A TWO-DIMENSIONAL DIGITAL WATERMARK

A.Z.Tirkel(+), R.G.van Schyndel(*), C.F.Osborne(*)

(+)Scientific Technology,
P.O.Box 3018, Dendy Brighton, 3186, Australia.

(*) Department of Physics, Monash University,
Clayton, 3168, Australia.

ABSTRACT

This paper discusses the feasibility of coding a robust, undetectable, digital water mark on a standard 512*512 intensity image with an 8 bit gray scale. The watermark is capable of carrying such information as authentication or authorisation codes, or a legend essential for image interpretation. This capability is envisaged to find application in image tagging, copyright enforcement, counterfeit protection, and controlled access. The method chosen is based on linear addition of the water mark to the image data. Originally, the authors made use of one dimensional encoding using m-sequences [1],[2], a process which, whilst showing promise, had considerable shortcomings. This paper analyses constructions to extend this work to two dimensions and discusses compatibility of the technique with JPEG image transmission.

1 Review

There exist two basic classes of electronic water marks: fragile and robust. Interest in both types has increased in recent times because of the explosion in digital communications and the rapidity and ease of transmission of electronic material which is subject to copyright. The authors have been concerned with the construction of the robust type, i.e. one which is resilient to some image distortions such as pixel or bit tampering, cropping, translation, rotation and shear. Another form of robustness concerns lossy compression processing, such as coding via the Discrete Cosine Transform, such as JPEG. At this stage, our watermark possesses limited immunity against the first three pixel related distortions. In this paper, we discuss methods of addressing JPEG compatibility.
Our watermarking method differs significantly from the novel technique recently introduced by Walton [3]. This involves a fragile watermark, where, by deliberate design, ***any*** distortions render the watermark non-recoverable and this becomes proof of tampering. Both methods use LSB manipulation. Walton [3], also introduces an ingenious and effective palette manipulation technique to increase the watermark effectiveness by involving the complete RGB image components.
A totally different technique and its variations is reviewed in [4]. Its major advantage is its compatibility with the JPEG format, whilst its principal disadvantage is that the watermark recovery requires the presence of the unencoded image. In this respect it differs from the other techniques.
Our technique involves a linear addition of the watermark pattern, followed by a correlative recovery. Correlation can be defined as: cyclic or extended, global or character specific.
Correlation functions can be decomposed into: even and odd, or periodic and aperiodic. At this stage we are confined to binary characters only. Our watermarks are chosen from two-dimensional array patterns based on m-sequences or extended m-sequences. An m-sequence basis is chosen because of their balance (zero mean), random appearance, resilience to filtering, cropping and individual bit errors, optimal autocorrelation properties and constrained cross-correlation. The water mark can be encoded by the choice of m-sequences and their phases.

2 Method

Our encoding method uses LSB addition for embedding the water mark [1], [2]. In many imaging systems the LSB is corrupted by hardware imperfections or quantisation noise and hence its manipulation is invisible, or of limited significance. The linear addition process is difficult to crack and makes it possible to embed multiple watermarks on the same image [2]. The decoding process makes use of the unique and optimal auto-correlation of m-sequence arrays to recover the watermark and suppress the image content. Since the correlation process involves averaging over long strings of binary digits, it is relatively immune to individual pixel errors, such as may occur in image transmission. The correlation process requires the examination of the complete bit pattern and must therefore be performed off-line, unless some form of dedicated, real-time, parallel processing is involved. The decoding process is not completely error free, due to partial correlation of the image data with the encoding sequence. In our previous work, we overcame this by filtering and dynamic range compression [2]. These artificial steps would be undesirable in a practical system. A typical 128*128 (unfiltered) image encoded with a one dimensional watermark is shown in Fig.1(Top left). The message is encoded on a line by line basis, using the ASCII character to select a sequence phase shift. There are numerous message repeats. The decoder output Fig.1(centre left) shows distinct message correlation peaks (white). Note that there are significant sidelobes due to image crosscorrelation effects. The top half of Fig.1. shows encoded images that have been progressively high-pass filtered, removing 10, 60 and 100 of the spatial frequency components from the total of 128. The watermark peaks survive all these filtering processes, demonstrating the robustness of the technique. The image content in the original and the decoded version is rendered negligible after the second or third of the filters. It is also clear that the filtering introduces progressively more severe ringing in the decoded output. This can result in ambiguities. We are presently investigating the feasibility of rectifying this shortcoming by the introduction of a matched filter in the decoding process.

