# Key Independent Watermark Detection

*R.G. van Schyndel*, A.Z. Tirkel[+], I. D. Svalbe**
*Department of Physics, Monash University, Clayton, 3168, Australia.
[+]Scientific Technology, 8 Cecil St, E.Brighton, 3187, Australia.

## Abstract

*Many types of pseudo-random signals have been used to embed signatures as watermarks, with spread spectrum signal techniques used to recover the signature from the encrypted data. Legendre sequences are a suitable candidate for signature encryption as they exhibit 'perfect' two level auto-correlation.*

*Additionally, Legendre sequences have the unusual and interesting property of invariance under Fourier transformation; the spatial and frequency representation of each sequence is identical up to a phase factor.*

*The presence of a Legendre-based watermark, embedded in the pixel or transform domain, can be detected by cross-correlating a sequence-encrypted image with its Fourier transform. This property enables verification of the presence of a watermark (of specified length), without requiring prior knowledge of the sequence type or key used for the encryption.*

**Keywords:** Multimedia, Data Security, Watermarking, Electronic Commerce

## 1. Introduction

Pseudo-random, spread spectrum sequences have been used as digital watermarks for over 5 years [9]. The ability to embed and recover a signature on audio signals, in images, or any other digital data, with minimal perceptual perturbation, has received a great deal of attention in many multi-media applications [2]. Here, we focus on the task of verifying the presence of a watermark, without requiring prior knowledge of the key or sequence details used to embed the signature. Establishing the presence of a watermark, prior to and independently of examining the watermark contents, will enable agents, for example server software, to automatically monitor and control data transfer rights, such as Internet copying.

This paper demonstrates that the above aims can be achieved successfully by encoding signatures onto digital data using Legendre sequences or arrays. The Fourier invariance property of Legendre sequences is the essential element in making our scheme work.

The correlation and Fourier invariance properties of Legendre sequences are presented, for simple 1D signals in section 2, with the details of our signature embedding and recovery scheme given in section 3. In section 4, we extend the analysis to 2D Legendre arrays, which lend themselves more appropriately to image watermarking. Section 5 discusses the information storage capacity of 2D arrays. The comparable technique of triple correlation for blind signature detection, applicable for linear "shift and add" invariant signals (such as M-sequences), is discussed in section 6. In section 7, we present some sample results.

## 2. Legendre Sequences and Fourier Invariance

The binary Legendre sequence [3] is a sequence with optimal auto-correlation properties. Such a sequence, $\boldsymbol{b_n}$, is defined by:

$$b_n = (n/p) = \begin{cases} 1, & n \in \Re \\ -1, & n \in \aleph \\ 0 & n \equiv 0 \end{cases} \tag{1}$$

where $\boldsymbol{p}$ is prime, $0 < \boldsymbol{n} < \boldsymbol{p}$, $\Re$ is the set of quadratic residues for the finite field $\boldsymbol{Z_p}$, and $\aleph$ is the set of non-residues over the same field. The Legendre sequence above can be generalised from binary to a grey level sequence, $\boldsymbol{a_n}$, comprised of values given by an alphabet of the higher roots of unity, [8]. The above equation becomes:

$$a_0 = 0$$

$$a_n = \exp\left(\frac{2\pi i\, r\, \mathrm{ind}_g\, n}{(p-1)}\right)$$

$$r \neq 0 \bmod (p\text{-}1),\ \mathrm{n} \neq 0 \bmod p, \tag{2}$$

where ***r*** is a scaling factor, $ind_g$ is the index function (or 'number-theoretic logarithm'), defined as the exponent of ***g***, a primitive root of the prime ***p***, required to produce *n*. There are (***p–2)*** Legendre sequences of length ***p***. Schroeder shows that the Discrete Fourier Transform (DFT), $\boldsymbol{B_n}$, of the binary Legendre sequence is

$$B_n = \sqrt{p} b_n, \qquad p \equiv 1 (\mathrm{mod}\, 4)$$

or

$$B_n = -i\sqrt{p} b_n, \qquad p \equiv 3 (\mathrm{mod}\, 4) \tag{3}$$

and that the DFT of the higher-alphabet Legendre sequence, $\boldsymbol{A_n}$, is

$$A_n = A_1 a_n^*, \tag{4}$$

that is, the conjugate Legendre sequence is related to its discrete Fourier transform by a complex constant, $\boldsymbol{A_1}$, the first component of the Fourier transform. The magnitude of this constant is √p, whilst the angle depends on the value of the multiplier *r*.

