

ous points. The equilibrium threshold is 99.9% and the maximal number of generations is 500. Fig. 2 shows the segmentation results according to the considered parameters.

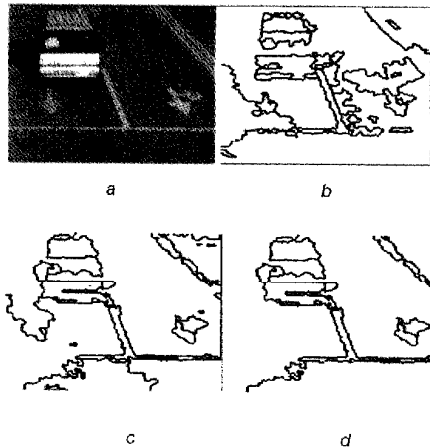


Fig. 2 Segmentation results

- a Original image
- b Results of optimising colour
- c Results of optimising colour and blurring
- d Results of optimising colour, blurring matrix and noise

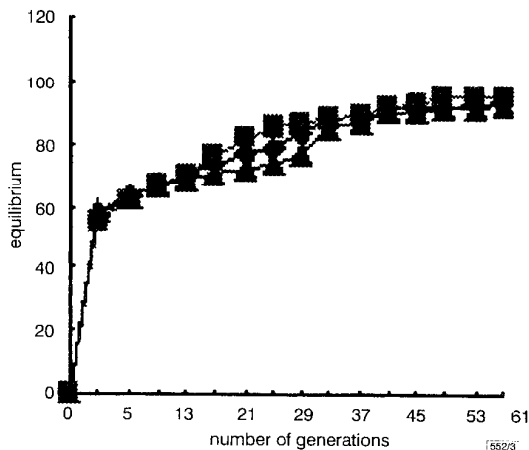


Fig. 3 Equilibrium against number of generations

- ▲— feature
- ◆— blurring and feature
- feature, blurring and noise

Fig. 3 shows the relationship between the equilibrium and generations of Fig. 2. As can be seen, the number of generations needed to reach the equilibrium threshold can be decreased when all parameters are optimised. This also shows that the computation time can be improved when the HDGA is performed in parallel.

Table 1: Evaluation of segmentation results of Fig. 2

Measure	Result (b)	Result (c)	Result (d)
Number of regions	23	20	31
F	50.8	39.6	32.2

Table 1 shows the values of F for the segmentation results of Fig. 2. In this table, F is the evaluation function defined in [6]. As shown in Table 1, the quality of the segmentation can be improved when all parameters are optimised. This also shows that our method has the potential to deal with natural images.

Conclusions: For unrestricted natural images, the unsupervised segmentation problem has not been completely resolved. This Letter proposed an unsupervised method for segmenting noisy and blurred images. We used an MRF model, which is robust to degradation. The performance of methods based on MRFs depends on correct parameter estimates. It is computationally too time

consuming to deal with a large number of unknown parameters, so we need a more complex and powerful segmentation algorithm. For this purpose we used a hierarchical distributed genetic algorithm that is unsupervised and parallel. Experimental results show that the proposed method is effective at segmenting real images. This method is too slow for real time applications, however, a problem which we are currently investigating.

Acknowledgment: This research was supported by Korea science and engineering foundation (KOSEF) under core research grant #971-0908-050-2.

© IEE 1998
Electronics Letters Online No: 19981674

4 September 1998

Hang Joon Kim, Eun Yi Kim, Jin Wook Kim and Se Hyun Park
(Department of Computer Engineering, KyungPook National University, Taegu, 702-701, South Korea)

