ple is the cascade form, followed by parallel, wave, direct and ladder. The continued-fraction design is still of no interest.

(ii) Use of multiplier blocks can drastically change the complexity relations between different structures. Despite using almost twice the wordlength, and many more coefficients (corresponding to having almost 2.5 times the complexity using the C_1 measure), the direct forms require similar numbers of adders to the waveform. Similarly, but less dramatically, the cascade and parallel forms are significantly better than wave whereas the C_1 measure indicates they should be inferior. The wave filter loses out on two counts. Apart from the isolation of its coefficients, which prohibits the use of multiplier blocks, the wave structure has a much larger number of structural adders, which were not counted towards complexity in the C_1 measure.

(iii) The number of adders required to implement the coefficients as individual shift-add binary multipliers is about $(W_f/2 - 1)M \simeq C_1/2$, which is much greater than B in all cases, even in the wave case where coefficients are all isolated. The use of the various multiplier block algorithms therefore guarantees huge savings over a binary implementation.

(iv) The use of multiplier blocks tends to cancel out the cost difference between direct forms I and II due to the extra delay elements of form I. In fact, the deficit is overcompensated for by the saving due to the use of one large block, including all the coefficients. In other words, the non-canonic form I is superior to the canonic form II.

A single example has been examined of a general principle: that use of multiplier blocks changes the cost relationships between IIR structures. The changes are so dramatic that this one example, chosen because it was readily accessible and published all the necessary figures, is highly unlikely to be a statistical aberration. The results are also of interest because they are contrary to the original conclusions drawn. The use of the rounded statistical wordlength, as opposed to the actual rounded wordlength, may be criticised, but the value of the actual wordlength is highly dependent on factors specific to an individual design; the statistical wordlength is more likely to give results that are general. The multiplier block costs are also dependent on the specific integers in the coefficient set but the possible variation due to this factor does not contradict the general principle demonstrated by these results.

22 July 1994
Electronics Letters Online No: 19941288

A. G. Dempster and M. D. Macleod (*University of Cambridge, Signal Processing and Communications Laboratory, Department of Engineering, Trumpington Street, Cambridge CB2 1PZ, United Kingdom*)

References

1 AVENHAUS, E.: 'On the design of digital filters with coefficients of limited word length', *IEEE Trans.*, 1972, **20**, (3), pp. 206–212
2 CROCHIERE, R.E.: 'A new statistical approach to the coefficient wordlength problem for digital filters', *IEEE Trans.*, 1975, **CAS-22**, pp. 190–196
3 GRENEZ, F.: 'Design of FIR linear phase digital filters to minimise the statistical word length of the coefficients', *IEE J. Electron. Circuits Syst.*, 1977, **1**, (5), pp. 181–185
4 CROCHIERE, R.E., and OPPENHEIM, V.: 'Analysis of linear digital networks', *Proc. IEEE*, 1975, **63**, (4), pp. 581–595
5 FETTWEIS, A.: 'Wave digital filters: Theory and practice', *IEEE Proc.*, 1986, **74**, (2), pp. 270–327
6 GASZI, L.: 'Explicit formulas for lattice wave digital filters', *IEEE Trans.*, 1985, **CAS-32**, (1), pp. 68–88
7 DEMPSTER, A.G., and MACLEOD, M.D.: 'Constant integer multiplication using minimum adders', to be published in *IEE Proc. G*
8 DEMPSTER, A.G., and MACLEOD, M.D.: 'Multiplication by an integer using minimum adders'. Mathematical Aspects of Digital Signal Processing Colloquium, February 1994, (IEE)
9 BULL, D.R., and HORROCKS, D.H.: 'Primitive operator digital filters', *IEE Proc. G*, 1991, **138**, (3), pp. 401–412
10 DEMPSTER, A.G., and MACLEOD, M.D.: 'Use of minimum-adder multiplier blocks in FIR digital filters', to be published in *IEEE Trans. Circuits and Systems II – Digital and Analog Signal Processing*
11 DEMPSTER, A.G., and MACLEOD, M.D.: 'Use of multiplier blocks to reduce filter complexity'. ISCAS 94, April/May 19941994, (IEEE)
12 BULL, D.R., and HORROCKS, D.H.: 'Realisation techniques for primitive operator infinite impulse response digital filters'. ISCAS 93, 1993, (IEEE), pp. 607–610

Unsupervised segmentation of textured images using a hierarchical neural structure

H. Yin and N.M. Allinson

Indexing terms: Neural networks, Segmentation (image processing)

A hierarchical learning structure, combining a randomly-placed local window, a self-organising map and a local-voting scheme, has been developed for the unsupervised segmentation of textured images, which are modelled by Markov random fields. The system learns to progressively estimate model parameters, and hence classify the various textured regions. A globally correct segregation has consistently been obtained during extensive experiments on both synthetic and natural textured images.