The following example illustrates this feature. Consider a binary Legendre sequence of length 5. Legendre sequences of length p = 4k+1 have a zero first element, the other elements are of unit magnitude. In this case the phase is 0 or π.

$$b_n = \quad 0, \quad 1, -1, -1, \quad 1$$

The Discrete Fourier Transform, $\boldsymbol{B_n}$, of this sequence:

$$B_n = \quad 0, \quad \sqrt{5}, \sqrt{-5}, \sqrt{-5}, \quad \sqrt{5}$$

is identical to $\boldsymbol{b_n}$ to within the scale factor √5.

The periodic cross-correlation, $\theta_k$ of data items, $\boldsymbol{d_n}$, with reference sequence, $\boldsymbol{a_n}$, both of length ***p***, is defined as:

$$\theta_k = \sum_{\substack{n=0 \\ n+k \neq 0}}^{p-1} d_n a_{n+k}^* \tag{5}$$

where *n+k* is reduced modulo *p* and * denotes complex conjugation. The periodic *auto-correlation* values, $\boldsymbol{R_k}$, of the sequence $b_n$ are:

$$R_k = \quad 4, -1, -1, -1, -1$$

The *cross-correlation* values of the sequence, $b_{n+k}$, with the DFT coefficients $B_n$, are

$$\theta_k = \quad 4\sqrt{5}, -\sqrt{5}, -\sqrt{5}, -\sqrt{5}, -\sqrt{5}$$

$\theta_k$ is a perfect two-valued cross-correlation, as is the auto-correlation of the sequence. This feature makes the Legendre sequence a unique watermark, in that the sequence and its Fourier transform have the same auto- and cross-correlation up to a scale factor. The Fourier invariance property is dependent on the sequence being in its characteristic phase (i.e. beginning with the zero magnitude term). It does not apply to non-zero cyclic shifts of the sequence. This is because a time shift in a sequence translates to a phase shift of the Fourier transform, this phase shift is different for different Fourier coefficients.

If a sequence is displaced from its characteristic phase by a cyclic shift $\tau_0$, then for any offset

$$\tau = -\tau_0 \bmod p \tag{6}$$

the characteristic phase is restored.

A simple implementation would restrict the embedded watermark to Legendre sequences in their characteristic phase only. Information could then be stored in the choice of the multiplier ***r*** of equation 2. Alternatively, the correlation process could involve two separate shift operations in order to find a global correlation peak: a shift operation for the Fourier transform computation and a shift operation on the reference template.

Although Legendre sequences have complex values, it is clear that, except for the first element, the sequence is entirely expressed in the complex phase. This means that if the correlation algorithm used to decode a sequence treats the first element as a special case, it is possible to compute the periodic correlation by treating the sequence as real valued only.

An example of a non-binary Legendre sequence of length 7, alphabet 3, has values '-,0,b,a,a,b,0', (corresponding to phase angles of 0=0, a=2π/3, b=4π/3), where '–' represents a zero magnitude, and the other elements assume unity magnitude.

## 3. Methods of Embedding

There are a number of ways to embed a watermark of this kind into data. For a 1D audio signal, a straightforward, but highly perceptible form of embedding is as follows. Since Legendre sequences are normally complex valued, they may be added to 1D data

via a carrier [10]. In this case, the carrier would be phase-modulated by the sequence

$$y_t = \cos(2\pi t + L_t),$$

where $L_t = 2\pi q_t/p$, $\boldsymbol{q_t}$ is the sequence and $\boldsymbol{p}$, its length.

Because the watermark is encoded entirely in the phase of the above signal, we are free to modify the amplitude according to other requirements.

In colour images, each data point *n* can be described by a vector in a 3D space. It is then possible to choose any two of the three pixel components as real and imaginary, mapping complex numbers onto this space. The angle of the pixel vector in that space can be manipulated by embedding sequences as before [11].

