

Polyphase adaptive filter banks for fingerprint image compression

Ö.N. Gerek and A.E. Çetin

A perfect reconstruction polyphase filter bank structure is presented in which the filters adapt to the changing input conditions. The use of such a filter bank leads to higher compression results for images containing sharp edges such as fingerprint images.

Perfect reconstruction adaptive polyphase filter banks: We propose an adaptive subband decomposition structure for compressing fingerprint images [1]. The filter bank is a polyphase structure [2, 3] in which one of the subband components is adaptively predicted from the other subband component. The resulting subsignals are then quantised using embedded zerotree type coders [4, 5].

The adaptive prediction concept is combined with the lifting idea [2] and the resulting adaptive filter bank structure is shown in Fig. 1. In this Figure, signal $x_2(n)$ is predicted from $x_1(n)$. Since the polyphase components $x_1(n)$ and $x_2(n)$ are highly correlated, the prediction is very effective at removing the redundant information in $x_2(n)$. In our experiments, we use an LMS-type algorithm for updating the coefficients of the prediction filter which adapts its coefficients to minimise the variance of $x_2(n)$.

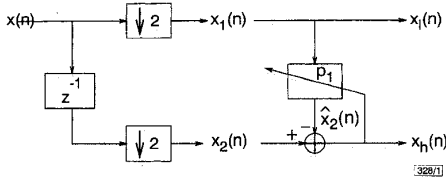


Fig. 1 Adaptive structure analysis stage

This decomposition scheme provides perfect reconstruction (PR) because the subsignals $x_1(n)$ and $x_h(n)$ are available at the decoder. The signal $x_h(n)$ corresponds to the error signal in the adaptation algorithm, so the decoder can update the filter coefficients according to the input $x_1(n) = x_1(n)$ and the error $x_h(n)$ as shown in Fig. 2.

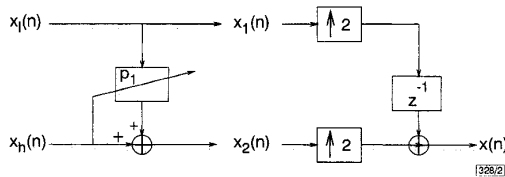


Fig. 2 Adaptive structure synthesis stage

Adaptation methods: The signal $x_2(n)$ is predicted from $x_1(n)$ as follows:

$$\hat{x}_2(n) = \sum_{k=-N}^N w_{n,k} x_1(n-k) = \sum_{k=-N}^M w_{n,k} x(2n-2k) \quad (1)$$

where the filter coefficients $w_{n,k}$ are updated using an LMS-type algorithm, and the subsignal x_h is given by

$$x_h(n) = x_2(n) - \hat{x}_2(n) \quad (2)$$

In our method, the normalised LMS type adaptation scheme for linear FIR filters is used:

$$\hat{\mathbf{w}}(n+1) = \hat{\mathbf{w}}(n) + \mu \frac{\tilde{\mathbf{x}}_n e(n)}{\|\tilde{\mathbf{x}}_n\|^2} \quad (3)$$

where $\hat{\mathbf{w}}(n)$ is the weight vector at time instant n . Vector $\tilde{\mathbf{x}}_n$ is given by

$$\tilde{\mathbf{x}}_n = [x_1(n-N), x_1(n-N+1), \dots, x_1(n+N-1), x_1(n+N)]^T \quad (4)$$

and

$$e(n) = x_2(n) - \tilde{\mathbf{x}}_n^T \hat{\mathbf{w}}(n) \quad (5)$$

To improve the adaptation performance, the step size parameter μ is also adaptively chosen according to the variance of the input $x_1(n)$. Since these data are available both at the encoder and at the decoder side, μ can be updated by the decoder according to the same algorithm, and the PR property is preserved.

Another choice of predictor is the adaptive order statistics (OS) filter [6, 7]. In this method, after rank ordering the input elements, the largest and smallest values are ignored and the remaining rank ordered elements are fed to an LMS adaptation block. This method gives better coding results especially for images containing regions separated by sharp edges. At the edges, the OS characteristics of the adaptive filter eliminate ringing effects.

Compression of fingerprint images: The compression of grey tone fingerprint images is performed by applying adaptive subband decomposition followed by the SPIHT coder [5], an embedded zero tree (EZT) type coder [4]. The level of decomposition is determined by the size of the image. OS adaptive filters give slightly better results than FIR adaptive filters for fingerprint images. Two levels of adaptive subband decomposition followed by three levels of regular subband decomposition are used for 256×256 images. Experimental results show that at 1 bit/pixel, our decomposition scheme with the SPIHT coder outperforms the traditional fixed wavelet SPIHT and embedded zerotree wavelet (EZW) coders [4, 5] which are state of the art grey tone image compression algorithms.