3. Watermark properties

An ideal watermark would possess:

(i) High in-phase autocorrelation peak for rows and columns [All]
(ii) Low out-of-phase autocorrelation for rows and columns [Costas Arrays]
(iii) Low cross-correlation between rows and between columns & between rows and columns [Perfect Maps, Hadamard Matrix, Legendre Arrays]
(iv) Low cross-correlation with image content [Folded M-sequence]
(v) Array diversity [Gold, Extended Gold Arrays]
(vi) Balance [All except Costas and some Gold]
(vii) Compatibility with standard image transmission format such as JPEG [Folded M-sequence].
(viii) Long span in order to prevent unauthorised cracking. [GMW codes]

The first two criteria are required for unambiguous watermark registration, the third is necessary to avoid scrambling, the fourth minimises image related artefacts, whilst the fifth is concerned with the information capacity of the watermark. The sixth criterion maximises the significance of the correlation operation: in the binary case, the minority symbol determines the correlation score.
The seventh criterion requires robustness against the low-pass filtering along a diagonal raster. It is described in more detail in 3.2. The eighth criterion relates to code inversion property. All codes can be generated by a recursion relation and this can be deduced from a sample of the code by solution of a set of simultaneous equations (matrix inversion). The minimum number of terms required for unambiguous inversion is called the span. M-sequences have a short span of 2n, where n is the order of the polynomial describing the recursion relation. This is because of their linear nature. GMW codes use non-linear recursion, which is optimised to yield much larger spans, with minimum impact on sequence properties. They are therefore ideal in situations where security is paramount.
Constructions can be optimised for each of these requirements. However, a global optimisation requires compromise. We have examined all the criteria in detail with particular reference to (iv) [8] and (vii).

3.1 Image crosstalk suppression

Clearly, it is possible to analyse the image content, by DCT or Walsh Transform and deduce a low crosscorrelation watermark by remapping any pattern, satisfying all criteria above except (iv). Similar effects could be assured by a random or adaptive search for a mapping to minimise the crosscorrelation with the image. However, such a procedure is impractical because there is no guarantee of uniqueness and hence the computation of the inverse mapping at the decoder.
There are at least three approaches which do not suffer from the above problem.

(1) Use longer m-sequences.
(2) Use high pass filtering.
(3) Use a "random" mapping.

The first is obvious (longer averagimg). The other methods rely on the low overlap of the spatial frequency content of the image and watermark. In most cases (except random or fractal images), the image exhibits a (peaked) spatial frequency content constrained to low frequencies. By contrast, the m-sequence content is almost perfectly white, as shown in Fig.2. Therefore, as demonstrated by Fig.1., high pass filtering can reduce image related artefacts, without significantly degrading the peak.

