~1 nm and inter-channel extinction ratio in excess of 15 dB. A broadband coupler was used to extract 15% of the signal power from the ring to the multi-wavelength laser output. The remaining 85% signal power was propagated through 9 km of dispersion shifted fibre (DSF) which equalised the channel powers through four wave mixing (FWM). The WDM channels did not experience Raman gain from the 1455 nm pump in the DSF as residual pump power was attenuated by the FBG circulator.

To determine CW operation of the laser each output channel was filtered in turn using two tunable, 3 nm bandpass filters in series to give sidemode suppression > 30 dB. The filtered channels were analysed using a photodetector with 100 ps rise time in conjunction with a 500 MHz bandwidth oscilloscope.

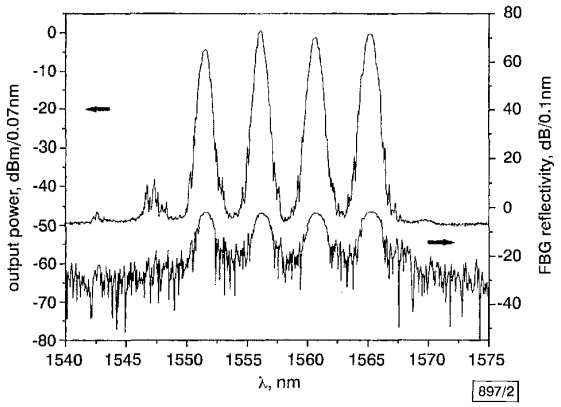

Fig. 2 *Spectra of laser output and reflectivity of FBGs*

Results: The output spectra of the multi-wavelength fibre Raman ring laser at a pump power of 0.55 W is shown in Fig. 2 accompanied by the reflectivity of the circulator coupled FBGs. The total output power of the multi-wavelength laser was 14.9 dBm. The highest channel power was 10.28 dBm at 1565 nm with the other channel powers within 5 dB. The 3 dB widths of the four channels were ~0.6 nm and extinction ratios of > 40 dB were observed. Comparisons between the spectra of the laser output and the reflectivity of the FBGs suggest that the spectral shape and power equalisation of the laser channels could be improved by using higher quality, specifically designed FBGs. It is envisaged that a greater number of FBGs could be used for a higher channel count and stretching of the FBGs would allow wavelength tuning of individual channels.

The operational characteristic for all four output channels analysed electrically was found to be dominantly CW. High frequency oscillations with a standard deviation from the DC level of ~10% were observed but not resolvable at the 500 MHz bandwidth limit. Similar results were observed when the 1455 nm pump source was analysed. Stimulated Brillouin scattering (SBS) in the long gain fibre was identified as another possible contributory factor to the small noise signal.

It is important to note that hysteresis of the wavelength channel powers with pump power was observed. This is believed to be a result of pump-power-dependent nonlinearity in the FBGs that affect the reflectivity of each FBG channel. It was also noted that the hysteresis changed when the length of DSF in the cavity was varied.

Conclusions: We have demonstrated a CW, room temperature four-wavelength fibre Raman ring laser employing FBGs. The four channels had line widths of ~0.6 nm, extinction ratios > 40 dB and powers ranging from 5.32 to 10.28 dBm between 1551 and 1565 nm. Temporal oscillations with an amplitude ~10% of the CW power were observed and attributed to pump fluctuations and SBS. The application of other FBGs could provide a higher channel count and offer wavelength tunability.

Acknowledgments: C.J.S. de Matos is supported by CAPES-Brazil. D.A. Chestnut and P.C. Reeves-Hall are supported by UK EPSRC studentships.

3 April 2001
Electronics Letters Online No: 20010574
DOI: 10.1049/el:20010574

C.J.S. de Matos, D.A. Chestnut, P.C. Reeves-Hall, F. Koch and J.R. Taylor (*Femtosecond Optics Group, Department of Physics, Imperial College, London SW7 2BW, United Kingdom*)

E-mail: pc.reeveshall@ic.ac.uk

References

1 IBSEN, M., RØNNEKLEIV, E., COWLE, G.J., ZERVAS, M.N., and LAMING, R.I.: 'Multiple wavelength all-fibre DFB lasers', *Electron. Lett.*, 2000, **36**, pp. 143–144

2 CHOW, J., TOWN, G., EGGLETON, B.J., IBSEN, M., SUGDEN, K., and BENNION, I.: 'Multiwavelength generation in an erbium-doped fibre laser using in-fibre comb filters', *IEEE Photonics Technol. Lett.*, 1996, **8**, pp. 60–62

