RADON/RIDGELET SIGNATURE FOR IMAGE AUTHENTICATION

Zhen Yao *Nasir Rajpoot*

Dept. of Computer Science, University of Warwick
Coventry, CV4 7AL
United Kingdom
email: {yao, nasir}@dcs.warwick.ac.uk

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, robust to content-preserving manipulations such as compression and allows a progressive authentication.

1. 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 [1] 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. Hence 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 neeed for finding better representations for nature images, several geometric wavelets (eg. ridgelet and curvelet) 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 [8], which take the advantage of invariant features of the transform to provide robustness, 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 idea.

[1] The *key* here refers to the authentication (public) key, which defines the authenticated space, instead of the encryption key.

0-7803-8554-3/04/$20.00 ©2004 IEEE.

Some experimental results are presented and the paper concludes with comments on the proposal and future directions of research.

2. 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

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

Discretisation has been a major difficulty in applying Radon transform to general image processing. 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. Recently, some other discrete (finite) Radon transforms have been proposed such as FRAT [9] and fast slant-stack [10].

The Radon transform is a linear transform and has several useful properties.

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

$$f(x - x_0, y - y_0) \Leftrightarrow R_f(\theta, t - x_0\cos\theta - y_0\sin\theta) \quad (2)$$

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

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

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

$$f(ax, ay) \Leftrightarrow \frac{1}{|a|}R_f(\theta, at) \quad (4)$$

The ridgelet transform, introduced in [11], has the continuous form of

$$CRT_f(a, b, \theta) = \int_{\mathbb{R}^2} \psi_{a,b,\theta}(x, y)f(x, y)dxdy \quad (5)$$

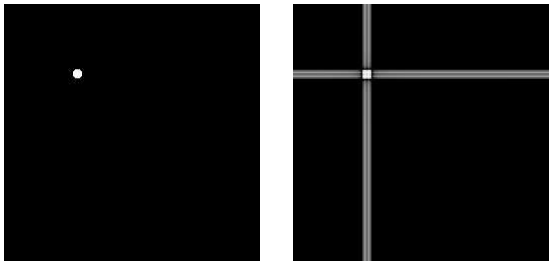
where the ridgelet $\psi_{a,b,\theta}(x, y)$ in 2-D are defined from a wavelet-type function in 1-D $\psi(x)$ as

$$\psi_{a,b,\theta}(x, y) = \frac{1}{\sqrt{a}}\psi\left(\frac{x\cos\theta + y\sin\theta - b}{a}\right) \quad (6)$$

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 (5) can be re-written as

$$CRT_f(a, b, \theta) = \int_{\mathbb{R}} \psi_{a,b}(t)R_f(\theta, t)dt \quad (7)$$

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



(a) (b)

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

3. 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 [9]. 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 $\Theta = \{\theta_1, \theta_2, ..., \theta_n\}$, 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.

4. 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` (512×512) image to present our results in this paper. Due to the space limitation we only present results on two typical attacks: the first one is content-preserving JPEG compression, and the second one is a malicious attack with a bird-shaped stamping (see figure 2).

Figures 2(c) and 2(d) suggest that robustness against content-preserving manipulations is possible, since the difference map is a reconstruction of $\{\mathbf{w}_i - \hat{\mathbf{w}}_i\}$. If f and $\hat{f}$ are visually identical, the energy of $f - \hat{f}$ should be nearly zero. However, the contrast enhanced version of the difference, such as in figure 2(d), may be useful in determining the nature of such manipulation. Robustness against geometrical manipulations can also be addressed [8], due to the invariant properties of Radon transform described in equation (2), (3) and (4).

Figure 2(e)-(h) demonstrate the tampering localisation ability of the signature. The tampered area is accurately detected by the intersection of "ridges". Figure 2(g),(h) is further enhanced by a soft thresholding on the constructed difference map, in order to suppress some undesired linear artifact of undercomplete projection. Such artifact is completely removed in figure 2(h), where more angles of projections are used. The difference map can be used to restore the tampered area, by simply adding the difference map back into the received image.

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. Figure 3 illustrates an instance when the authentication is verified with lowpass band of the signature, which is only half of the total ridgelet coefficients. The tampering localisation is effectively identical to its counterpart in figure 2(g).