References

- HANSEN, F.R., and ELLIOTT, H.: 'Image segmentation using simple Markov field models', *Comput. Graphics Image Process.*, 1982, **20**, pp. 101–132
- KIM, I.Y., and YANG, H.S.: 'Efficient image labeling based on Markov random field and error backpropagation network', *Pattern Recogn.*, 1993, **26**, (11), pp. 1695–1707
- KIM, J.W., and ZEIGER, B.P.: 'Hierarchical distributed genetic algorithms: A fuzzy logic controller design application', *IEEE Expert*, 1996, **11**, (3), pp. 76–84
- JIN WOOK KIM, EUN YI KIM, SE HYUN PARK, and HANG JOON KIM.: 'Segmentation of MRF based image using hierarchical genetic algorithm'. ACCV'98, 1997, Vol. 1, pp. 730–737
- GEMAM, S., and GEMAN, D.: 'Stochastic relaxation, Gibbs distributions, and the Bayesian restoration of images', *IEEE Trans.*, 1984, **PAMI-6**, (6), pp. 721–741
- JIANHONG LIN, and YEE-HONG YANG.: 'Multiresolution color image segmentation', *IEEE Trans.*, 1994, **PAMI-16**, (7), pp. 689–700

Wavelet filtering algorithm for fan-beam CT

Shiying Zhao, Ge Wang and Jiang Hsieh

To date, all wavelet computed tomography (CT) work has been based on the assumption of a parallel-beam geometry. The authors directly formulate wavelet CT based on the fan-beam geometry, using recently developed theory for wavelet filtering in filtered backprojection. Experiments with clinical raw projection data demonstrate the feasibility and utility of the approach.

Introduction: In recent years, the use of wavelets in computed tomography (CT) has attracted significant interest (see [1] and references therein). However, none of the published results in this area was obtained for the fan-beam geometry, which is the standard sampling mode of modern CT scanners. Although rebinning can be used to convert fan-beam data to parallel-beam data, resolution degradation, computational overhead and artefact complications will be encountered. Hence, it is desirable to extend wavelet CT methods to the fan-beam scanning geometry. In this Letter, we directly formulate wavelet CT based on the fan-beam geometry, and demonstrate its feasibility and utility.

Fan-beam reconstruction: Let Ω be a bounded region in the plane, and $f \in L^2(\Omega)$ be an image. X-ray CT is used to recover the image f from its Radon transform $\mathbf{R}f$ defined by

$$(\mathbf{R}_\theta f)(s) = \int_{\{X \in \Omega: X \cdot \Theta = s\}} f(X + s\Theta) dX$$

for $s \in \mathbb{R}$ and $\Theta = (\cos\theta, \sin\theta) \in \mathbb{S}$, where \mathbb{R} denotes the real line and \mathbb{S} the unit circle.

The equiangular fan-beam geometry is given in terms of the coordinates (α, β) , where $\alpha \in [-\gamma_m, \gamma_m] \subset (-\pi/2, \pi/2)$ and $\beta \in [0, 2\pi]$ are the detector angular position and the X-ray source angular position, respectively. The filtered backprojection in this case can be expressed as [2]:

$$f(r, \varphi) = \frac{1}{4\pi} \int_0^{2\pi} \frac{1}{L^2} (\Lambda_{\sin} \mathbf{R}'_f f)(\gamma) d\beta$$

where the weighted projection \mathbf{R}'_f is given by $(\mathbf{R}'_f f)(\alpha) = (\mathbf{R}_{\alpha/\beta} f)(D \sin \alpha)(D \cos \alpha)$, and the filtering operator Λ_{\sin} can be expressed as

$$(\Lambda_{\sin} g)(\gamma) = \frac{1}{2\pi} \int_{-\infty}^{\infty} |\xi| \int_{-\gamma_m}^{\gamma_m} g(\alpha) e^{i\xi \sin(\gamma-\alpha)} d\alpha d\xi$$

Wavelet filtering: Recently, wavelet filtering theory was developed for filtered backprojection [1]. In this theory, the following finding plays an instrumental role: the wavelet ramp filter with sufficient regularity is a biorthogonal wavelet. Hence, the wavelet filtering can be implemented by wavelet decomposition and consequent wavelet reconstruction with respect to the two sets of wavelets. Although the wavelet filtered by Λ_{\sin} is no longer a wavelet, due to the nonlinear function sine, the wavelet filtering process in the parallel-beam geometry can still be adapted to the fan-beam geometry by assuming that \mathbf{R}'_f has a limited bandwidth, which is equivalent to the replacement of Λ_{\sin} with the standard ramp filter Λ -operator: then the sub-band coding algorithm for parallel-beam wavelet filtering [1] can be directly applied to fan-beam wavelet filtering.