3 PARK, N., and WYSOCKI, P.F.: '24-Line multiwavelength operation of erbium-doped fibre-ring laser', *IEEE Photonics Technol. Lett.*, 1996, **8**, pp. 1459–1461

4 WEI, D., LI, T., ZHAO, Y., and JIAN, S.: 'Multiwavelength erbium-doped fiber ring lasers with overlapwritten fiber Bragg gratings', *Opt. Lett.*, 2000, **25**, pp. 1150–1152

5 SOUSA, J.M., and OKHOTNIKOV, O.G.: 'Multiple wavelength Q-switched fibre laser', *IEEE Photonics Technol. Lett.*, 1999, **11**, pp. 1117–1119

6 KIM, S.K., CHU, M.C., LEE, D.H., and KIM, J.G.: 'Wideband multiwavelength erbium-doped fiber ring laser'. Tech. Dig. Postconference Edition. Trends in Optics and Photonics Vol. 37, Opt. Soc. America, 4, 8–10 Vol. 3, 2000

7 KOCH, F., REEVES-HALL, P.C., CHERNIKOV, S.V., and TAYLOR, J.R.: 'CW, multiple wavelength, room temperature, Raman fiber ring laser with external 19 channel, 10 GHz pulse generation in a single electro-absorption modulator'. Optical Fiber Conf. 2001 Tech. Dig. Series Conference Edition, Opt. Soc. America, 2001, Paper WDD7, pp. 1–3

Efficient and robust watermarking algorithm with vector quantisation

Hsiang-Cheh Huang, Feng-Hsing Wang and Jeng-Shyang Pan

A new method for watermarking based on vector quantisation is proposed. It is efficient for implementation with conventional techniques, and simulation results show its robustness under a variety of attacks. It also represents superiority over existing algorithms.

Introduction: Digital watermarking of images is one way to embed secret information, or the watermark, into the original image itself and/or into the secret key to protect the copyright of the original sources. Transform-domain techniques with discrete cosine transform (DCT) [1], and vector quantisation (VQ)-based watermarking schemes [2], have been explored. We make use of the characteristics of natural images and the efficient VQ compression technique for embedding the watermark into our system.

Algorithm: Let the input image be $\mathbf{X}$ with size $M \times N$. Our objective is to embed a robust watermark with VQ into $\mathbf{X}$, and have a watermarked reconstruction with a secret key at the output after the embedding process is accomplished.

Assume that the binary-valued watermark to be embedded is $\mathbf{W}$, the size being $M_W \times N_W$. We perform the VQ operation first [3] and obtain the codewords. We are then able to embed the watermark with the characteristics of the indices in the VQ domain. To survive picture-cropping attacks, a pseudorandom number traversing method [1] is applied to permute the watermark to disperse its spatial relationships. With a predetermined key, key_1, we have the permuted watermark $\mathbf{W}_p$ for embedding into the VQ indices.

In the VQ encoding procedure, $\mathbf{X}$ is divided into vectors $\mathbf{x}$ the size being $M/M_W \times N/N_W$, then each $\mathbf{x}$ finds its nearest codeword c_i in the codebook $\mathbf{C}$, and the index i is assigned to $\mathbf{x}$. While decoding with the VQ indices, the decoder merely performs a table

look-up process on the received index i' to obtain c_i' and then obtain the reconstruction image $\mathbf{X}'$.

In our algorithm, we perform VQ with the codebook size L. The codebook, $\mathbf{C}$, and the codewords, c_i, $i \in [0, L-1]$, can be denoted by

$$\mathbf{C} = \{c_0, c_1, ..., c_{L-1}\} \tag{1}$$

Assume that the block at position (m, n) of the original source $\mathbf{X}$ is $\mathbf{x}(m, n)$. After performing VQ, the indices $\mathbf{Y}$ and $\mathbf{y}(m, n)$ can be represented by

$$\mathbf{Y} = VQ(\mathbf{X}) = \bigcup_{m=0}^{\frac{M}{M_W}-1} \bigcup_{n=0}^{\frac{N}{N_W}-1} VQ(\mathbf{x}(m,n)) = \bigcup_{m=0}^{\frac{M}{M_W}-1} \bigcup_{n=0}^{\frac{N}{N_W}-1} \mathbf{y}(m,n) \tag{2}$$

To embed the binary watermark into the original source, we need to adopt some relationships, or the polarities, $\mathbf{P}$, between the two. For natural images, the VQ indices among the neighbouring blocks tend to be very similar, and we can consider this property to generate $\mathbf{P}$.

