experimentally observed scattering behaviour of different trapezoidal strip grating surfaces of the same period $d = 0.833\lambda$.

**Table 1:** Scattering behaviour of different trapezoidal strip gratings of period $d = 0.833\lambda$

| Strip grating dimensions | | Dielectric thickness | Optimum blazing angle of incidence | Bandwidth (below –40dB) |
|---|---|---|---|---|
| $a_1/\lambda$ | $a_2/\lambda$ | h/λ | | |
| | | | deg | GHz |
| 0.833 | 0.000 | 0.116 | 36.0 | 1.455 |
| 0.733 | 0.100 | 0.116 | 44.0 | 2.305 |
| 0.666 | 0.166 | 0.123 | 50.0 | 3.600 |
| 0.566 | 0.266 | 0.120 | 45.0 | 2.800 |
| 0.500 | 0.333 | 0.120 | 40.0 | 0.950 |
| 0.417 | 0.417 | 0.123 | 37.5 | 0.650 |

*Conclusions:* A trapezoidal strip grating on a dielectric substrate backed by a metallic ground plane eliminates specular reflections almost over the entire X-band frequency range. This broad-band behaviour is very suitable for applications such as RCS reduction techniques, frequency scanned reflectors etc.

*Acknowledgment:* The authors acknowledge the University Grants Commission, Govt. of India, for providing financial support. T. Mathew acknowledges CSIR, Govt. of India for providing a research fellowship.


*10 May 1994*
*Electronics Letters Online No: 19940729*

T. Mathew, D. S. Stephen, C. K. Aanandan, P. Mohanan and K. G. Nair (*Department of Electronics, Cochin University of Science and Technology, Cochin-682 022, India*)

**References**

1 JULL, E. V., HEATH, J. W., and EBBESSON, G. R.: 'Gratings that diffract all incident energy', *J. Opt. Soc. Am.*, 1977, **67**, pp. 557–560
2 HEATH, J. W., and JULL , E. V.: 'Perfectly blazed reflection gratings with rectangular grooves', *J. Opt. Soc. Am.*, 1978, **68**, pp. 1211–1217
3 JOSE, K. A., and NAIR, K. G.: 'Reflector backed perfectly blazed strip gratings simulate corrugated reflector effects', *Electron. Lett.*, 1987, **23**, pp. 86–87
4 MATHEW, T., STEPHEN, D. S., JOSE, K. A., AANANDAN, C. K., MOHANAN, P., and NAIR, K. G.: 'Performance of a novel simulated corrugated surface for the reduction of radar cross section', *Microw. & Opt. Technol. Lett.*, 1993, **6**, pp. 615–617
5 JULL, E. V., and BEAULIEU, N. C.: 'An unusual reflection grating behaviour suitable for frequency scanning'. IEEE AP-S Int. Antennas and Propagation Symp. Dig., 1980, pp. 189–191
6 STEPHEN, D. S., MATHEW, T., JOSE, K. A., AANANDAN, C. K., MOHANAN, P., and NAIR, K. G.: 'A new simulated scattering surface giving wide band characteristics', *Electron. Lett.*, 1993, **29**, pp. 329–331
7 KALHOR, H. A.: 'Electromagnetic scattering by a dielectric slab loaded with periodic array of strips over a ground plane', *IEEE Trans.*, 1988, **AP-36**, pp. 147–151

## Design of FIR linear phase filters with discrete coefficients using Hopfield neural networks

X. Zhang and H. Iwakura

*Indexing terms: Digital filters, Hopfield neural networks*

A novel method is presented for designing FIR linear phase filters with discrete coefficients using Hopfield neural networks. The proposed procedure is based on the minimisation of the energy function of the Hopfield neural network, and can produce a good solution to the design of FIR linear phase filters with discrete coefficients.

*Introduction:* To reduce the circuit complexity and maintain the designed filter's performance, it is preferable to design FIR digital filters with discrete coefficients to meet some desired specifications directly. There are many procedures [1, 2] relating to the design of FIR linear phase filters with discrete coefficients. Unfortunately, these approaches often have a very high computational cost and/or require complicated operations.

The purpose of this Letter is to develop a new method for designing FIR linear phase filters with discrete coefficients. The proposed procedure is based on the minimisation of the energy function of a Hopfield neural network [3], which is well known to be extremely effective in computing, and can provide a good solution to difficult optimisation problems. First, we describe how the design problem of FIR linear phase filters with discrete coefficients can be solved by the use of a Hopfield neural network, then present a design example to demonstrate the effectiveness of the proposed method.

