An efficient encoding method that removes the statistical dependency of the height tree is also developed. Experimental results show that the height tree image coder offers meaningful improvements compared with other tree structure image coders.

11 November 1994
Electronics Letters Online No: 19950059

Yongkyu Kim and Kuy Tae Park (*Department of Electronic Engineering, Yonsei University, Seoul, Korea*)

Hyoung Gon Kim (*Division of Electronics and Information Technology, KIST, Seoul, Korea*)

References

1 ANTONINI, M., BARLAUD, M., MATHIEU, P., and DAUBECHIES, I.: 'Image coding using wavelet transform', *IEEE Trans.*, 1992, **IP-1**, (2), pp. 205–220
2 SHAPIRO, J.M.: 'Embedded image coding using zerotrees of wavelet coefficients', *IEEE Trans.*, 1993, **SP-41**, pp. 3445–3462
3 WITTEN, I.H., NEAL, R.M., and CLEARY, J.G.: 'Arithmetic coding for data compression', *Commun. ACM*, 1987, **30**, pp. 520–540
4 BARNARD, H.J., WEBER, J.H., and BIEMOND, J.: 'Efficient signal extension of subband/wavelet decomposition of arbitrary length signals'. SPIE Vol. 2094 Visual Communication and Image Processing, 1993, pp. 966–975

Wavelet vector quantisation scheme for image sequence coding at 64kbit/s

D.G. Sampson, E.A.B. da Silva and M. Ghanbari

Indexing terms: Image coding, Vector quantisation, Wavelet transforms

A new method for low bit rate video coding based on overlapped block matching and successive approximation wavelet vector quantisation is described. The main advantage of this scheme is that the most important data of the motion compensated interframe prediction error image are coded prioritarily, resulting in excellent coding performance. Simulation results show that at 64kbit/s, the proposed method outpertorms the RM8 implementation of H.261 by 2–3dB.

Introduction: The data compression of video signals is an important research topic with several applications, such as videotelephony, video-conferencing and high definition television (HDTV). In this Letter we propose a method for low bit rate video coding based on wavelet lattice vector quantisation. Motion estimation/compensation for the wavelet video coder is first discussed. It is shown that overlapped block matching (OBM) [1] significantly increases the efficiency of the wavelet transform coder. This is achieved by eliminating the blocking effects in the prediction error image introduced from conventional block matching. The motion compensated interframe prediction error signal is coded using successive approximation wavelet vector quantisation (SA-W-VQ) [2]. In this technique, the most important blocks of wavelet coefficients are successively coded by a series of vectors of decreasing magnitude. Moreover, the structural similarities between the wavelet bands of the same orientation are exploited by incorporating a block zero-tree structure. Simulation results demonstrate that the proposed video coder achieves excellent coding performance which outperforms most of the low bit rate wavelet video coding methods reported in the literature. Comparison with the RM8 model of the ITU (former CCITT) recommendation H.261 video coder [3], shows that the proposed coder gives a significant improvement in both the peak signal-to-noise ratio performance (2–3dB on average, at 64kbit/s) and the picture quality of the reconstructed frames.

Low bit rate video coding using wavelet lattice quantisation: We describe a new method suitable for the low bit rate coding of video signals. The proposed coder consists of two main parts:

(i) the motion estimation/compensation, where the overlapped block matching algorithm is employed

(ii) the wavelet vector quantisation method employed for the compression of the motion compensated interframe prediction error images, which is based on the successive approximation wavelet vector quantisation.

Temporal redundancy between successive image frames can be removed by taking into consideration the displacements of moving objects. Block matching (BM) motion estimation has been widely used in video coding applications. Although BM motion estimation has proved very successful in reducing the energy (and consequently the amount of data) of the interframe prediction error, it fails to estimate the true motion present in the scene. As a result of the discontinuities in the motion field, considerable blocking artifacts are introduced into the prediction error image. Blockiness on the boundaries of the motion blocks is translated to large signal power in the high frequency bands. This can significantly deteriorate the coding efficiency of sub-band/wavelet coders, where the entire image and not a small sub-image is transformed. Hence, it is important to employ a motion estimation/compensation technique that does not lead to blocking artifacts. To overcome this problem we have used a variation of block matching, where the blocks are overlapped with each other, the so-called overlapped block matching (OBM) motion compensation proposed in [1]. Here, we demonstrate the efficiency of OBM-MC for low bit rate video coding using the SA-W-VQ scheme.