3.2 JPEG compatibility

As already demonstrated in Fig.1, the watermark is resilient against severe (0.25 quality factor) DCT high-pass filtering. Since the watermark mask is almost perfectly (spectrally) white, the same is true about low-pass filtering. In order to preserve this feature in raster format, the m-sequence should be embedded in a commensurate diagonal manner. The folded m-sequence of [5] is ideal for this purpose. The partitioning of the process into 8*8 blocks should pose no significant problems. The m-sequence employed in Fig.1. was 4 times longer than the linear dimension of the image, with no discernible effects on the result. We have actually experimented with 8*8 blocks and found no surprises. The only disadvantage of JPEG processing is that the high-pass filtering method of image-related artefacts (section 3.1) is incompatible, with the low-pass filtering involved in image compression. The same is likely to apply to the random mapping technique. Hence, the suppression of image related effects can only be achieved by the use of longer sequences. This imposes a limit on the information content of the watermark. The effects of sequence length on information content have been discussed in [1].
Another feature of JPEG processing is the capability of performing image manipulations on-line. This poses no problems at the encoding stage of our watermark. However, the watermark recovery process requires the execution of a sliding correlation to determine the location of a global maximum. At present, this process is being performed sequentially and hence off-line. We are investigating hardware and software techniques to render these operation parallel. Alternatively, a DCT-based correlation computation could be devised. This is also being examined.

4 Two-dimensional m-sequence based arrays

M-Sequences can be formed from starting vectors by a Fibonacci recursion relation. They are of maximal length (2^n-1) for a vector of length n. The autocorrelation function of an m-sequence is two valued: 2^n-1 (in phase), -1 (out of phase).

4.1 Extension of one dimensional arrays

A two-dimensional construction can be performed using a row by row phase shift. The effect on columns is that of decimation. Unique phase shifts as determined from Galois Field theory lead to the formation of columns, which are themselves m-sequences. The resulting array is an unbalanced Hadamard Matrix. Alternatively, a long sequence can be folded diagonally into an array format [5]. In this manner, the desirable one-dimensional autocorrelation property can be extended to two dimensions. The encoding and decoding performance of the Hadamard technique suffers from the image related effects because the correlations are performed on the (short and thus interference prone) row or column basis. The folded m-sequence is more immune to these effects, owing to its increased length. However, its information storage capacity is inferior. Watermarks encoded by both methods are presented, compared and analysed in the paper.

4.2 Intrinsic 2D constructions

We have also studied other fundamentally two-dimensional constructions. Costas Arrays are optimal in that their out-of-phase autocorrelation is minimum for shifts in either or both dimensions [6]. (Uniformly low sidelobe point- spread-function). They have been successfully deployed in radar and sonar, where time delays and frequency shifts (Doppler) can occur simultaneously. However, they are highly unbalanced and therefore prone to image related artefacts. Perfect Maps are constructions, where every m*n basis vector occurs once in a large pattern or map and hence can be used for automatic location. (An m-sequence is a one dimensional example of this category). The construction algorithm for Perfect Maps of large dimensions, commensurate with our image sizes is complicated [7]. However, some perfect maps are also Hadamard Matrices. We have examined examples of these, but still found them to be inadequate at rejecting image related artefacts. Legendre sequences and modified Legendre sequences, which are based on a quadratic residue (modulo n) and are similar to m-sequences of non-maximal length are also being studied. They are expected to improve on m-sequences for short lengths only. Extended m-sequences are attractive because they are commensurate with the image size (2^n). Whenever the extension by adding a zero to the m-sequence is performed to the longest run length of zeros, the resulting sequence still exhibits a strong in-phase autocorrelation peak of 2^n. This peak is surrounded by n zero values on either side, making it easy to recognise by filtering techniques. However, this is at the expense of numerous sidelobes at other phase shifts. The effect of these is being investigated. Gold Codes are linear additions of a preferred pair of m-sequences with a prescribed relative phase shift. Alternatively, they can be viewed as sequences generated by a non-maximal feedback configuration shift register constructed to implement a product of the individual m-sequence generating polynomials. The family of codes can be generated by all the relative phase shifts and the original parent m-sequences in 2^n+1, of which approximately half are balanced. The auto and cross correlations are constrained to approximately $2^{n/2}$. These linear codes can be folded into array format, just as m-sequences. They offer greater information storage capacity because of their great diversity and constrained correlations. Gold codes can also be extended to length 2^n in a similar manner to m-sequences.