We calculate the variance of $\mathbf{y}(m, n)$ and its surrounding indices with

$$\sigma^2(m,n) = \left(\frac{1}{9}\sum_{i=m-1}^{m+1}\sum_{j=n-1}^{n+1}\mathbf{y}^2(i,j)\right) - \left(\frac{1}{9}\sum_{i=m-1}^{m+1}\sum_{j=n-1}^{n+1}\mathbf{y}(i,j)\right)^2 \tag{3}$$

The polarities based on the variances can be decided with a predetermined threshold value by

$$\mathbf{P} = \bigcup_{m=0}^{\frac{M}{M_W}-1} \bigcup_{n=0}^{\frac{N}{N_W}-1} \{P(m,n)\} \tag{4}$$

where

$$P(m,n) = \begin{cases} 1 & \text{if } \sigma^2(m,n) \geq \text{threshold} \\ 0 & \text{otherwise} \end{cases} \tag{5}$$

We set the threshold to be half of the codebook size, $L/2$, for convenience. We are then able to generate the secret key with the exclusive-or operation

$$key_2 = \mathbf{W}_P \oplus \mathbf{P} \tag{6}$$

After the inverse-VQ operation, both the reconstructed image, $\mathbf{X}'$, and the secret key, key_2, work together to protect the ownership of the original image.

From another point of view, the proposed algorithm is efficient for implementation with the conventional VQ compression algorithms. Once the codeword of each block is determined, we have the polarity of each block; consequently, we obtain the secret key. Both $\mathbf{X}'$ and key_2 are transmitted to the receiver.

In extracting the watermarks, we calculate the estimated polarities $\mathbf{P}'$ from $\mathbf{X}'$ first, and then obtain an estimate of the permuted watermark

$$\mathbf{W}_P' = \mathbf{P}' \oplus key_2 \tag{7}$$

Finally, we can perform the inverse operation of the permuted watermark with key_1 to acquire the extracted one, $\mathbf{W}'$.

Simulation results: In our simulation, we take the well-known test image, Lena, size 512 × 512, as the original source. We have the embedded watermark, rose, with size 128 × 128. The original source is divided into a 4 × 4 block for VQ compression, which also meets the number of bits to be embedded in the watermark. The watermarked reconstruction of the VQ compressed Lena image with the conventional VQ algorithm [3] is 31.53 dB with the codebook size 512. We employ the normalised cross-correlation (NC) for evaluating the effectiveness of our algorithm [1]. In addition to simulating our algorithm, we also make comparisons with the techniques in [2] under different attacking methods to show the superiority and usefulness of our method.

The simulation results using our algorithm are depicted in Fig. 1, and their corresponding outcomes with the methods in [2] are displayed in Fig. 2. The extracted watermarks when no attacks applied are shown in Figs. 1*a* and 2*a*, and their counterparts with a variety of attacking methods are illustrated in Figs. 1*b–h* and Figs. 2*b–h*, respectively.

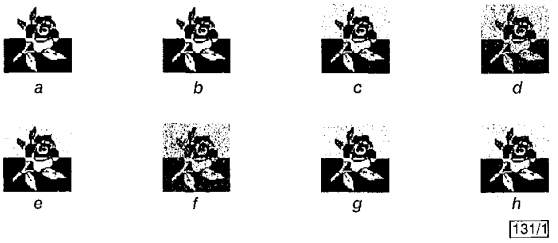

Fig. 1 *Extracted watermarks (size 128 × 128) and NC values of proposed algorithm under various attacking methods*

a No attack, $NC_1 = 1.0$
b VQ codebook 1, $NC_1 = 1.0$
c VQ codebook 2, $NC_1 = 0.9707$
d VQ codebook 3, $NC_1 = 0.8869$
e JPEG, $QF = 60\%$, $NC_1 = 0.9888$
f Image cropping, $NC_1 = 0.8604$
g Lowpass filter, $NC_1 = 0.9745$
h Median filter, $NC_1 = 0.9848$

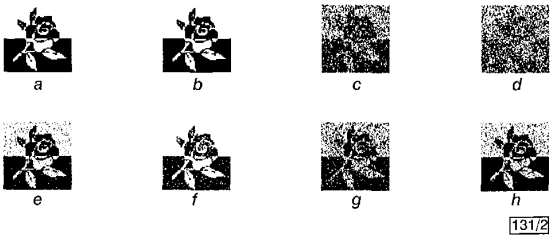

Fig. 2 *Extracted watermarks (size 128 × 128) and NC values using method in [2] to compare with Fig. 1*

a No attack, $NC_2 = 1.0$
b VQ codebook 1, $NC_2 = 1.0$
c VQ codebook 2, $NC_2 = 0.6798$
d VQ codebook 3, $NC_2 = 0.5914$
e JPEG, $QF = 60\%$, $NC_2 = 0.9095$
f Image cropping, $NC_2 = 0.8807$
g Low-pass filter, $NC_2 = 0.7370$
h Median filter, $NC_2 = 0.8657$