Introduction: Markov random field (MRF) models have been widely used to analyse statistical textures [1, 2]. The equivalence between MRF and Gibbs, or Boltzman, distributions has been demonstrated [3]; there are apparent similarities between some properties of human visual processing and these statistical machines. The model parameters describe the interactions between the neighbouring pixels and can be compared to different features of human visual discrimination, such as orientation, patches and coarseness.

The Kohonen self-organising map (SOM) [4], when employed as a data clustering technique or a pattern classifier, will eventually minimise the mean-square distortions in its approximation of the input data space, at least locally. Lampinen and Oja [5] used an autoregressive (AR) series to model textures and proposed a self-organising AR model for segmenting textured images into meaningful regions. The SOM matching law and Widrow-Hoff learning rule were combined to obtain the model parameters. However, for two-dimensional images, causal AR series may not be a valid assumption because only unilateral neighbourhoods were used. In addition, their learning is pixel-based. The inhomogeneity of each single pixel could heavily affect the parameter estimation and the segmentation.

In the algorithm proposed here, a simple and crude estimate of local parameters is first obtained over a randomly-placed window. An SOM learns to classify these crude data and re-estimate the parameters and hence classify the different regions. A second level, local voting (LV) network, which represents the region label of the pixels, updates the label votes according to the winner of the SOM, in order to estimate texture labels.

Hierarchical structure: Texture regions are represented by patches of pixels rather than collections of isolated pixels. The boundaries between different regions are generally smooth. Using these properties, we apply a local window, termed the estimating window, which is randomly placed on the image at each iteration for characterising the local texture homogeneously and estimating the local MRF model parameters. These crude or noisy parameters are used as the inputs to a one-dimensional SOM network, whose size in terms of its total number of neurons is set by the number of regions to be segregated. The winning neuron indicates which texture type the current window is most like and forms an input to the next level for estimating the underlying region label. This second stage could be another SOM [6], however, in the present case, it is an LV network. The functional difference between employing an SOM or an LV network is that the former will converge to the mean of the input data distribution, whereas the latter will converge to its time average. When the estimator noise is an ergodic

process, the final result will be equivalent. However there are significant computational advantages in using an LV network. The estimating window is set to a large size at the beginning in order to form globally correct segmentation of patch-like texture regions. The randomness of positioning of the window at each iteration will ensure that consecutive inputs to the SOM network are uncorrelated. The effects of the shrinking window and the LV network are to reduce noise and to provide a clear segmentation.

Suppose that at time, t, the estimating window, denoted by $\Omega(t)$, is randomly placed on the image Π. The corresponding parameter estimate is expressed as $\Theta(t) = [\theta_1(t), \theta_2(t), \ldots \theta_M(t)]^T$, where M is the number of parameters. For the SOM, each neuron compares its weights $\mathbf{W}_k(t)=[w_1(t), w_2(t), \ldots w_M(t)]^T$, $k = 1, 2, \ldots N$ with the current input, $\Theta(t)$. The winning neuron then updates its weights according to the SOM learning law

$$\mathbf{W}_v(t+1) = \mathbf{W}_v(t) + \alpha(t)\{\Theta(t) - \mathbf{W}_v(t)\} \quad (1)$$

where $\{\alpha(t), t > 0\}$ is the scalar-valued adaptation gain. Normally there is no requirement to update the weights of the winner's neighbours as there is no need to topologically order the texture labels.

In the LV network, every pixel (i, j) has a voting unit, which represents its label variable and is an N-dimensional vector corresponding to the label votes to each region at location (i, j), i.e. $[l_{ij}^1(t), l_{ij}^2(t), \ldots l_{ij}^N(t)]^T$, which are set to zero at the start of learning. If the SOM's winning neuron is v, at time t, then the voting units are updated according to

$$\begin{aligned} l_{ij}^v(t+1) &= l_{ij}^v(t) + 1 \\ l_{ij}^k(t+1) &= l_{ij}^k(t) \end{aligned} \quad \text{for } (i,j) \in \Omega(t) \text{ and } k \neq v \quad (2)$$

The updating is restricted to the current estimating window. The largest voting element for every unit in the image indicates its region type, r, given by

$$l_{ij}^r(t) = \max\{l_{ij}^k(t)\} \quad \forall (i,j) \in \Pi \quad k = 1, 2, \ldots, N \quad (3)$$

Finally, the LV network will converge to the region's texture labels, and each neuron's weights in the SOM will converge to the model parameters of each region of the image.