Fig. 3 Two fingerprint images

a Binary
b Grey tone

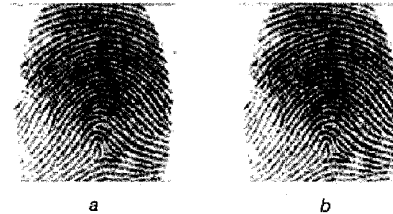


Fig. 4 Reconstructed images at 1 and 0.5 bit/pixel

a 1 bit/pixel
b 0.5 bit/pixel

In our simulation studies, we used fingerprint images taken from the National Institute of Standards and Technology (NIST) database examples for compression. All of the fingerprint images used are 8 bit 256×256 images. An example grey tone image is shown in Fig. 3. In Fig. 4, two coded versions of this grey tone fingerprint image at different compression ratios are shown. Our adaptive filter bank algorithm accomplishes a PSNR of 28.46dB at 1 bit/pixel, whereas the well known SPIHT and EZW coders [4, 5] have PSNRs of 28.35 and 27.86dB at the same bit rate, respectively. Furthermore, the ringing effects present in the SPIHT and EZT coded image are eliminated by our method.

We also compare the average PSNRs obtained by the adaptive filter bank algorithm to the results obtained by an SPIHT coder for a set of 20 grey tone fingerprint images. According to the test results, at 1 bit/pixel, the average PSNRs over these images obtained by the SPIHT and adaptive filter bank method are 28.26 and 28.36dB, respectively. We observe that the adaptative filter bank produces the best compression results.

The compression of binary fingerprint images needs more elaboration. The application of a filter bank, including adaptive subband decomposition, increases the dynamic range. To avoid this

increase in range, a quantisation scheme is used to keep the decoded signal in binary form.

The LMS algorithm used in the filter bank usually produces non-binary coefficients, so the filtered signal is not binary, in general. Therefore, quantisation to binary levels is necessary for the reconstructed image. Another problem is that the LMS filter may become unstable in the black regions of a fingerprint image where most of the pixel values are zero. To avoid this situation the LMS algorithm is switched to a constant prediction filter in the flat regions where all the pixels are either black or white, and the prediction value of the filter output in Fig. 1 is set to zero (one) for black (white) regions. With this filter bank, the highband sub-signal becomes zero in the flat regions (black or white) of a fingerprint image. The prediction errors occur in the transition regions which correspond to the edge portions of the image. As a result, highpass signal $x_h(n)$ contains nonzero elements only in transition regions. This shows that the low and highband signals are decorrelated by the adaptive subband decomposition scheme. At both encoder and decoder sides, the filter bank switches between the adaptive and fixed prediction filter banks synchronously, depending on the values of black or white pixels in the region of support in \tilde{x}_n . Therefore, the PR property is retained. Finally, the reconstructed image is quantised to a binary representation by thresholding. The quantisation of these subband signals does not produce ringing effects in the decoded image. The only visible effect in the reconstructed image is an occasional shift in the edge portions which separate the black and white regions.



Fig. 5 Reconstructed binary fingerprint image at CR = 13.92:1

In Fig. 5, the compressed version of the binary fingerprint test image in Fig. 3 with CR = 13.92:1 is shown. The coded image preserves the discriminating features of fingerprint images such as core and delta points. The JBIG standard compresses the same image only to CR = 5.88:1.

We compare the average compression ratios obtained by the adaptive filter bank algorithm to the results obtained by an SPIHT wavelet coder for a set of 20 binary fingerprint images. According to the test results, at the same high visual quality level (35dB PSNR), the average CRs over these images obtained by the SPIHT and adaptive filter bank method are 13.66:1 and 13.80:1, respectively. The JBIG lossless compression standard compresses only at a ratio of 6.0:1.

The coding results for the set of binary fingerprint images are in agreement with the grey tone image coding results. Improvements in compression performance are obtained due to the use of the adaptive filter bank.

Acknowledgments: This work is supported by TUBITAK (Turkish Scientific and Technical Research Council), and NSF Grant No. INT9406954. It will be partially presented in EUSIPCO 1998.