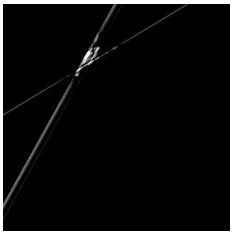


Fig. 3. Thresholded difference map constructed by the lowpass subband at resolution 256×256 (6 projections).

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

Table 1. Signature lengths with different number of projections (in bytes).

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 always impose. 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 1 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 within below the capacity and can be embedded as a form of self-embedding watermark.

5. CONCLUSIONS

A content-based, robust image authentication signature has been proposed. The signature, essentially a coded undercomplete ridgelet transform of the image, can localise tampering in a multi-resolution fashion. The work is also one of our first practical attempts in ridgelet encoding, although the novelty is in authentication rather than compression. Since

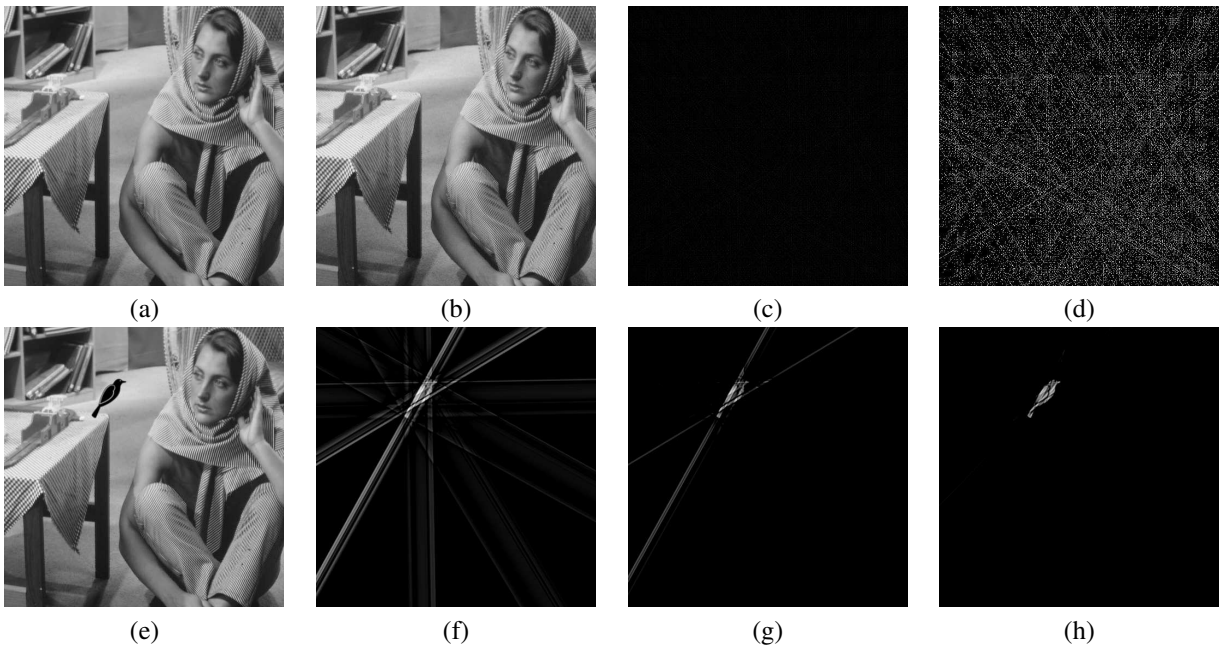


Fig. 2. Authentication results. (a) Original. (b) JPEG compressed. (c) The difference map, 6 projections (d) Contrast enhanced (c). (e) The tampered image (object addition) (f) The difference map, 6 projections (g) The thresholded difference map with 6 projections (h) The thresholded difference map with 12 projections.

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 the image coding community on a direction beyond wavelet. It remains to be seen how interpolation algorithms can incorporated in the scheme which may help to reduce the linear artifact exhibited from the inverse Radon transform.

6. REFERENCES

[1] E.T. Lin and E.J. Delp, "A review of fragile image watermarks," in *Proc. of ACM Multimeida & 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.

[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] 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.

[9] 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.

[10] 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.

[11] E.J. Candés, *Ridgelets: Theory and applications*, Ph.D. thesis, Dept. of Stats, Stanford Univ., Stanford, CA, 1998.