

# Secure Arrays for Digital Watermarking

A.Z.Tirkel, R.G. van Schyndel\*, T.E.Hall<sup>†</sup>, C.F.Osborne\*

<sup>†</sup>Department of Mathematics, Monash University, Clayton 3168. Australia.

\*Department of Physics, Monash University, Clayton 3168. Australia.

## Abstract

This paper introduces two-dimensional arrays for watermarking images. Binary, greyscale and colour (3D) arrays are examined. New constructions known as the “distinct sums” (ds) arrays are presented.

## 1. Background

A current objective of steganography (the art/science of information hiding) is to provide proof of ownership of an image or an audit trail through the use of an imperceptible watermark. Different methods achieve this aim, specifically for text, computer graphics natural images and multimedia. Most methods employ slight randomness inherent in or tolerable in a natural image. These techniques, introduced by Tirkel and Osborne in 1993 [9], and further reviewed in [3] resemble spread spectrum encoding. The watermark can be embedded in the spatial (pixel) domain [8], or transform domain, using magnitude [6] or phase [5]. Thresholding techniques using statistical and psychophysical masking criteria [6] have enhanced watermark robustness, without compromising detectability, by hiding information in statistically or spectrally significant regions of the image.

Many advances have occurred since 1993, but the issues of image registration and distortion compensation are still being resolved. Images can be distorted during transmission, deliberately or unintentionally by the recipient. Distortions include lossy compression, such as JPEG, cropping, rotation, skew, greyscale and colour translations, rescaling, frame reordering etc.

## 2. Introduction

Watermarks can be fragile or robust (resistant to most image distortions). This paper is concerned with the robust type.

Our correlative recovery process is intrinsically tolerant to some of these. Most importantly, the original (un-watermarked) image is not required. The method is based on embedding a suitable imperceptible pattern on the image.

This pattern is one of a library of arrays chosen by the author of the image. These can be cyclic shifts of the same array. Recovery is based on correlation with a template array as the basis of maximum likelihood. Where cyclic shifts of the one array form the entire ensemble,

autocorrelation is involved. Otherwise, the key property is cross-correlation between different arrays.

In the former case, the embedded array should possess the following properties, in order of diminishing importance: (1) high figure of merit for periodic/apperiodic autocorrelation; (2) approximate balance; (3) window property; (4) compatibility with size and aspect ratio required by standard image compression; and (5) random appearance. Property (1) is required for minimum ambiguity, (2) for minimum cross-correlation with the image, (3) for location of cropped, lost or corrupted data. The aperiodic autocorrelation is appropriate for isolated patterns, whilst periodic autocorrelation is used for the retrieval of repeated watermarks (mosaics).

## 3. Watermark Coding and Registration

Without loss of generality, we concentrate on arrays with entries  $-1,0,1$ , since in different applications, scaling of the entries can occur. Where the registration pattern is balanced (the number of 1's is approximately equal to the number of -1's), the mean value of the image intensity is unaltered.

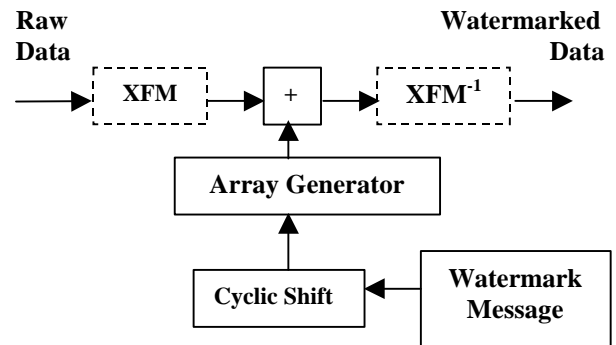
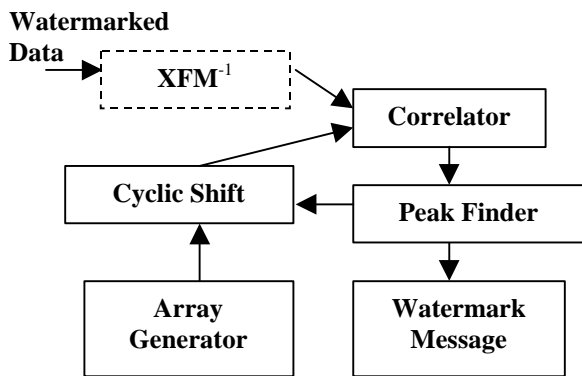


Figure 1. Encoding the watermark onto a data stream involves applying cyclically shifted binary array to the data stream (Note that the transforms (XFM) are optional and their use is application dependent).

