, the total

capacity is 32768 bytes. Table IV lists the length of signatures we obtained from various images and different number of projections. They are encoded by a zero-order arithmetic coder with simple uniform scalar quantisation, but are still below the capacity and can be embedded as a form of self-embedding watermark.

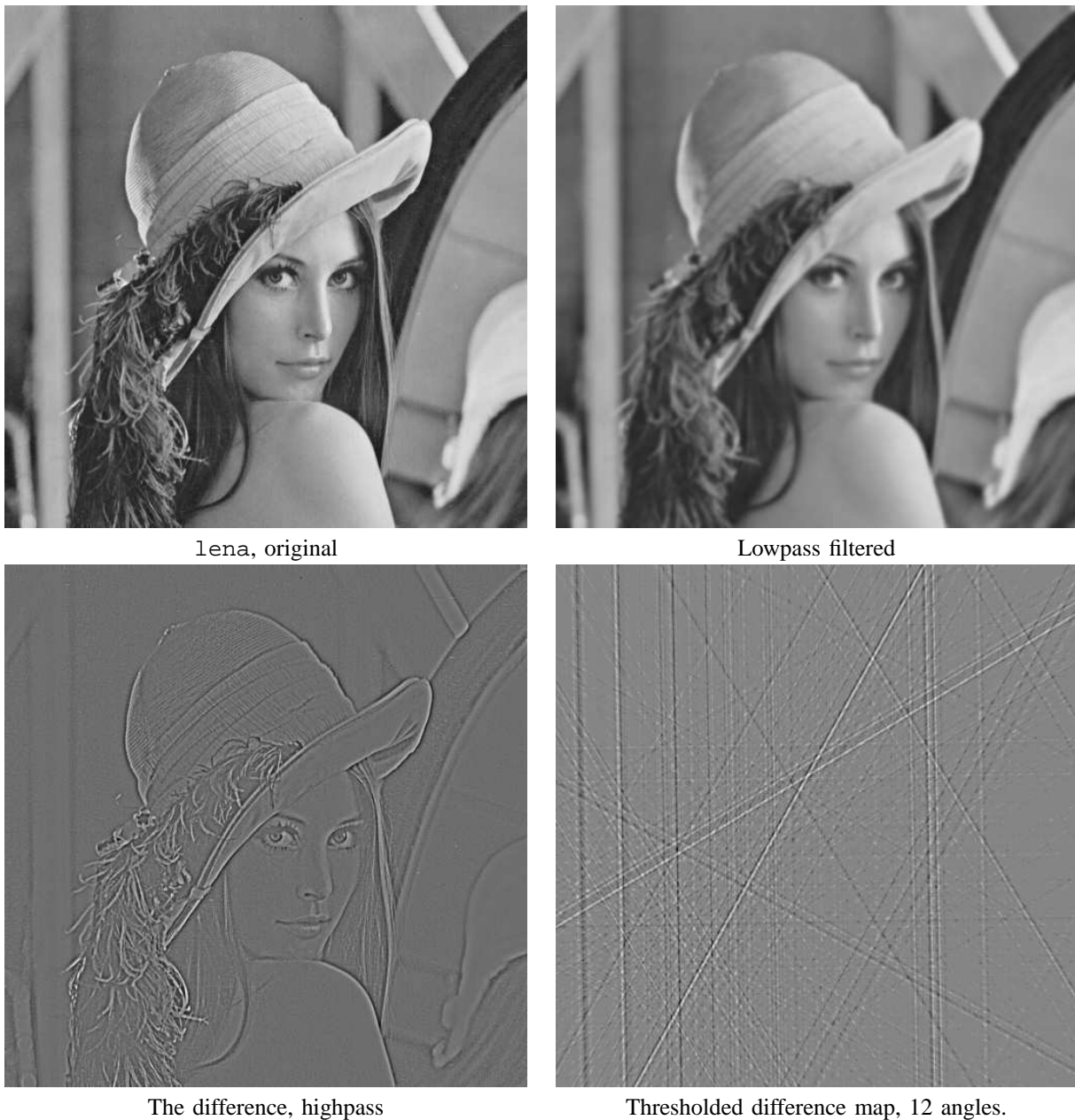


Fig. 4. Authentication results from lowpass filtered image

TABLE II
ROBUSTNESS MEASURES ON barbara

barbara	Original	Scaled	Noisy	Lowpass	Contrast
Original	-Inf	-2.3888	-0.7215	-2.0745	-5.8159
Scaled	-2.3888	-Inf	-0.6645	-2.3556	-2.2025
Noisy	-0.7215	-0.6645	-Inf	-0.6606	-0.6408
Lowpass	-2.0745	-2.3556	-0.6606	-Inf	-1.8015
Contrast	-5.8159	-2.2025	-0.6408	-1.8015	-Inf

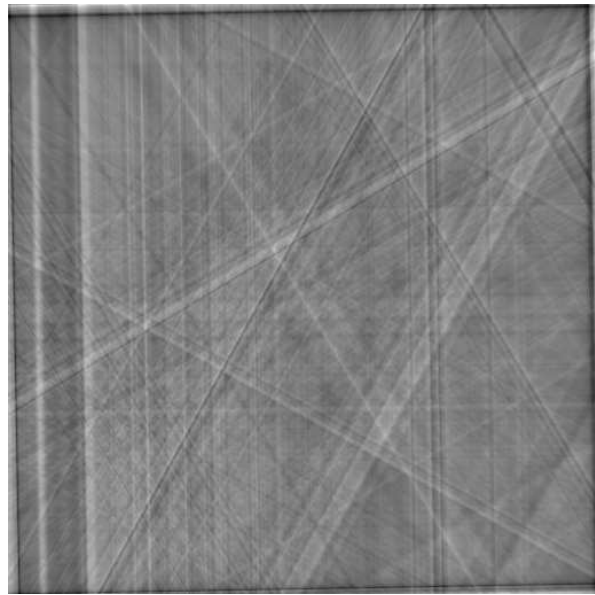
VI. CONCLUSIONS

