Conclusion: Two fast recursive algorithms for computing the short-time DCT are proposed. The algorithms are based on a recursive relationship between three subsequent local DCT spectra. The algorithms require essentially fewer multiplications and additions compared with known fast DCT algorithms. The inverse transform for signal processing in a running window is also presented.

Acknowledgment: V. Kober acknowledges financial support from NATO and grant 99-01-00269 from the Russian Foundation for Basic Research.

23 April 1999
Electronics Letters Online No: 19990877
DOI: 10.1049/el:19990877

V. Kober and G. Cristobal (*Institute of Optics (CSIC), Imaging and Vision Department, Serrano 121, 28006 Madrid, Spain*)

E-mail: vkober@fresno.csic.es

References

1 OPPENHEIM, A.V., and SHAFER, R.W.: 'Discrete-time signal processing' (Prentice Hall, Englewood Cliffs, NJ, 1989)
2 VITKUS, R.Y., and YAROSLAVSKY, L.P.: 'Recursive algorithms for local adaptive linear filtration' *in* YAROSLAVSKY, L.P., ROSENFELD, A., and WILHELMI, W. (Eds.): 'Mathematical research' (Academy Verlag, Berlin, 1987), pp. 34–39
3 AHMED, N., NATARAJAN, T., and RAO, K.R.: 'Discrete cosine transform', *IEEE Trans.*, 1974, **C–23**, pp. 90–93
4 HOU, H.S.: 'A fast recursive algorithm for computing the discrete cosine transform', *IEEE Trans.*, 1987, **ASSP–35**, (10), pp. 1455–1461
5 SUEHIRO, N., and HATORI, M.: 'Fast algorithms for the DFT and other sinusoidal transforms', *IEEE Trans.*, 1986, **ASSP–34**, pp. 642–644
6 BRITANAK, V.: 'On the discrete cosine computation', *Sig. Process.*, 1994, **40**, (2–3), pp. 183–194

Robust sinusoidal watermark for images

H. Choi, H. Kim and T. Kim

A robust two-dimensional watermark for images which is quite secure and reliably detected under the influences of signal processing and/or geometrical alterations is proposed. The watermark is a matrix in which the rows are information-bearing pseudorandom sequences and columns are sinusoidal waves of a fixed frequency. The sinusoidal wave is used to confirm the existence of the watermark and to compensate for possible geometric distortion. To spread the energy across an image, the watermark is added to a set of selected samples in the sub-band domain. Experiments demonstrate the robustness and reliable detectability of the proposed watermark whether or not reference is made to the original image.

Introduction: Digital watermarking is a technique for embedding given information in digital audio signals or images under three conditions: (i) it should not be perceived by the users, (ii) it should not be easily tampered with, and (iii) the embedded information should be retrievable from mildly changed originals [1, 2]. Examples of embedded information are copyright owners, authorised users, and descriptions of the original data. In this Letter we introduce a new technique that is suitable for watermarking digital images.

Generation: A common watermarking process involves adding to the original image a sequence, called a watermark, representing the information to be embedded, where the sequence is taken from a nearly orthogonal set and is easily identified by a correlation detector. It is basically a well-known process in digital communications with orthogonal signals and additive noise [3]. The watermark energy contributes to the detection probability as in communication problems, but should be bounded from above by the condition that it should not be perceived by the users. The fact that perceptibility is related not to the total energy but to the local magnitude leads to the idea that the energy of the watermark should be maximised but should be spread over as large an area of the image as possible.

We consider a set of nearly orthogonal binary sequences, $\mathbf{a}_i$, $i = 1, 2, \ldots, L$, $\mathbf{a}_i = (a_{i1}, a_{i2}, \ldots, a_{iK})^t$, in which t represents the transpose, and index i carries the information to be embedded in the watermark; i.e. one of L pre-determined messages will be recognised by the detector. We define one of the two components of the watermark to be $\mathbf{u}_i = (u_{i1}, u_{i2}, \ldots, u_{iN})^t$, $u_{in} = 1/K \sum_{k=1}^{K} a_{ik}(\sin 2\pi k n/N)$, where N is adjusted to fit the size of the sub-image into which the watermark is to be embedded. Assume that $N \geq K$: we note that $\mathbf{u}_i^t \mathbf{u}_j = N/2K^2\, \mathbf{a}_i^t \mathbf{a}_j$ and that $\{\mathbf{u}_i, i = 1, 2, \ldots, L\}$ is a nearly orthogonal set.

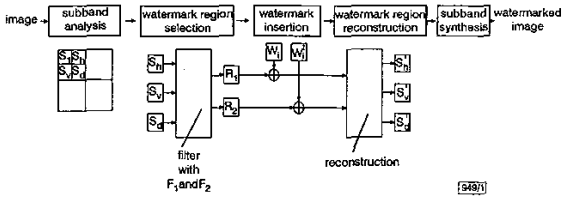

Fig. 1 *Watermark insertion*

The other component of the watermark is derived from the condition that it should be detectable after typical image processing and/or alteration. When a watermark undergoes geometric alteration, such as resizing, translation and rotation, the loss of synchronism hinders the detection. A sinusoidal wave of a fixed period spread out over a large area of an image is used to compensate for geometric distortions; it will be used as a reference for synchronisation in the detection process, especially when the watermark is inserted into the spatial domain.