Our recovery is based on the correlation of the encoded image with a template. It is insensitive to registration errors and image cropping, but susceptible to errors due to lossy compression, such as JPEG.



**Figure 2.** Watermark decoding is achieved by correlation of the encoded image with the ensemble of template arrays and their cyclic shifts until a peak is found. The cyclic shift and/or the choice of array determine the information in the watermark.

Imperfect registration results from cropping, or as a consequence of framing or sync corruption in the communication channel. This causes substitution or loss of pixels and results in improper watermark decoding. In schemes where watermark recovery is predicated on a comparison with the unwatermarked image, registration is achieved by subtraction. The method proposed by Tirkel and Osborne [7],[9] uses a correlative technique to recover the watermark. Importantly, this is achieved without reference to the original image. This technique relies on perfect registration, which can be accomplished by using a separate registration pattern [8].

#### 4. Orthogonal and Quasi-Orthogonal Arrays

Spread spectrum sequences have been studied by communications engineers because of their low autocorrelation and crosscorrelation sidelobes. Watermarking requires extension to two and three dimensions, which can be achieved by computer search or abstract algebra. The first is impractical for arrays with more than 40 binary elements.

The simplest implementation of the latter method is the generation of two-dimensional arrays from one-dimensional sequences.

##### 4.1 Distinct Sum Arrays

Our construction uses a seed sequence as a row in the array and derives the remaining rows as shifts of that seed. Pseudonoise sequences [2] are suitable seeds.

Our arrays can be derived analytically for prime lengths [7]. An example is shown in Figure 3, for the small prime 5: in practice, primes around several hundred could be used. Consider a seed row of length 5 (a Legendre sequence)

0	+	-	-	+
---	---	---	---	---

Adjacent rows are generated by applying differential cyclic shifts of the form 0,1,2,3,4. (The last shift is the cyclic wraparound). This is the array shown below as  $m=1$ . Array  $m=2$  has relative shifts 0,2,4,1,3 (0,2,4,6,8 reduced Modulo 5). Array  $m=3$  has relative shifts 0,3,1,4,2 (0,3,6,9,12 reduced Modulo 5). Array  $m=4$  has relative shifts 0,4,3,2,1 (0,4,8,12,16 reduced Modulo 5)

0	+	-	-	+
0	+	-	-	+
+	0	+	-	-
-	-	+	0	+
+	0	+	-	-

$m = 1$

0	+	-	-	+
0	+	-	-	+
-	+	0	+	-
+	0	+	-	-
-	+	0	+	-

$m = 2$

0	+	-	-	+
0	+	-	-	+
-	-	+	0	+
+	-	-	+	0
-	-	+	0	+

$m = 3$

0	+	-	-	+
0	+	-	-	+
+	-	-	+	0
-	+	0	+	-
+	-	-	+	0

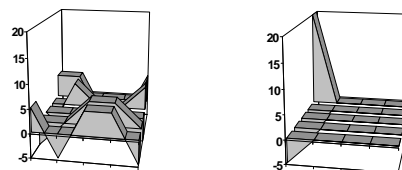
$m = 4$

**Figure 3.** “distinct sums” Array Generation Method

The “distinct sums” construction determines the relative shifts so that the resultant array can only have 0 or 1 columns matching compared with any shift of itself. When the seed sequence of length  $q$  is pseudonoise, its autocorrelation values are  $q,-1$ . The autocorrelation of such an array is  $pq, -p, q-p+1$ . For  $p \approx q$ , the sidelobes tend to  $-p$  and  $+1$ . For large  $p$ , these become negligible compared with the crosscorrelation with the image. The major sidelobe is negative, so where polarity is preserved or known, it can be disregarded. The required sequence of shifts possesses the “distinct sums property” (dsp). Where sequences of shifts do not possess dsp, the autocorrelation depends on the number of columns which can match simultaneously.