4.3 Extensions to Multi-Dimensional Arrays

So far, our watermarking scheme has been confined to one and two-dimensional spatial constructions employing a gray scale image. Extensions to colour (RGB) encoding have the potential of enlarging the dimensionality to a total of 5. This could be employed for:

(i) Increasing the information content of the watermark. For example, three independent, two-dimensional messages could be encoded instead of one.
(ii) Increasing the length of the watermark code to reduce image related effects.
(iii) Redundancy coding.
(iv) Novel, multi-dimensional array coding.
(v) Non-binary character sequences.

These aspects are presently being evaluated.

4.4 Non-imaging applications

The watermarking technique discussed here has potential applications to audio copyright protection and audio system and equalisation control. Two one-dimensional patterns can be embedded in each of the stereo channels on CD-ROM or DAT. These codes could be designed to have a deliberately long span (such as GMW codes), in order to prevent cracking. This technique offers potential resistance to resampling/subsampling, which are akin to scaling/rotation. These codes could also be employed in automatic spectral and delay calibration/equalisation of the sound system, because of their optimal impulse response. This feature could be particularly useful in dynamic situations, where the audio environment is constantly changing.

5 Conclusion

This paper presents a method of encoding and recovery of a two-dimensional digital water mark on test images. The compatibility of the watermarking process with JPEG coding is discussed.

6 Acknowledgements

The authors would like to extend their gratitude to Nicholas Mee and Gerard Rankin for their assistance in mathematical theory and computer based sequence generation and analysis respectively. Their contributions have been invaluable.

7 References

[1] A.Z.Tirkel, G.A.Rankin, R.M.van Schyndel, W.J.Ho, N.R.A.Mee, C.F.Osborne. Electronic Water Mark. DICTA-93 Macquarie University, Sydney, December 1993. p.666-672.
[2] R.G. van Schyndel, A.Z.Tirkel, N.R.A.Mee, C.F.Osborne. A Digital Watermark. First IEEE Image Processing Conference, Houston TX, November 15-17, 1994, vol II, p.86-90.
[3] S.Walton. Image Authentication for a Slippery New Age. Dr.Dobb's Journal, April 1995. p.18-26, 82-87.
[4] F.M.Boland, J.K.K. Ó Rouanaidh and C.Dautzenberg. Watermarking Digital Images for Copyright Protection.
[5]. F.J. MacWilliams and N.J.A.Sloane. Pseudo-random Sequences and Arrays. Proc.IEEE, vol 64, 1715-1729, Dec.1976.
[6] S.W.Golomb and H.Taylor. Two-Dimensional Synchronization Patterns for Minimum Ambiguity. IEEE Trans. on Information Theory, vol IT-28, no.4, p.600-604, July 1982.
[7] T.Etzion. Construction for Perfect Maps and Pseudorandom Arrays. IEEE Trans. on Information Theory, vol 34, no 5, p.1308-1317. September 1988.