Combining the above two components, we obtain the following two-dimensional watermark, denoted by a matrix W_i the (m, n)th element of which is

$$W_i(m,n) = \frac{A}{K}\left(\sin 2\pi b \frac{m}{M}\right)\sum_{k=1}^{K} a_{ik}\left(\sin 2\pi k \frac{n}{N}\right) \quad m = 1, \ldots, M \quad n = 1, \ldots, N \qquad (1)$$

where A and b are constants representing amplitude and frequency, respectively. Each row of the watermark is a noise-like sequence, and each column is a sinusoidal pattern. Either W_i or its transpose W_i^t or both can be used depending on the application. When used together, they can help detection under various geometric distortions.

Insertion: As pointed out in the Introduction, the watermark should be spread over as large an area of the image as possible. Insertion in the frequency domain naturally provides a solution, and is a popular approach in current research. To provide further security, we choose a watermark region which comprises a subset of original samples with which the watermark is mixed. A well-chosen watermark region will make erasures and attack difficult. Consider two watermark regions, R_1 for the watermark W_i and R_2 for W_i^t, among the sub-bands S_l, S_h, S_v, and Sd, which, respectively, denote the lowest-frequency, the horizontal mid-frequency, the vertical mid-frequency, and the diagonal mid-frequency sub-bands in the seven-band splitting shown in Fig. 1. Each of R_1 and R_2 is a set, or a matrix, of pixels of size S_l and is determined by the selection table of the same size: F_1 for R_1 and F_2 for R_2. For each location (m, n), the corresponding element $F_1(m, n)$ of F_1 takes a value from $\{h, v, d\}$, and R_1 is determined by the rule

$$R_1(m,n) = \begin{cases} s_h(m,n) & \text{if } F_1(m,n) = h \\ s_v(m,n) & \text{if } F_1(m,n) = v \\ s_d(m,n) & \text{if } F_1(m,n) = d \end{cases}$$

The region R_2 is determined likewise by F_2. The selection tables F_1 and F_2 serve as a protection key to the watermark. If we choose them to be dependent on S_l, on its pixel gradient for example, then the robustness of the watermark can be slightly enhanced at the cost of a small amount of security [4]. We can further include pixels from other sub-bands in the watermark regions in the same manner. Finally, the insertion process simply involves adding W_i

and W_i^I to R_1 and R_2, respectively. The watermark mixed into the sub-bands spreads out over the entire image after going through the synthesis operation, as intended. The proposed procedure is summarised in Fig. 1.

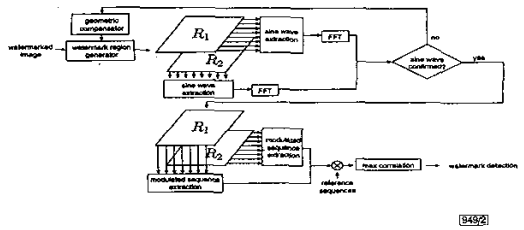

Fig. 2 *Watermark detection*

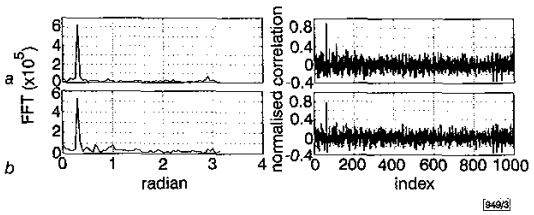

Fig. 3 *Detection results for JPEG coded (34.06dB) and resized Lena image*

a Detection with original
b Detection without original

Detection: The detection of the proposed watermark is performed in two steps. The first step is to confirm the existence and compensate for any distortion of the watermark, and the second step is to retrieve the hidden information. We first reconstruct R_1 and R_2 from the original image if it is available, or otherwise from the watermarked image. Since the lowest sub-band remains almost undistorted after common signal processing, we assume that correct reconstruction of the watermark region is possible without the original image. Next, we compute the projection sum of the pixel values along the rows of R_1 and along the columns of R_2. The projection operation averages out any unwanted random fluctuations in the pixel values to improve the detection performance. If the Fourier transform of the projection sum shows a prominent peak at frequency $2\pi b/M$, then the existence of the watermark is confirmed. On making a confirmation, we proceed to the second step in which the hidden information is extracted. We compute the projection sums of R_1 and R_2 along the direction orthogonal to those of the first step. By searching for the maximum cross-correlations between the projection sums and the reference sequences $\mathbf{u}_1, \mathbf{u}_2, ..., \mathbf{u}_L$, we finally determine the information-bearing index i among $\{1, 2, ..., L\}$. Should the geometrical alterations make watermark detection difficult, the sinusoidal structure of the projection sums in the first step can be used to compensate for the distortion. Because of insertion in the sub-band domain, geometric compensation is not as effective as insertion in the spatial domain. The overall detection scheme is summarised in Fig. 2.