A content-based, robust image authentication signature based on a directional image representation has been studied in this work. The signature, essentially a coded undercomplete ridgelet transform of the image, can localise tampering in a multi-resolution fashion, and has the robustness against various

content-preserving manipulations. The work is also one of the first practical attempts in ridgelet encoding, although the novelty is in authentication rather than compression. Since the encoder used in this work is very simple, an efficient compression algorithm for ridgelet representation can significantly improve the compactness of the signature and may benefit



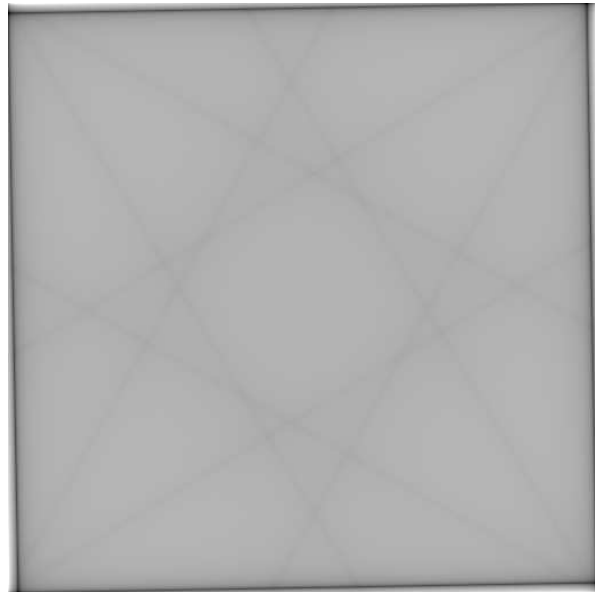
lena, Contrast adjusted



Normalised difference map, 6 angles



lena, Brightness adjusted



Normalised difference map, 6 angles.