*Hopfield neural network:* It is well known [3] that the Hopfield neural network can collectively compute good solutions to difficult optimisation problems. In a Hopfield neural network, neurons change their states according to the following motion equations:

$$\frac{du_i}{dt} = \sum_j T_{ij}V_j + I_i \tag{1}$$

$$V_i = g(u_i) = \frac{1}{2}\left\{1 + \tanh\left(\frac{u_i}{u_0}\right)\right\} \tag{2}$$

where $V_i$ and $u_i$ are output and input voltages of neuron $i$, respectively, $T_{ij}$ is a synaptic connection which connects the output of neuron $j$ to the input of neuron $i$, $I_i$ is an external input current, and $u_0$ is a positive constant. It has been shown that for symmetric connections ($T_{ij} = T_{ji}$) this network always leads to convergence to stable states. When the diagonal elements $T_{ii}$ are 0, and $u_0$ is small, the stable states are the local minima of energy function

$$E = -\frac{1}{2}\sum_i\sum_j T_{ij}V_iV_j - \sum_i I_iV_i \tag{3}$$

and the output $V_i$ of neurons in the stable states is 0 or 1.

*FIR filter design problem:* The magnitude response of an even-order FIR linear phase filter is defined as

$$H(\omega) = \sum_{i=0}^{N} a_i \cos(i\omega) \tag{4}$$

where $N$ is half the filter order, and the coefficients $a_i$ are restricted to be

$$a_i = \sum_{j=1}^{M} b_{ij}2^{-j} - b_{i0} \tag{5}$$

where $b_{ij} \in \{0,1\}$, and $M$ is an integer; then, the magnitude response of eqn. 4 becomes

$$H(\omega) = \sum_{i=0}^{N}\sum_{j=0}^{M} b_{ij}Y_{ij} \tag{6}$$

where $Y_{i0} = -\cos(i\omega)$, and $Y_{ij} = 2^{-j}\cos(i\omega)$ when $j > 0$

The FIR filter design problem can be viewed as an optimisation of the error function $E_{LS}$ in the specified frequency range $R \in [0 - \pi]$

$$E_{LS} = \int_R |H(\omega) - H_d(\omega)|^2 d\omega \tag{7}$$

where $H_d(\omega)$ is the desired magnitude response. For a lowpass filter,

$$H_d(\omega) = \begin{cases} K & 0 \le \omega \le \omega_p \\ 0 & \omega_s \le \omega \le \pi \end{cases} \tag{8}$$

where $K$ is a filter gain factor, and $\omega_p$ and $\omega_s$ are passband and stopband edge frequencies, respectively. To avoid the effect of non-uniformly distributed coefficient grid induced by discretising the filter coefficients, we search for an optimal filter gain factor $K$ between 0.75 and 1.5

Next, we describe how the design problem can be solved by a Hopfield neural network. We choose a representation scheme in which each power-of-two term $b_{ij}$ of the coefficients is specified by

the output $V_{ij}$ of a neuron, and form an objective function to be minimised as follows:

$$E = \alpha E_p + (1-\alpha)E_s + \beta E_d \qquad (9)$$

where $E_p$ and $E_s$ are the error functions in the passband and stopband, respectively, $\alpha$ ($0 \le \alpha \le 1$) controls the relative accuracies of the approximation in the passband and stopband,

$$E_d = \sum_i \sum_j b_{ij}(1-b_{ij}) \qquad (10)$$

is set to guarantee the output of neurons in the stable states to be 0 or 1, and $\beta$ can be decided by the diagonal elements $T_{ijij} = 0$. Then, by comparing the objective function of eqn. 9 with the energy function of eqn. 3, we can obtain the synaptic connections and the external input currents of the neural network as follows:

$$\begin{cases} T_{ijmn} = -2\left[\alpha\int_0^{\omega_p} Y_{ij}Y_{mn}d\omega + (1-\alpha)\int_{\omega_s}^{\pi} Y_{ij}Y_{mn}d\omega\right] \\ \qquad (i \neq m \text{ or } j \neq n) \\ I_{ij} = 2\alpha K\int_0^{\omega_p} Y_{ij}d\omega - \alpha\int_0^{\omega_p} Y_{ij}^2 d\omega - (1-\alpha)\int_{\omega_s}^{\pi} Y_{ij}^2 d\omega \end{cases} \qquad (11)$$

It is clear from eqn. 6 that $Y_{ij}$ is a cosine function of $\omega$, therefore the synaptic connections $T_{ijmn}$ and the external input currents $I_{ij}$ can be simply computed. Once the filter specifications are given, we can construct a Hopfield neural network by computing the synaptic connections and the external input currents of eqn. 11. We then simulate the equations of motion of eqn. 1 to obtain the stable states of the neural network. The output states of neurons in the stable states give a set of filter coefficients. The Hopfield neural network can find a good solution, but is not guaranteed to obtain the optimal solution. The quality of the solutions is dependent on the initial states of neurons to a great extent, and can be improved by using some simulated annealing techniques [4]. Here, to start with we choose some random initial states, then search for a best solution between the obtained solutions.