We have developed an efficient method for coding wavelet transform coefficients [2]. In this method blocks of wavelet coefficients are quantised with a novel successive approximation vector quantisation (SA-VQ) scheme, such that blocks are coded progressively in several stages. At each stage, the residual quantisation error of the previous passes is further refined, until a certain level of distortion is achieved, or the bit rate budget is exhausted. This scheme works in a way that, at each stage the blocks with higher energy are coded first. The wavelet coefficient vectors are scanned according to their reconstructed values, the higher energies first, as in [4]. This guarantees that the most important information is always coded first, which is very desirable in video coding. Indeed, an important advantage of the proposed coding algorithm for video coding applications is that a constant bit rate can be achieved by allocating a fixed number of bits for each frame. This eliminates the need for a buffer to smooth out the bit rate variation. This is the result of always coding the most important coefficients (in terms of energy) first. This feature of the coder guarantees that the bit rate budget will be efficiently used for coding those image data that would result in maximum distortion. Furthermore, the use of lattice-based codebooks leads to a very simple encoding algorithm [5].

Simulation results: The performance of the SA-W-VQ for low bit rate video coding applications is evaluated and compared to the RM8 implementation of the standard H.261 video coder and the overlapped motion compensation/wavelet transform (OMC-WT) suggested in [1]. For our experiments, we have used the first 100 frames of three different image sequences, namely 'Miss America ', 'Claire ' and 'Salesman'. These are standard test sequences suitable for videophone and video-conference applications. We have used a two-stage wavelet transform, because it can be directly implemented with the original CIF image frames. The wavelet transform was implemented using the biorthogonal filter bank 6.b5_ra7 described in [6]. In all the experiments, the first frame of the sequence is coded using intraframe SA-W-VQ at 0.5bit/pixel. The orientation codebook of SA-W-VQ was based on the E_8-shell 1+2 lattice [5], which has given on average the best PSNR performance and also has a reasonable codebook size ($N = 2160$).

First, the efficiency of the overlapped block matching motion compensation (OBM-MC) for the SA-W-VQ video coder is demonstrated. Fig. 1 plots the PSNR performance of the coder using the OBM and the conventional BM motion compensation, for 'Claire' at 64kbit/s. In both cases, the core MC block is 16×16 pixels and a search area of ± 15 pixels is assumed. In the OBM-MC, the size of the overlapped blocks is 32×32 pixels and the window function is the 2-D raised cosine. In our simulations the absolute values of the horizontal and vertical components of the

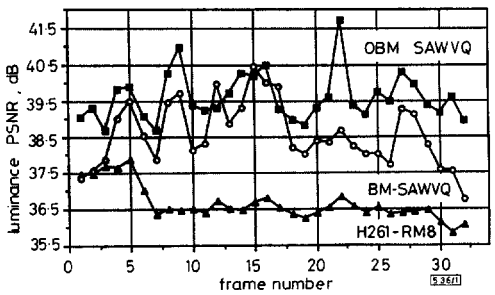

Fig. 1 *PSNR performance of 'Claire', CIF 10Hz at 64kbit/s*

—▲— H261-RM8
—○— BM-SAWVQ
—■— OBM-SAWVQ

motion vectors (including nonzero vectors) are coded using an adaptive arithmetic coder [7] and embedded in the bitstream. Fig. 1 shows the improvement in PSNR obtained by employing the OBM-MC instead of the conventional BM. This improvement is also reflected in the picture quality of the reconstructed frames. It is interesting to note that, with OBM, as opposed to conventional BM, there is no PSNR degradation as the sequence advances towards higher order frames.

The performance of the proposed coding scheme is also compared with the RM8/H.261 [3] and OMC-WT [1]. Fig. 1 illustrates the PSNR improvement achieved by the OBM-SAWVQ over the RM8 simulations. The picture quality of the OBM-SAWVQ coded pictures is very good and free of the annoying blocking artifacts in RM8 coded images. Table 1 shows the average luminance PSNR obtained by RM8, OMC-WT and the OBM-SAWVQ for 'Salesman' and 'Miss America', CIF 10Hz, coded at 64kbit/s. It can be seen that the proposed method outperforms both schemes by 2–3 dB.

Table 1: Average luminance PSNR performance comparison for the test image sequences, CIF 10Hz, 64kbit/s

Image sequence	Average *PSNR*	Method
	dB	
Miss America	39.15	OMC-WT [1]
Miss America	40.33	H.261-RM8
Miss America	41.98	OBM-SAWVQ
Salesman	32.50	OMC-WT [1]
Salesman	31.90	H.261-RM8
Salesman	34.50	OBM-SAWVQ

Conclusions: We have presented a new video coding method based on the lattice quantisation of wavelet coefficients. The OBM-SAWVQ video coder offers constant bit rate, with no need for a buffer, yet remarkably the PSNR fluctuations from frame to frame are reasonably small. This is because the SAWVQ always codes the most important image data first. Moreover, there is no quantisation error accumulation as the image sequence is advanced to higher order frames. Simulation results demonstrate that OBM-SAWVQ outperforms not only the RM8 implementation of the H.261 recommendation, but also most of the sub-band/wavelet coders reported for low bit rate video coding applications.