Let $\{\psi, \tilde{\psi}\}$ be a pair of compactly supported MRA biorthogonal wavelets [3] with scaling functions $\{\phi, \tilde{\phi}\}$. According to the wavelet filtering theory [1], if $\Lambda\psi \in L^2(\mathbb{R})$ then there exists a pair of scaling functions $\{\Phi, \tilde{\Phi}\}$ so that the corresponding wavelets coincide with $\{\Lambda\psi, \Lambda^{-1}\tilde{\psi}\}$. Therefore, wavelet filtering can be achieved by using three filters: lowpass filter $\{H_k\}$, highpass filter $\{G_k\}$, and transition filter $\{L_k\}$. They are determined by two-scale relations, e.g. $(\Lambda\psi)(\gamma) = \sum_{k \in \mathbb{Z}} L_k \Phi(2\gamma - k)$.

For a given projection profile g with $\Lambda g \in L^2(\mathbb{R})$, we suppose that g can be approximated by the inhomogeneous wavelet expansion

$$g(\alpha) = \sum_{k \in \mathbb{Z}} \tilde{c}_{n,k} \tilde{\phi}_{n,k}(\alpha) + \sum_{j \geq n} \sum_{k \in \mathbb{Z}} \tilde{d}_{j,k} \tilde{\psi}_{j,k}(\alpha)$$

for some integer $n \in \mathbb{Z}$ with only finite nonzero coefficients: $\tilde{c}_{j,k} = \langle g, \tilde{\phi}_{j,k} \rangle$ and $\tilde{d}_{j,k} = \langle g, \tilde{\psi}_{j,k} \rangle$. Using the sub-band coding scheme [3, 1] we obtain

$$(\Lambda g)(\gamma) = \sum_{k \in \mathbb{Z}} 2^N \tilde{C}_{N,k} \Phi_{N,k}(\gamma) + \sum_{j \geq N} \sum_{k \in \mathbb{Z}} 2^j \tilde{d}_{j,k} (\Lambda \tilde{\psi})_{j,k}(\gamma)$$

for any pre-assigned integer $N > n$, where the sequence $\{\tilde{C}_{j,k}; j > n, k \in \mathbb{Z}\}$ is defined by

$$\tilde{C}_{j+1,k} = \sum_{\ell \in \mathbb{Z}} (H_{\ell-2k} \tilde{C}_{j,\ell} + G_{\ell-2k} \tilde{d}_{j,\ell})$$

for $j > n$ and $k \in \mathbb{Z}$, and with $C_{j,\ell} = c_{j,\ell}$ and $H_{\ell-2k}$ substituted by $L_{\ell-2k}$ when $j = n$.

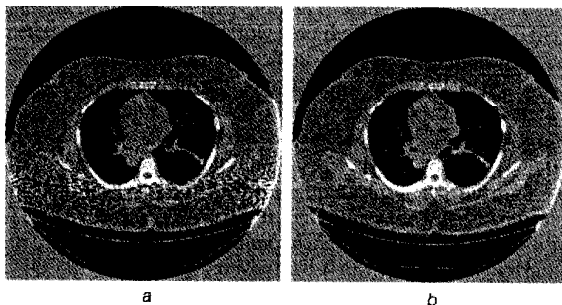


Fig. 1 Fan-beam reconstruction of patient scan via wavelet denoising
a Reconstruction via standard filtered backprojection, containing streaking artefacts due to photo-starvation
b Wavelet reconstruction after adaptive denoising, with strong suppression of artefacts