Results: Experiments were performed on Lena and Pepper images of size 512×512. After the images were octave-band decomposed into seven sub-bands in two levels using Daubechies filters [5], the watermarks were embedded in the watermark region. When $A = 2$ and $b = 6$ were used, the watermarked images were indistinguishable from the originals. We carried out detection in two ways: with and without the original, under the influence of JPEG coding, additive Gaussian noise, lowpass filtering, cropping, and resizing. The detection was reliable in every case, and some results are shown in Fig. 3.

Remarks: The security of the proposed watermark is ensured by factors such as the pseudorandom sequences $\mathbf{a}_i$ or $\mathbf{u}_i$, $i = 1, 2, ..., L$, the sinusoidal frequency b, and the watermark regions R_1 and R_2. Since these factors encompass a sufficient degree of freedom, the proposed watermark can be considered relatively robust to hostile attempts.

The detectability without reference to the original is important in practice, because maintaining readily available original images is an enormous burden. We can also consider watermark detection without reference to the original as an express or prescreening procedure for the main detection.

10 May 1999
Electronics Letters Online No: 19990873
DOI: 10.1049/el:19990873

H. Choi, H. Kim and T. Kim (*School of Electrical Engineering and Institute of New Media and Communications, Seoul National University, Shillim-dong, Kwanak-gu, Seoul 151-742, Korea*)

E-mail: camel@pine.snu.ac.kr

References

1 COX, I.J., KILIAN, J., LEIGHTON, T., and SHAMOON, T.: 'Secure spread spectrum watermarking for multimedia', *IEEE Trans.*, 1997, **IP-6**, (12), pp. 1673–1687
2 SWANSON, M.D., KOBAYASHI, M., and TEWFIK, A.H.: 'Multimedia data embedding and watermarking techniques', *Proc. IEEE*, 1998, **86**, (6), pp. 1064–1087
3 VAN TREES, H.L.: 'Detection, estimation, and modulation theory' (John Wiley, 1971) [5]
4 CHOI, H., KIM, H., and KIM, T.: 'Robust watermarks for images in the subband domain'. Proc. IEEE Int. Workshop on Intelligent Signal Processing and Communication Systems, Nov. 1998, Vol. 1, pp. 168–172
5 WOODS, J.W.: 'Subband image coding' (Kluwer Academic Publishers, 1991)

Breaking and fixing the Helsinki protocol using SMV

Yuqing Zhang and Guozhen Xiao

An analysis is made of the Helsinki protocol using SMV, a model checker. The results show that the Horng-Hsu attack is the only successful attack on the protocol, and a new modified Helsinki protocol is proposed which is immune to the attack and better than the previous revised Helsinki protocol.

Introduction: The Helsinki protocol is a key establishment protocol contained in a draft international standard, ISO/IEC DIS 11770-3 [2]. It is designed to establish a shared secret key K_{AB} between two principals A and B, and the protocol messages are as follows:

$$\begin{aligned} 1 \quad & A \rightarrow B: \quad KT_{A1} = E_B(A, K_A, r_A) \\ 2 \quad & B \rightarrow A: \quad KT_B = E_A(K_B, r_A, r_B) \\ 3 \quad & A \rightarrow B: \quad KT_{A2} = r_B \end{aligned}$$

where $E_X(Y)$ denotes the public key encryption of data Y with X's public key, r_A and r_B are random nonces, and K_A and K_B are partial keys, generated by A and B, respectively. The final key K_{AB} is computed as a one-way function f of K_A and K_B.

Recently, Horng and Hsu proposed an active attack on the Helsinki protocol in [1]. This attack on the protocol allows an intruder C to impersonate another principal A to set up a false session with B. The attack involves two simultaneous runs of the protocol: in run 1, A establishes a valid session with C; in run 2, C impersonates A to establish a fake session with B. The Horng-Hsu attack is as follows:

$$\begin{aligned} 1.1 \quad & A \rightarrow C: \quad KT_{A1} = E_C(A, K_A, r_A) \\ 2.1 \quad & C(A) \rightarrow B: \quad KT_{A1} = E_B(A, K_C, r_A) \\ 2.2 \quad & B \rightarrow C(A): \quad KT_B = E_A(K_B, r_A, r_B) \\ 1.2 \quad & C \rightarrow A: \quad KT_C = E_A(K_B, r_A, r_B) \\ 1.3 \quad & A \rightarrow C: \quad KT_{A2} = r_B \\ 2.3 \quad & C(A) \rightarrow B: \quad KT_{A2} = r_B \end{aligned}$$

After these exchanges, A obtains the session key $K_{AC} = f(K_A, K_C)$, and B believes that it has established a shared secret key $K_{AB} = f(K_C, K_B)$ with A. This is an example of an 'insider attack'.