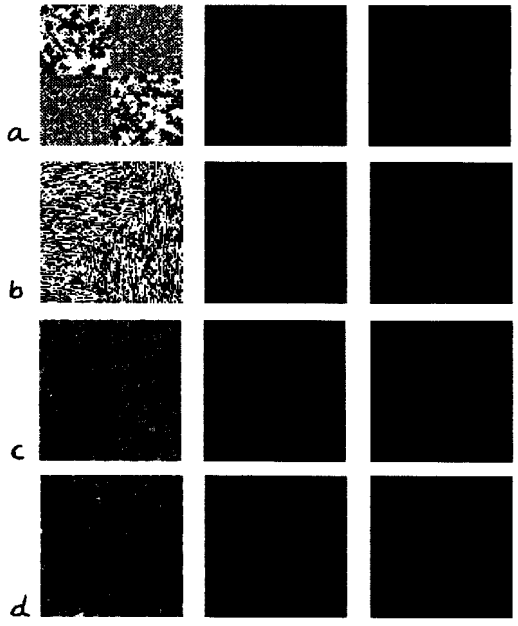

Fig. 1 *Typical segmentation results for synthetic and natural textured images*

a, b synthetic composite textures
c Brodatz images [7]: water (D38) and beach sand (D29)
d Brodatz images: grass lawn (D) and pressed calf leather (D24)

Experimental results: This hierarchical structure has been extensively applied in the segmentation of various synthetic and natural textured images. The conditions for the test results presented here are an image of 128 × 128 pixels and an initial estimating window of 70 × 70 pixels. This window shrinks as training progresses to a pre-specified limit. A second-order MRF model is employed. The least-square method is used for estimating model parameters over the estimating window, on the basis of its low computational cost. The pre-specified minimum size of the estimating window varies from image to image. It is found that for synthetic textures this size can be very small (typically 5 × 5 pixels) because such textures are very homogeneous. However for natural textures, which are often inhomogeneous, the local characteristics cannot be preserved for such small windows. The window size has to be larger than typically 10 × 10 pixels in order to maintain local homogeneity. After many iterations, the voting network will smooth out the effects of large windows and greatly reduce noise at the boundaries.

Some typical results, obtained after 2 000 iterations, are shown in Fig. 1. The left-hand picture in each sequence is a composite image of two different textures; the central image is the corresponding intermediate trained output of the SOM; the right-hand image is the final output after the LV network, i.e. the segmentation output of the entire system. The misclassified pixel errors are 4.92%, 1.91%, 2.56%, and 5.32%, for (*a*), (*b*), (*c*), and (*d*), respectively.

Conclusions: The Letter has shown how the SOM algorithm can successfully be incorporated with other local representation methods to construct a hierarchical network for the unsupervised segmentation of textured images. The simple computational forms have been adopted for each part of the structure and robust performance has been achieved.

1 September 1994
Electronics Letters Online No: 19941275

H. Yin and N. M. Allinson (*Image Engineering Laboratory, Department of Electronics, University of York, York YO1 5DD, United Kingdom*)

References

1 LAKSHMANAN, S., and DERIN, H.: 'Simultaneous parameter estimation and segmentation of Gibbs random fields using simulated annealing', *IEEE Trans.*, 1989, **PAMI-11**, (8), pp. 799–813
2 MANJUNATH, B.S., and CHELLAPPA, R.: 'Unsupervised texture segmentation using Markov random field models', *IEEE Trans.*, 1991, **PAMI-13**, (5), pp. 478–482
3 GEMAN, S., and GEMAN, D.: 'Stochastic relaxation, Gibbs distributions, and the Bayesian restoration of images', *IEEE Trans.*, 1984, **PAMI-6**, (6), pp. 721–741
4 KOHONEN, T.: 'Self-organization and associative memory' (Springer-Verlag, 1984)
5 LAMPINEN, J., and OJA, E.: 'Self-organizing maps for spatial and temporal AR models'. Proc. 6th Scandinavian Conf. on Image Analysis, 1989, pp. 120–127
6 YIN, H., and ALLINSON, N.M.: 'Self-organised segmentation for textured images'. Proc. ICANN'94, 1994, pp. 1149–1152
7 BRODATZ, P.: 'Textures: A photographic album for artists and designers' (Dover Publication, New York, 1966)

Security of RSA-type cryptosystems over elliptic curves against Hastad attack

H. Kuwakado and K. Koyama

Indexing terms: Cryptography, Public key cryptography, Number theory

It is shown that RSA-type cryptosystems over elliptic curves are more secure than the original RSA cryptosystem against the Hastad attack.

Introduction: In broadcast applications, the original RSA cryptosystem [1] is not secure if the encryption key e is small [2]. In other words, an attack based on the Hastad theorem (called the Hastad