Fig. 5. Authentication results from lowpass filtered image

TABLE III

ROBUSTNESS MEASURES BETWEEN lena AND barbara

barbara/lena	Original	Scaled	Noisy	Lowpass	Contrast
Original	8.3873	8.3807	8.3919	8.3845	8.3875
Scaled	8.3873	8.3806	8.3918	8.3845	8.3874
Noisy	8.3820	8.3753	8.3867	8.3791	8.3821
Lowpass	8.3857	8.3790	8.3903	8.3829	8.3858
Contrast	8.3875	8.3809	8.3921	8.3847	8.3877

the image coding community on a direction beyond wavelet. It remains to be seen how interpolation algorithms can be incorporated in the scheme which may help to reduce the linear artifact exhibited from the inverse Radon transform, and better choices of selecting the projection angles is also need to be explored.

REFERENCES

- [1] E.T. Lin and E.J. Delp, "A review of fragile image watermarks," in *Proc. of ACM Multimedia & Security Workshop*, Orlando, 1999, pp. 25–29.
- [2] G.L. Friedman, "The trustworthy digital camera: Restoring credibility to the photographic image," *IEEE Trans. on Consumer Electronics*, vol. 39, no. 4, pp. 905–910, Nov. 1993.
- [3] M. Schneider and S.F. Chang, "A robust content based digital signature for image authentication," in *Proc. of ICIP*, 1996, vol. 3, pp. 227–230.

TABLE IV

SIGNATURE LENGTHS WITH DIFFERENT NUMBER OF PROJECTIONS (IN BYTES).

Image	$ \Theta =6$	$ \Theta =9$	$ \Theta =18$
lena	2183	4034	7843
barbara	2372	4152	8012
goldhill	2280	4198	7911

- [4] N.Holliman and N. Memon, "Counterfeiting attacks on oblivious block-wise independent invisible watermarking schemes," *IEEE Trans. on Image Processing*, vol. 9, no. 3, pp. 432–441, March 2000.
- [5] J. Fridrich, M. Goljan, and R. Du, "Lossless data embedding - new paradigm in digital watermarking," *EURASIP Journ. Appl. Sig. Proc.*, vol. 2002, no. 2, pp. 185–196, Feb 2002.
- [6] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, pp. 656–715, Oct. 1949.
- [7] C.S. Lu and H.Y.M. Liao, "Structural digital signature for image authentication: An incidental distortion resistant scheme," *IEEE Trans. on Multimedia*, vol. 5, no. 2, pp. 161–173, 2003.
- [8] E.J. Candés, *Ridgelets: Theory and applications*, Ph.D. thesis, Dept. of Stats, Stanford Univ., Stanford, CA, 1998.
- [9] E.J. Candés and D.L. Donoho, "Curvelets - a suprisingly effective nonadaptive representation for objects with edges," in *Curves and Surfaces*, C. Rabut, A. Cohen, and L.L. Schumaker, Eds., pp. 105–120. Vanderbilt University Press, Nashville, TN, 2000.
- [10] F. Lefebvre, J. Czyz, and B. Macq, "A robust soft hash algorithm for digital image signature," in *Proc. of ICIP*, Barcelona, Sept. 2003, vol. II, pp. 495–498.
- [11] M.L. Brady, "A fast discrete approximation algorithm for the Radon transform," *SIAM Journal of Computing*, vol. 27, no. 1, pp. 107–119, 1998.
- [12] A. Brandt, J. Mann, M. Brodski, and M. Galun, "A fast and accurate multilevel inversion of the Radon transform," *SIAM journal of Applied Mathematics*, vol. 60, no. 2, pp. 437–462, 2000.
- [13] W.A. Götze and H.J. Druckmüller, "A fast digital Radon transform - an efficient means for evaluating the Hough transform," *Pattern Recognition*, vol. 28, no. 12, pp. 1985–1992, 1995.
- [14] F. Matúš and J. Flusser, "Image representation via a finite Radon transform," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 15, no. 10, pp. 996–1006, October 1993.
- [15] Minh N. Do and Martin Vetterli, "The finite ridgelet transform for image representation," *IEEE Trans. Image Processing*, vol. 12, no. 1, pp. 16–28, Jan. 2003.
- [16] A. Averbuch, R. Coifman, D.L. Donoho, and M. Israeli, "Fast slant stack: A notion of radon transform for data in a cartesian grid which is rapidly computible, algebraically exact, geometrically faithful and invertible," to appear in *SIAM Scientific Computing*.