Alternatively, if a colour image is mapped to a colour space where one of the components represents some sort of angle (eg. HSV or HLS [4], where the Hue component is often represented as a position in a rainbow colour wheel), then that angle can be directly modified in proportion to the phase angles of the sequence.

Again, since the encoding is entirely in the phase of the signal, amplitude modulation of the watermark component can be used to hide the watermark (in this case, visual edge masking).

Clearly, from section 2, it is unimportant, in terms of recoverability, whether the sequence is applied in the pixel or transform domain. The factors determining where to apply the sequence have more to do with such aspects as visibility and resistance to rotation or scaling.

# 4. Multi-dimensional Arrays

A 2D Legendre array can be constructed by multiplying row and column sequences directly to form a product array [12].

For non-square arrays, given that our sequence construction is separable, $\boldsymbol{a_{mn}}$ is given by

$$a_{mn} = 0 \quad \text{for any m or n} = 0$$

$$a_{mn} = \exp\left(2\pi i\left(\frac{r\,\mathrm{ind}_g(n)}{p-1} + \frac{s\,\mathrm{ind}_h(m)}{q-1}\right)\right), \tag{7}$$

where *p, q* are the row and column lengths (prime), *g, h* are primitive roots modulo *p, q* respectively, *ind* is a function returning the exponent of *g, h* required to produce *m* or *n*, and *r, s* are any integers less than *p, q*.

A 1D Legendre sequence can also be mapped into 2D by a number of other schemes [12].

We define an *embedding traversal direction*, as the sequence in which adjacent elements of the watermark are applied to the image. Possible embedding traversal directions include:

- individual row- or column-wise scans (a new sequence for each row/column),
- row- or column-wise raster scans (a single sequence for the whole image),
- either of the above over sub-portions of an image and these then tiled over the whole image,
- the JPEG-like 8x8 diagonal folding, then tiling
- non-adjacent traversals.

| 0 | 0 | 0 | 0 | 0 |
|---|---|---|---|---|
| 0 | +1 | -1 | -1 | +1 |
| 0 | -1 | +1 | +1 | -1 |
| 0 | -1 | +1 | +1 | -1 |
| 0 | +1 | -1 | -1 | +1 |

**(a) Binary Legendre Array**

| +5 | +5 | -20 | +5 | +5 |
|---|---|---|---|---|
| +5 | +5 | -20 | +5 | +5 |
| -20 | -20 | 80 | -20 | -20 |
| +5 | +5 | -20 | +5 | +5 |
| +5 | +5 | -20 | +5 | +5 |

**(d) Cross-correlation of the Legendre Array and its Fourier Transform**

| +1 | +1 | -4 | +1 | +1 |
|---|---|---|---|---|
| +1 | +1 | -4 | +1 | +1 |
| -4 | -4 | 16 | -4 | -4 |
| +1 | +1 | -4 | +1 | +1 |
| +1 | +1 | -4 | +1 | +1 |

**(b) Auto-Correlation**

| 0 | 0 | 0 | 0 | 0 |
|---|---|---|---|---|
| 0 | +5 | -5 | -5 | +5 |
| 0 | -5 | +5 | +5 | -5 |
| 0 | -5 | +5 | +5 | -5 |
| 0 | +5 | -5 | -5 | +5 |

**(c) DFT of Legendre Array**

**Table 1**: **A 5x5 2D Legendre Array (a), its auto-correlation (b) and Fourier transform (c) , and the cross-correlation (d) of the array (a) and its Transform (c), showing the factor 5 between (b) and (d).**

In all these cases, data for the Fourier Transform and correlation must be accessed in the same manner as the watermark sequence or array over the image.

For simplicity, the embedding traversal direction used in section 7 is a simple, 1D single-row-per-sequence scan.

If the product array traversal was used as introduced at the start of this section, the Fourier Transform and correlator become the standard 2D versions.

The above discussion presents a key-less detection scheme based on Fourier transform invariance. At the time of writing, it is not known whether there exist sequences or signals which are invariant to other transforms frequently used in signal or image processing, such as the Discrete Cosine Transform (DCT).