Figs. 1*a* and 2*a* show the extracted watermark when no attacking is applied. Both the NC values are 1.0, meaning that both the algorithms are able to extract the embedded watermarks perfectly because the embedded watermark and the extracted one are identical. Figs. 1*b–d* and Figs. 2*b–d* demonstrate the results under VQ attacks. Assume that there are three codebooks to be trained in advance. Codebook 1 is trained from Lena with size 512, codebook 2 is obtained by Pepper with size 512, and codebook 3 is acquired from both pepper and baboon with size 256. In view of the results shown, we are certain that our algorithm is robust under VQ attacks; in contrast, the methods in [2] failed to pass the VQ attacks with various codebooks.

We had other attacking methods, including JPEG compression with different quality factors (QF), image cropping, lowpass and median filtering techniques, on the watermarked image. The extracted watermarks and the NC values are shown in Figs. 1*e–h* and Figs. 2*e–h*, respectively. Among the extracted watermarks in our algorithm, those after experiencing JPEG with $QF = 60\%$, lowpass and median filtering attacks successfully survived because $NC \rightarrow 1.0$. The NC values in [2] are insufficiently high to compare with our results, since we adopt the information of the surrounding blocks to embed the watermark to resist the intentional attacks. Finally, although the NC in the image cropping case is somewhat smaller in our algorithm, the information conveyed therein is still recognisable. Therefore, we are able to claim the robustness and effectiveness of the proposed algorithm and its superiority in comparison with the methods in [2].

In summary, except for the image cropping case, the rest of the extracted watermarks in our algorithm have higher NC values. Generally, after experiencing the intentional attacks, our algorithm has better chances of survival. The techniques in [2] failed to pass some of the attacks. Therefore, the effectiveness of the proposed algorithm is demonstrated.

Conclusion: An efficient and robust algorithm for VQ-based watermarking has been presented. It is efficient since it uses the VQ indices to proceed with the embedding process, and to hide the information into the secret key. Hence, watermarked image quality would be guaranteed. In addition, in view of the simulation results under a variety of attacking techniques, we are able to claim its robustness, effectiveness, and superiority over the existing algorithm. Further work will concentrate on embedding multiple watermarks into the same original source in the VQ domain to protect the original source more effectively.

17 April 2001
Electronics Letters Online No: 20010567
DOI: 10.1049/el:20010567

Hsiang-Cheh Huang (*Department of Electronics Engineering, National Chiao Tung University, Hsinchu, Taiwan, Republic of China*)

Feng-Hsing Wang and Jeng-Shyang Pan (*Department of Electronic Engineering, National Kaohsiung University of Applied Sciences, Kaohsiung, Taiwan, Republic of China*)

References

1 HSU, C.T., and WU, J.L.: 'Hidden digital watermarks in images', *IEEE Trans. Image Process.*, 1999, **IP-8**, (1), pp. 58–68
2 LU, Z.M., and SUN, S.H.: 'Digital image watermarking technique based on vector quantisation', *Electron. Lett.*, 2000, **36**, (4), pp. 303–305
3 LINDE, Y., BUZO, A., and GRAY, R.M.: 'An algorithm for vector quantizer design', *IEEE Trans. Commun.*, 1980, **COM-28**, (1), pp. 84–95

Voice traffic multiplexing scheme with guaranteed QoS between VoIP access routers using DiffServ

E.J. Ha and J.T. Park

A new efficient voice traffic multiplexing scheme with guaranteed QoS between VoIP access routers using differentiated services (DiffServ) is presented. The performance of the proposed scheme for traffic with various bit rate types is analysed. The proposed scheme satisfactorily guarantees the QoS requirements.

Introduction: There is a growing interest in building a VoIP system because of the increase in use of the Internet. Low bit rate codes such as G.723.1 and G.729 are applied to the baseline codec of VoIP at present. Current VoIP transfer methods are still very inefficient due to their small payload in comparison with their large overhead. Moreover, the traffic load on the access routers tends to geometrically increase when the incoming traffic flow of short packets increases. These factors cause problems such as intolerable delay, jitter, and packet loss, which cause serious deterioration in the voice quality. There have been some related investigations dealing with these voice streams using a multiplexing technique [1]. These solutions do not satisfy the true QoS requirements. In this Letter, we propose a new QoS guaranteeing mechanism by combining a RTP/UDP/IP packet multiplexing scheme with DiffServ QoS architecture.