Embedded denoising: The formulation of filtered backprojection in a wavelet framework allows a natural separation of various types of features in the Radon data, which is useful in a number of

ways. It has previously been determined that wavelet CT is advantageous for local region reconstruction [4, 5]. We point out here that wavelet CT facilitates effective denoising of raw data. It was reported that severe streaking artefacts can be generated due to X-ray photon starvation. To combat these artefacts, an adaptive filtering scheme was proposed at a significant computational complexity [6]. With the wavelet filtering method, an adaptive denoising mechanism can be efficiently and conveniently embedded between the wavelet decomposition and the wavelet reconstruction. This wavelet denoising process was designed according to the principle of wavelet shrinkage [7]. As shown in Fig. 1, our wavelet filtering and denoising techniques basically eliminated the streaking produced in standard filtered backprojection. A wavelet ramp filter for a biorthogonal coiflet with four vanishing moments [3] was used in the reconstruction (see [1], Appendix E).

Discussion: Our wavelet filtering algorithm for fan-beam CT has great potential in medical X-ray CT, especially for radiation exposure reduction, because of its capabilities of local reconstruction and data denoising. Additionally, our algorithm is faster than the standard filtered backprojection algorithm, because the filter responses can be truncated to only a few terms due to multiple vanishing moments of the selected wavelets [1]. Further work on refining this algorithm and extending it to the spiral scanning geometry is underway.

Acknowledgments: The projection data were provided by GE Medical Systems. This work was supported in part by the UM Research Board, University of Missouri, under Grant #S-3-4098.

© IEE 1998

23 October 1998

Electronics Letters Online No: 19981690

Shiyong Zhao (Department of Mathematics and Computer Science, University of Missouri - St. Louis, St. Louis, MO 63121, USA)

Ge Wang (Department of Radiology, University of Iowa, Iowa City, Iowa 52242, USA)

Jiang Hsieh (Applied Science Laboratory, GE Medical Systems, Milwaukee, WI 53201, USA)

References

- ZHAO, S.: 'Wavelet filtering for filtered backprojection in CT', to be published in *Appl. Comput. Harmon. Anal.*
- ROSENFELD, A., and KAK, AVINASH C.: 'Digital picture processing' (Academic Press, New York, 1982), Vol. 1, 2nd Edn.
- DAUBICHES, I.: 'Ten lectures on wavelets', CBMS-NSF Series in Applied Mathematics, SIAM, Philadelphia, 1992
- RASHID-FARROKHI, F., LIU, K.J.R., BERENSTEIN, C., and WALNUT, D.: 'Wavelet-based multiresolution local tomography', *IEEE Trans.*, 1997, **IP-22**, pp. 1412-1430
- ZHAO, S., and WANG, G.: 'Wavelet operators and their applications in computerized tomography', *Proc. SPIE*, 1997, pp. 337-348
- HSIEH, J.: 'Adaptive streak artifact reduction in CT resulting from excessive x-ray photon noise', *Med. Phys.*, 1998, **25**, (11), pp. 2139-2147
- DONOHO, D.L., and JOHNSTONE, I.M.: 'Ideal spatial adaptation by wavelength shrinkage', *Biometrika*, 1994, **81**, pp. 425-455

Compatible cofactor multiplication for Diffie-Hellman primitives

B.S. Kaliski Jr.

Cofactor multiplication has recently been proposed as a technique for protecting Diffie-Hellman primitives against certain attacks. However, a Diffie-Hellman primitive protected with cofactor multiplication as initially described produces different keys when not under attack than its unprotected counterpart. A simple modification to cofactor multiplication is presented that overcomes this incompatibility.

Introduction: In Classic Diffie-Hellman key agreement [1], two parties generate key pairs $(g^a \text{ mod } p, a)$ and $(g^b \text{ mod } p, b)$ where g is an element of $GF(p)$, p is a prime, and a and b are integers. They then exchange the public keys $g^a \text{ mod } p$ and $g^b \text{ mod } p$.