# 5. Information Storage

The Legendre product array is capable of information storage in its cyclic shift from a reference template array. For a $\boldsymbol{p \times p}$ array, there are $\boldsymbol{p^2}$ such shifts. Therefore, a word of size $\boldsymbol{Int(2\log_2 p)}$ can be accommodated. Additional information may be embedded in the choice of array e.g. the choice of the multiplier $\boldsymbol{r}$ for the row and

column sequences. This can add another word of storage equivalent to the first.

The cross-correlation between two ***p x p*** Legendre arrays also factors into the product of two cross-correlations of the component Legendre sequences:

$$\begin{aligned}\theta_{k,l}^{u,v} &= \sum_{i=0}^{p-2}\sum_{j=0}^{q-2} c_{i,j}^{u^*} c_{i+k,j+l}^{v} \\ &= \sum_{i=0}^{p-2}\sum_{j=0}^{q-2} a_i^{u^*} b_j^{u^*} a_{i+k}^{v} b_{j+l}^{v} \\ &= \sum_{i=0}^{p-2} a_i^{u^*} a_{i+k}^{v} \sum_{j=0}^{q-2} b_j^{u^*} b_{j+l}^{v} \\ &= \theta_k^{uv}\theta_l^{uv}.\end{aligned} \tag{8}$$

The cross-correlation $\theta_k$ between two generalised Legendre sequences of different alphabets is ***0*** for ***k=0,*** and is a complex quantity of magnitude $\sqrt{p}$ otherwise. Therefore, the cross-correlation between two different arrays is ***0*** (for ***k*** or ***l = 0,*** i.e. on either axis) or a complex number of magnitude ***p*** off axis. The auto-correlation peak is $(p-1)^2$. Therefore, the peak/false-peak ratio approaches ***p*** for large ***p*** on a null image. The above raises the possibility of embedding ***n*** different arrays in the same image [12]. On average, the peak/false-peak ratio would degrade to $p/\sqrt{n}$ for a null image. However, by a careful mapping, tens or even hundreds of words may be capable of being stored in ***512x512*** images. Some overhead could be apportioned to error correction/detection. It should be noted that the addition of multiple arrays results in watermarks with more random "noise-like" appearance, which are therefore less perceptible.

In practice, watermark visibility will constrain the number of watermarks that can be applied well before any other capacity constraints. The number of simultaneous watermarks is thus necessarily image dependent.

# 6. Key-less Signature Detection Using Higher Order Correlation

An alternative scheme for key-less signature detection relies on higher order correlation. In particular, triple correlations have been used in the detection of direct sequence spread spectrum signals in a code division multiple access scenario [1]. The 1D triple correlation $\theta(\tau_1, \tau_2)$ is defined as:

$$\theta_{\tau_1,\tau_2} = \sum_{i=0}^{l-1} a_i a_{i+\tau_1} a_{i+\tau_2}. \tag{9}$$

The m-sequence is a member of a class of binary sequences possessing the shift-and-add property. In the case of *binary* m-sequences, the isomorphism between (0, 1) and the roots of unity (-1, 1) results in the product $(a^*_i\, a_{i+\tau})$ being equivalent to $(a_{i+\tau'})$. Therefore, the triple correlation exhibits peaks of height ***h*** (the sequence length) whenever $\tau_2 = \tau'$. Otherwise, the triple correlation results in the off-peak auto-correlation value of –1. This is independent of the m-sequence involved, but relies on the correlation being performed over the exact sequence length. This restriction is not severe, since partial correlation asymptotes to this result as the correlation length tends to the correct value. Since binary m-sequences are only available in lengths of $2^n-1$, the search for an unknown sequence need only include these lengths. The presence of other embedded m-sequences results in a higher background, because of cross-correlation effects. This results in distinct peaks attributable to each sequence and some cross-correlation peaks. The latter can be constrained by the choice of sequences to be less than *the* square root of the length. Cross-correlation between binary m-sequences has been theoretically analysed [6,7].

The extension of the above theory to applications in two or more dimensions is straightforward. M-sequences of composite length can be folded into m-arrays. The original m-sequence appears along the diagonal of such an array. Consequently, the array retains the 'shift and add' property of the original sequence.