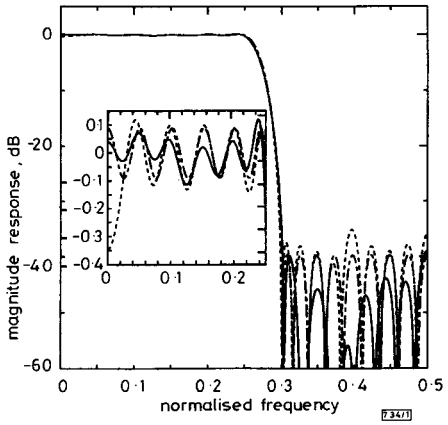


**Fig. 1** *Magnitude response of FIR lowpass filter*

——— neuron
- - - - REMEZ8
— · — REMEZ

*Design example:* The aim is to design an FIR linear phase lowpass filter with the following specification: the filter order is 40 ($N$ = 20), $M$ = 8, $\omega_p = 0.5\pi$, $\omega_s = 0.6\pi$ and $\alpha = 0.5$. An FIR lowpass filter is designed by using the proposed procedure. In this example, the stable states of the neural network have been computed 10 times from random initial states for each $K$, and $K$ is chosen from 0.8 to 1.5 with a step size $\Delta K = 0.1$. In the obtained solutions, the best filter response is chosen. The optimal filter gain factor is $K$ = 1.4 , and the resulting magnitude response is shown in Fig. 1. In Fig. 1, the magnitude responses of the continuous coefficient filter designed by the Remez algorithm (REMEZ) and the filter obtained by simply rounding the above continuous coefficients (REMEZ8) are shown also. It is seen that the proposed procedure performs better than the simple rounding by 4dB and is ~1dB away from the continuous design in the stopband.

*Conclusion:* A new design method for FIR linear phase filters with discrete coefficients has been proposed using a Hopfield neural network. The proposed procedure is based on the minimisation of the energy functions of a Hopfield neural network. A design example has been presented to show that the proposed procedure can provide a good solution to the design of FIR linear phase filters with discrete coefficients.


*11 April 1994*
*Electronics Letters Online No: 19940709*

X. Zhang and H. Iwakura (*Department of Communications and Systems Engineering, University of Electro-Communications, 1-5-1 Chofugaoka, Chofu-shi, Tokyo 182 Japan*)

**References**

1 KODEK, D.M.: 'Design of optimal finite wordlength FIR digital filters using linear programming techniques', *IEEE Trans.*, 1980, **ASSP-28**, pp. 304–308
2 LIM, Y.C., and PARKER, S.R.: 'Discrete coefficient FIR digital filter design based upon LMS criteria', *IEEE Trans.*, 1983, **CAS-30**, pp. 723–739
3 HOPFIELD, J.J., and TANK, D.W.: 'Neural' computation of decisions in optimization problems', *Biol. Cybern*, 1985, **52**, pp. 141–152
4 RUTENBAR, R.A.: 'Simulated annealing algorithms: an overview', *IEEE Circuits and Devices Magazine*, 1989, **5**, pp. 19–26

## Fortifying key negotiation schemes with poorly chosen passwords

R.J. Anderson and T.M.A. Lomas

*Indexing terms: Data privacy, Cryptography*

Key exchange schemes such as Diffie Hellman are vulnerable to middleperson attacks, and thus are often augmented by means of shared secrets. Where these secrets must be memorised, they will usually be vulnerable to guessing attacks. The authors show how collision-rich hash functions can be used to detect such attacks while they are in progress and thus frustrate them.

*Introduction:* In communications security design, one of the most important questions is whether an opponent will ever have unsupervised access to the equipment. If the answer is no, then we can greatly simplify the design by storing long term secrets. However, the equipment will then have to be well guarded at all times.

This may be feasible for military equipment, but in the commercial world, physical security procedures are generally insufficient to stop an opponent from obtaining occasional access. It follows that we must either use tamper resistant hardware, or avoid using long term secrets. In the latter case, the well known Diffie Hellman key negotiation scheme [1] is very useful, and has indeed been used in secure telephone designs.

The problem with the Diffie Hellman scheme is of course the middleperson attack; Eve interposes herself into the communications link between Alice and Bob, so that when Alice and Bob try to set up a secure channel, they actually end up with two: one between Alice and Eve, and another between Eve and Bob.

In some telephones, authentication is provided by the parties recognising each others' voices. There are applications, however, where more security is needed. Of course, if the users have the capacity to remember secret keys, then they can use the Diffie Hellman scheme followed by a challenge-response protocol to check that there is no intruder in the circuit [2]; this kind of solution is not always feasible, however.

*Remote login:* Consider for example the problem of remote login to a computer system, where a user $U$ wishes to access a host system $H$. It is well known that humans cannot in general remember good keys, and that the passwords which they are able to remember are likely to succumb to guessing attacks. We shall therefore assume that $U$ and $H$ share a password $P$ with $n$ bits of entropy, while the eavesdropper $E$ can perform $2^n$ computations.