5 September 1994
Electronics Letters Online No: 19950057

D.G. Sampson, E.A.B. da Silva and M. Ghanbari (*Department of Electronic Systems Engineering, University of Essex, Colchester CO4 3SQ, United Kingdom*)

References

1 OHTA, M., and NOGASI, S.: 'Hybrid picture coding with wavelet transform and overlapped motion-compensated interframe prediction coding', *IEEE Trans.*, 1993, **SP-41**, (12), pp. 3416–3423
2 SAMPSON, D.G., DA SILVA, E.A.B., and GHANBARI, M.: 'Wavelet transform image coding using lattice vector quantisation', *Electron. Lett.*, 1994, **30**, pp.
3 CCITT SGXV Recommendation Reference Model 8: 'Coding for visual telephony'. Document 525, June 1989
4 SHAPIRO, J.M.: 'Embedded image coding using zerotrees to wavelet coefficients', *IEEE Trans.*, 1993, **SP-41**, pp. 3445–3462
5 SAMPSON, D.G., and GHANBARI, M.: 'Fast lattice-based gain-shape vector quantization for image sequence coding', *IEE Proc. I*, 1993, **140**, (1), pp. 55–65
6 DA SILVA, E.A.B., and GHANBARI, M.: 'On the coding gain of wavelet transforms'. 1994 IEEE Int. Symp. Circuits and Systems, London, June 1994, pp. 3.193–3.196
7 WITTEN, J.W., NEAL, R.M., and CLEARY, J.G.: 'Arithmetic coding for data compression', *Commun. ACM*, 1987, **30**, pp. 520–540

Multisecret-sharing scheme based on one-way function

J. He and E. Dawson

Indexing terms: Cryptography, Data privacy

The authors propose a multisecret-sharing scheme. In such a scheme, many secrets are shared in such a way that all secrets can be reconstructed independently. Each share is of the same size as that of any single shared secret. This is an improvement on a previously proposed multistage secret-sharing scheme.

Introduction: In [1] the authors proposed a multistage secret-sharing scheme. In such a scheme, many secrets are shared but only one share is kept by each user. The share is the same size as that of any single secret. The secrets must be reconstructed stage-by-stage in a specified order, although the reconstruction of secrets at earlier stages does not reveal or weaken the secrecy of the remaining secrets.

Multistage secret-sharing schemes have the restriction that secrets must be reconstructed in a prespecified order, which is not desirable in many applications. In this Letter we remove this order restriction by proposing a multisecret-sharing scheme which allows the secrets to be reconstructed without any order restriction. The scheme is based on a one-way function as in [1]. Note that, to achieve multiple secret-sharing with short shares, the security can no longer be unconditional as indicated in [2, 3]. Thus we use the weakest computational assumption, i.e. the existence of one-way functions [4].

Our key technique is to use one single secret many times without compromising the secret itself. To achieve this, we introduce the concept of two-variable one-way functions. We prove the existence of two-variable one-way functions based on the existence of traditional one-variable one-way functions. Then the exact same method of public shift technique in [1], together with a two-variable one-way function, can be used to share multiple secrets. Also, a simple solution is obtained for the problem of dynamic secret sharing [5].

Two-variable one-way functions: Intuitively, a (one-variable) function f is one-way if it is easy to compute but hard to invert, i.e. given x, the value of $f(x)$ can be computed in polynomial time, but any polynomial algorithm A can output a y such that $f(y) = f(x)$ upon input $f(x)$ (where x is chosen uniformly from the domian of f) with only a negligible probability. For formal definition of one-way functions, see, for example, [6].

Now consider a two-variable function $F(x, y)$. How should we define F to be a one-way function? One nontrivial property in which we are interested is the following:

From any given $F(x, y_1)$, $F(x, y_2)$,..., $F(x, y_l)$, where y_i $(1 \leq i \leq l)$ are known, it is hard to calculate any $F(x, y)$ for some $y \neq y_i$, $1 \leq i \leq l$.

A formal definition is the following, where $F[x]$ denotes the set of values $F(x,y)$ for all possible y.