The triple correlation method is more computationally intensive than the scheme proposed here and is also more difficult to interpret. It will not detect Legendre sequences, just as M-sequences cannot be detected using the Fourier invariance property. As with the Legendre invariance described in section 4, the correlator traversal direction must match the embedding traversal direction.

# 7. Results

In this section, we present some sample results to demonstrate how the proposed method works.

A 127 element 1D binary Legendre sequence with values [$-m$,$+m$] was added to each row of an image ($m$ is a watermark 'strength' parameter whose value can be image dependent or locally adaptive).

Recognising that any image traversal can be used, row-wise traversal and processing was used here for simplicity. The results apply in general to any image traversal direction, as long as the spatial pattern of

traversal is known, as described in section 4.

In our case, we used m=8 for a 256 level image for demonstration purposes. (A value of m=1 will elicit a peak for this sequence length, but convolution with a 1D Laplacian is needed to extract this peak. For longer sequences, this Laplacian convolution would not be required).

Figure 1 shows the original image. Since the embedded sequence is balanced (mean = 0), and the image is unipolar (all numbers positive), a row mean is subtracted from each row to avoid a background offset in the cross-correlation.

A 3D representation is shown of the normalised cross-correlation magnitude between the watermarked image with the watermark alone (Figure 2); and between the watermarked image with its Fourier transform, (Figure 3). These are all performed separately on each row.

Figure 2 shows the characteristic peak at column zero in the cross-correlation of watermarked image and watermark. This procedure required knowledge of the watermark and thus the encryption key.

Figure 3 shows the normalised cross-correlation magnitude between image and its Fourier transform. This does *not* require knowledge of the watermark or key.

Compare Figure 3 with Figure 4, which shows the normalised cross-correlation magnitude of the unwatermarked image with its Fourier Transform.

The background of correlation values can approach the watermark peak in places. This is one factor limiting the strength, *m*, of the watermark to be applied to the image.

The power spectral density of each row can be used to drive an adaptive mechanism determining a different *m* for each row. Hartung [5] claims that, to maximise resistance against attacks, a spread-spectrum watermark's PSD should be a scaled version of the PSD of the image.

Since our watermark is encoded entirely in the phase of the image row, its amplitude could be adjusted according to the maximum PSD value for that row (figure 5) – crudely approximating (by row) Hartung's assertion. Figure 6 shows the image with a binary watermark added whose row *m*-values depend on the row PSD.

## 8. Acknowledgments

The authors wish to thank Dr. T. E. Hall for his invaluable input into the understanding of generalised Legendre sequences and K. F. Wilson for her helpful suggestion to utilise the Fourier invariance property.

## 9. References

1. E. R. Adams, M. Gouda, P. C. J. Hill, *Detection and Characterisation of DS/SS Signals Using Higher-Order Correlation*, Proc. IEEE, ISSSTA'96, Mainz, Germany, September 22-25, 1996, vol. 1, pp. 27-31.
2. J. F. Delaigle, C. De Vleeschouwer, B. Macq, *Watermarking Algorithm Based on a Human Visual Model*, Signal Processing (66) 3 (1998) pp. 319-335.
3. D. Everett, *Periodic Digital Sequences With Pseudonoise Properties*, GEC Journal, 1966, Vol. 33, No. 3, pp. 115-126.
4. J. D. Foley and A van Dam, *Fundamentals of Interactive Computer Graphics*, Addison-Wesley, 1982.
5. F. Hartung, J. K. Su, B. Girod, *Spread Spectrum Watermarking : Malicious Attacks and Counter-attacks*, Presented at Electronic Imaging 99, SPIE, Vol 3657, San Jose, USA, January 24-29, 1999.
6. F. J. Mac Williams, N. J. A. Sloane, *Pseudo-random sequences and Arrays*, Proc. IEEE, vol. 64, pp. 1715-1729, Dec 1976.
7. D. V. Sarwate, M. B. Pursley, *Cross-correlation Properties of Pseudorandom and Related Sequences*, Proc. of the IEEE vol. 68, no 5, May 1980, pp. 593-619.
8. M. R. Schroeder, *Number Theory in Science and Communications*, Ch 15, 2nd Ed.1997, Springer-Verlag.
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, pp. 666-672.
10. R. G. van Schyndel, A. Z. Tirkel, I. D. Svalbe, *Delay Recovery from a Non-linear Polynomial-Response System*, ISPACS'98, Melbourne, November 5-7, 1998, pp. 294-298
11. R. G. van Schyndel, A. Z. Tirkel, I. D. Svalbe, *A Multiplicative Colour Watermark*, Accepted in NSIP'99, Antalya, Turkey, June 20-23, 1999.
12. R. G. van Schyndel, A. Z. Tirkel, I. D. Svalbe, T. E. Hall, C. F. Osborne, *Algebraic Construction of a new class of Quasi-Orthogonal Arrays in Steganography*, Presented at Electronic Imaging 99, SPIE, Vol 3657, San Jose, USA, January 24-29, 1999.