VoIP system architecture using DiffServ: We present an overall VoIP architecture and its multiplexing packet format using DiffServ. Fig. 1 shows the overall architecture. The number of access networks, connected to one ingress router depends on the real capacity of the ingress router. We use the RTP/UDP/IP packet multiplexing concept based on [2] to reduce the packet overhead. However, the major problem of [2] is that it does not take into account any QoS requirements. Thus, we expand the voice traffic multiplexing scheme in [2] in order to support QoS requirements. We propose a new multiplexing scheme using the diffserv code point (DSCP) of DiffServ. The key idea is as follows: Add a voice stream multiplexing scheme with identical destination IP address and DSCP.

To guarantee the QoS requirements, we propose a new RTP/UDP/IP packet format at the ingress router. We define a parameter *L_packet* (long packet), which adapts DSCP of DiffServ to RTP/UDP/IP packet format. Fig. 2 shows the *L_packet* format, which uses the ingress, intermediate, and egress routers. At the ingress router, the *L_packet*, which has the same destination and DSCP, is classified and sent to the egress router through several intermediate routers. At the intermediate router, it only transits the *L_packet* without any modification based on the DSCP value. At the egress router, the *L_packet*s that have arrived are separated and processed according to the priority of the DSCP value.

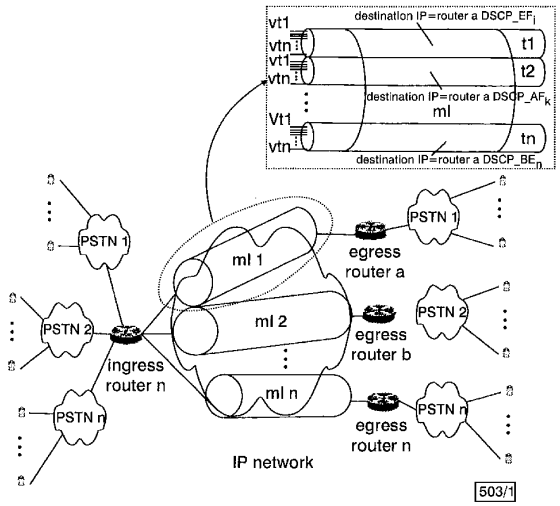

Fig. 1 *Overall architecture of proposed scheme*

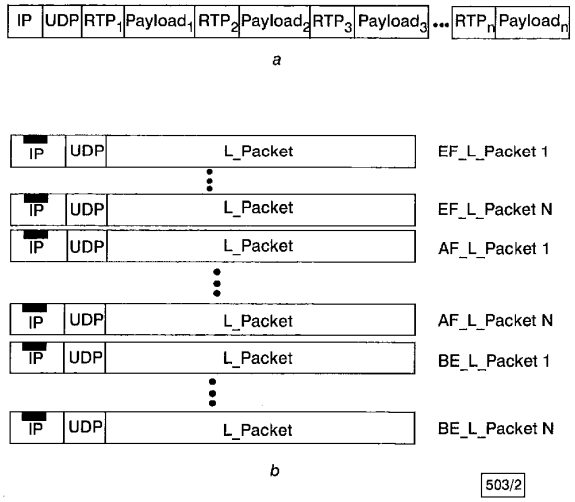

Fig. 2 *Multiplexing RTP/UDP/IP packet format*

a Previous RTP/UDP/IP packet format
b Proposed RTP/UDP/IP packet format using DiffServ

An ingress router contains a server, which is composed of DSCP_EF (DSCP expedited forwarding), DSCP_AF (assured forwarding), and DSCP_BE (best effort) queues. When large amounts of incoming voice traffic enter the ingress router simultaneously, packets are classified into different QoS guaranteed types by classifiers. At the policer, the classified packets are checked if they violate the bandwidth constraint requested in advance. Additionally, the qualified packets are queued in the DSCP_EF, DSCP_AF, and DSCP_BE server in turn. The process is executed in a first come first serve (FCFS) manner and a non-pre-emptive priority service discipline is employed.

Performance evaluation: In the near future, it is expected that the backbone network will be installed with a very high-speed WDM network with more than 10 Gbit/s. In this very high-speed backbone network, the main problem of QoS deterioration may be caused by poor bandwidth control. Thus, in Fig. 1, we describe the voice traffic blocking probability between VoIP access routers