For prime array lengths such as  $p=5$ , representative auto and crosscorrelation plots are shown in Figure 4, demonstrating the quasi-orthogonal nature of these arrays.

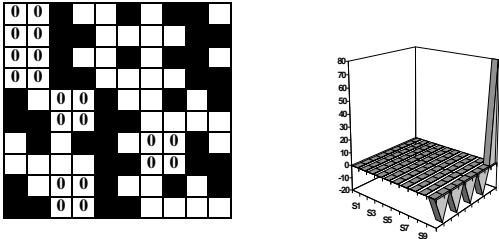
Low cross-correlation between different arrays is due to 0, 1, or 2 columns, from  $p$  columns, matching.



**Figure 4. Auto and Cross Correlation of a 5x5 “distinct sums” Array**

## 4.2 Non-prime Distinct Sum Arrays

The “distinct sums” arrays can be convolved with other arrays [4] with desirable properties, to generate new arrays of different sizes, with predictable auto and crosscorrelations. For example, a 10x10 array can be constructed from a Legendre Sequence of length 5.

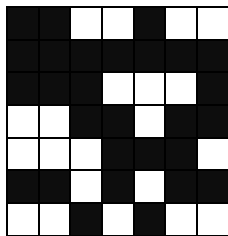


**Figure 5.**

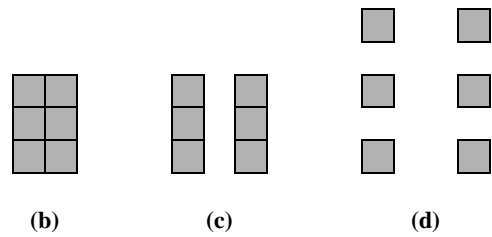
**10x10 Ternary Array and its Autocorrelation**

## 5. Significant Properties of DS Arrays

The distinct sums arrays possess some unusual properties due to their method of construction. Some of these are discussed below. Distinct sum arrays can exhibit the window property for several simultaneous “split” windows.



**Figure 6a. 7x7 “distinct sums” Array (m=1)**



**Figure 6b-d. Different Possible Split Windows**

Colour watermarks can be treated as sets of ordered triples (RGB) or as arrays over a non-binary alphabet. The former case enables embedding and correlative recovery of 3 quasi-orthogonal binary arrays (different values of  $m$ ) on the different colours. This increases the information capacity and the diversity of watermarks, whilst maintaining the accuracy of the recovery process.

## 6. Conclusion

Quasi-orthogonal two dimensional watermarks can be generated using the distinct sums construction. Such arrays meet the criteria outlined in Section 2. These arrays are expected to find application in watermarking, coded aperture imaging and image compression.

## 7. References

1. I.J.Cox, J.Kilian, T.Leighton, T.Shamoon. Secure Spread Spectrum Watermarks for Video. ICIP-96, Lausanne, September 16-19, 1996. p.243-246.
2. D. Everett. “Periodic Digital Sequences With Pseudonoise Properties”. GEC Journal, 1966, Vol. 33, No.3, p.115-126.
3. G.C.Langelaar, J.C.A. van der Lubbe, J.Biemond. “Copy Protection for Multimedia Data Based on Labeling Techniques” <http://www.it.et.tudelft.nl/pda/smash/public/benelux.cr.html>
4. Lüke. Binäre Folgen und Arrays mit optimalen48, (1994) p.213-220.
5. Ó Ruanaidh, W.J.Dowling, F.M.Boland. Phase Watermarking of Digital Images. Proc ICIP-96, Lausanne, September 16-19, 1996. p.239-242.
6. M.D.Swanson, B.Zhu and A.Tewfik. “Transparent Robust Image Watermarking”. Proc ICIP-96, Lausanne, September 16-19, 1996. p.211-214.
7. A.Z.Tirkel, T.E.Hall, C.F.Osborne. “Steganography-Applications of Coding Theory”. IEEE Information Theory Workshop, Svalbard 1997, p.59-60.
8. A.Z.Tirkel, C.F.Osborne, T.E.Hall. Image and Watermark Registration. Special Issue, “Signal Processing”
9. 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, Sydney, December 1993. p.666-672.