**Figure 1**
**The original 127x127x8 bit gray image.**

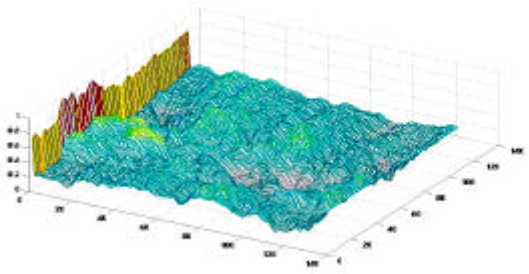

**Figure 2**
**Normalised cross-correlation magnitude of the image plus watermark with the known watermark sequence (by row). Note the peak at column zero for each row.**

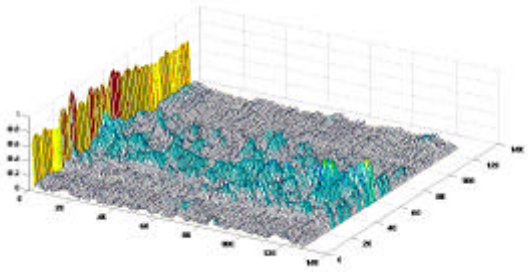

**Figure 3**
**Normalised cross-correlation magnitude of the image plus watermark with its row-wise Fast Fourier transform. These were obtained without knowledge of the key or watermark.**

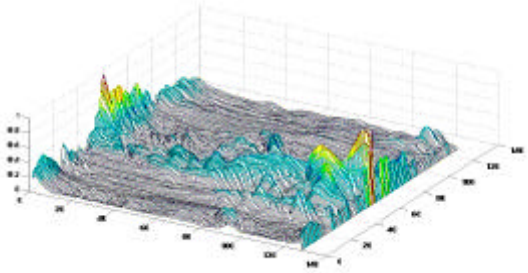

**Figure 4**
**Normalised Cross-correlation Magnitude of the unwatermarked image with its row-wise Fast Fourier Transform. Note the absence of peaks in column zero.**

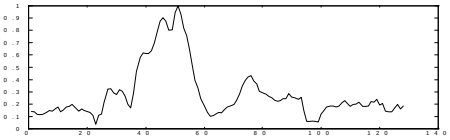

**Figure 5.**
**The normalised maximum Power Spectral Density of the image of figure 1, by row. The watermark amplitude can be scaled by the maximum value of the PSD for each row.**

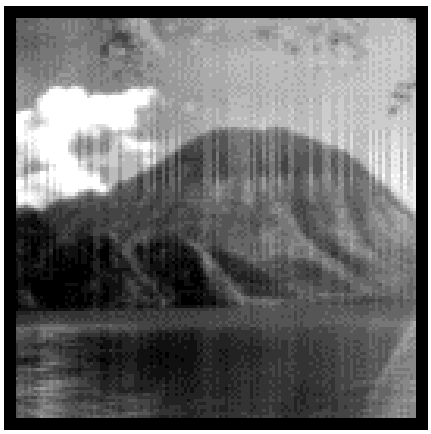

**Figure 6.**
**The image, watermarked, with row-amplitude profile as in Figure 5 (exaggerated to reveal the watermark)**