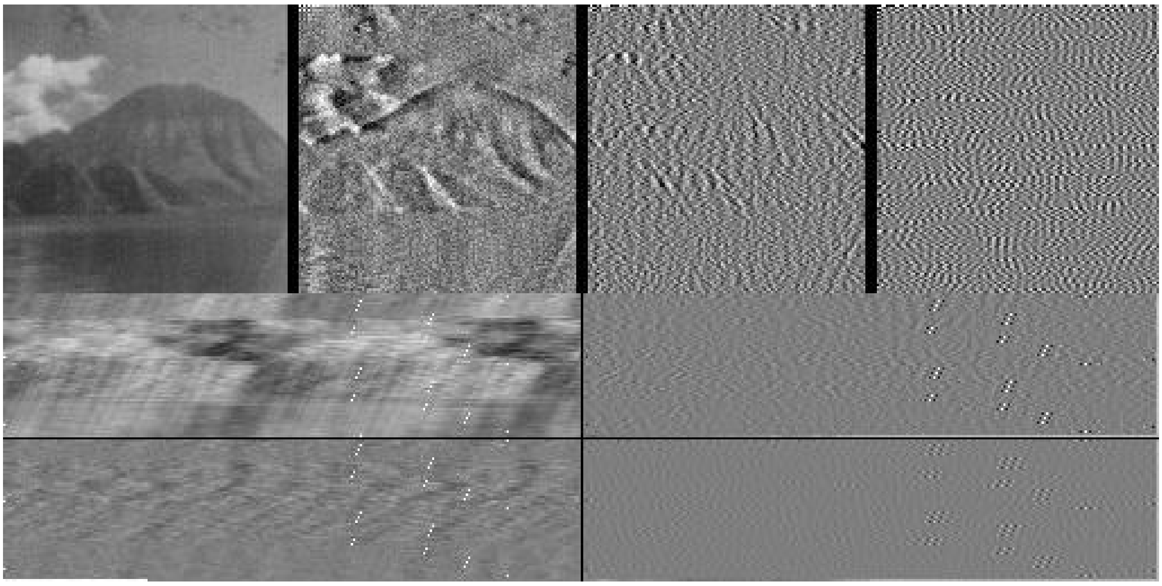

Figure 1
Upper (left to right: Encoded image after high pass filtering, removing
(a) 0, (b) 10, (c) 60, (d) 100 of 128 Spatial Frequency Components
Lower (Centre Left, Bottom Left, Centre Right, Bottom Right) : Corresponding Decoded Patterns
(Medium gray=0, darker=negative, lighter=positive - all image intensities have been suitably scaled)

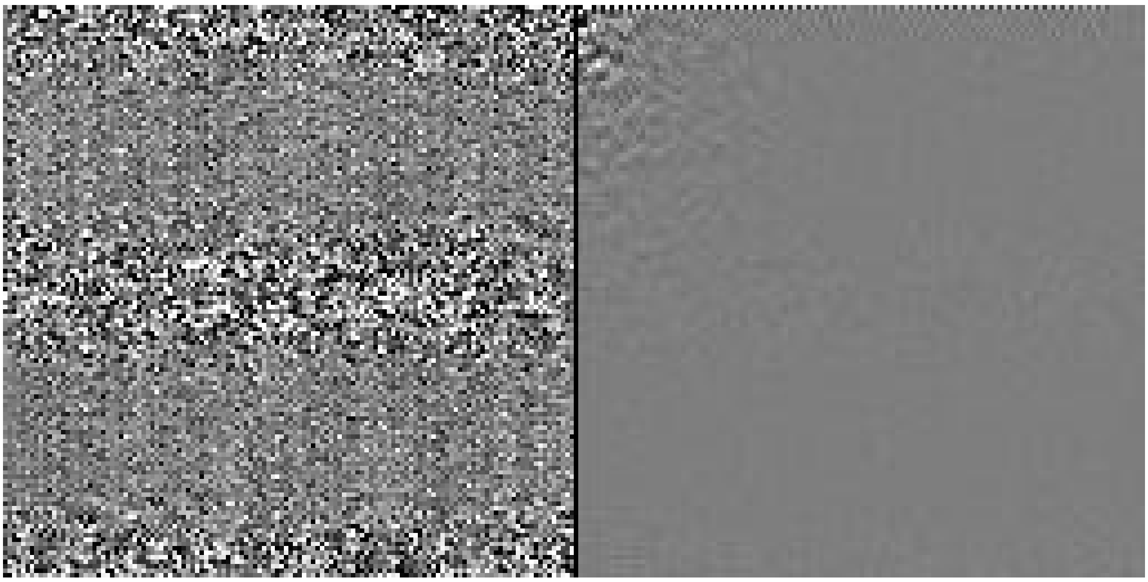

Fig 2.
Left - DCT of watermark
Right - DCT of image
(Interpretation as in Fig 1)