© IEE 1998

24 August 1998

Electronics Letters Online No: 19981279

Ö.N. Gerek and A.E. Çetin (Bilkent University, Department of Electrical Engineering, Bilkent, Ankara, TR-06533, Turkey)

E-mail: gerek@ee.bilkent.edu.tr

References

- 1 Federal Bureau of Investigation: 'WSQ gray-scale fingerprint image compression specification'. Document IAFIS-IC-0110v2, February 1993
- 2 SWELDENS, W.: 'The lifting scheme: A new philosophy in biorthogonal wavelet constructions' in LAINE, A.F., and UNSER, M. (Eds.): 'Wavelet applications in signal and image processing III'. Proc. SPIE 2569, 1995, pp. 68-79

- 3 DAUBECHIES, I., and SWELDENS, W.: 'Factoring wavelet transforms into lifting steps', *J. Fourier Anal. Appl.*, 1998, 4, (3), pp. 247-269
- 4 SHAPIRO, J.M.: 'Embedded image coding using zerotrees of wavelet coefficients', *IEEE Trans.*, 1993, SP-41, (12), pp. 3445-3462
- 5 SAID, A., and PEARLMAN, W.A.: 'An image multiresolution representation for lossless and lossy image compression', *IEEE Trans.*, 1996, IP-5, pp. 1303-1310
- 6 PITAS, I., and VENETSANOPOULOS, A.: 'Adaptive filters based on order statistics', *IEEE Trans.*, 1991, SP-39, pp. 518-522
- 7 SALEMBIER, P., and JAQUENOUD, L.: 'Adaptive morphological multiresolution decomposition' in GADER, D. (Ed.): 'Image algebra and mathematical morphology' San Diego, USA, 1991, Vol. 1568, pp. 26-37
- 8 GEREK, Ö.N., and ÇETIN, A.E.: 'Linear/nonlinear adaptive polyphase subband decomposition structures for image compression'. IEEE Int. Conf. Acoustics, Speech, and Signal Processing, ICASSP'98, Seattle, WA, 12-15 May 1998

Clock-controlled chaotic keystream generators

Sang Tao, Wang Ruli and Yan Yixun

The authors propose clock-controlled chaotic keystream generators, for generating keystreams with periods long enough for cryptographic use while maintaining the good statistical properties of chaotic dynamics. These keystream generators may provide higher security than other proposed methods.

Introduction: 'Short cycle length' is one of important problems of chaotic keystream generators, which results from the finite precision of computers [1-4]. To extend the cycle length of chaotic systems, we suggested a perturbation algorithm in [4]. To obtain a much longer period, in this Letter we propose a better method which uses clock-controlled chaotic keystream generators as follows:

Method: This method involves the use of one register to irregularly clock a chaotic system to be perturbed by another register. It consists of the following steps:

(1) **Input:**

(i) System parameters for:

(a) a chaotic iterative system $x_{t+1} = G(x_t)$ where $t = 0, 1, 2, \dots$ denote the iteration numbers, and the internal states $x_t \in [0, 1]$ have the form for a P computing precision [2]: $x_t = 0.x_{t,1}x_{t,2}\dots x_{t,i}\dots x_{t,P}$, $x_{t,i} \in \{0, 1\}$ for all $i = 1, 2, \dots, P$. The chaotic mapping $G: [0, 1] \rightarrow [0, 1]$ is chosen according to the good-statistical-property principle, including uniform distribution and double-valued autocorrelation, etc. [4]. As an example, here we use the rescaled version of Zhou's mapping [3, 4]

$$G(x) = \begin{cases} (c_{i+1} - x)/(c_{i+1} - c_i) & \text{if } x \in [c_i, c_{i+1}) \\ 0 & \text{if } x = 0.5 \\ G(1 - x) & \text{if } x \in (0.5, 1] \end{cases} \quad (1)$$

where $x \in [0, 1]$, $0 = c_0 < c_1 < \dots < c_i < \dots < c_{N+1} = 0.5$, $N \geq 1$, $i = 0, 1, \dots, N$;

(b) a control register m-LFSR₁ with degree L_1 and period $T_1 = 2^{L_1} - 1$ (where m-LFSR₁ is a maximal length linear feedback shift register [5, 6]), and its internal states denoted by $U_k = (u_k, u_{k+1}, \dots, u_{k+L_1-1})$, $u_k \in \{0, 1\}$ for all $k = 0, 1, 2, \dots$,

(c) a perturbing register m-LFSR₂ (also a maximal length linear feedback shift register) with degree L_2 and period $T_2 = 2^{L_2} - 1$, and its internal states denoted by $V_k = (v_k, v_{k+1}, \dots, v_{k+L_2-1})$, $v_k \in \{0, 1\}$ for all $k = 0, 1, 2, \dots$

(2) **Seed keys:** Nonzero initial states x_0, U_0, V_0 ;

(ii) For $k = 0, 1, 2, \dots$, do

(1) clock m-LFSR₁ once and evaluate the number Δ_k by the form of the binary rate multiplier [5], i.e. $\Delta_k = 1 + \sum_{j=0}^{n-1} 2^{n-1-j} \cdot u_{k+L_1-j}$ (here $1 \leq n < L_1$);

(2) clock m-LFSR₂ once and extract the bit sequence V_{k+1} to perturb the chaotic system by assigning the state