



# Spread-Spectrum Digital Watermarking Concepts and Higher Dimensional Array Constructions\*

Ron G. van Schyndel<sup>1</sup>, Andrew Z. Tirkel<sup>2</sup>,  
Imants D. Svalbe<sup>1</sup>, Thomas E. Hall<sup>3</sup>, and Charles F. Osborne<sup>1</sup>

ron.vanschyndel@sci.monash.edu.au

<sup>1</sup> Department of Physics, Monash University, Clayton 3168, Australia

Supported by an Australian Postgraduate Award scholarship.

<sup>2</sup> Scientific Technology, 8 Cecil St, East Brighton 3187, Australia

<sup>3</sup> Department of Mathematics, Monash University, Clayton 3168, Australia

## Abstract

The use of digital multimedia for profit is pressing for the development of a robust and indelible method of protecting the intellectual property rights of the content creators.

The fields of digital watermarking and steganography have exploded over the last few years as a potentially viable technique as addressing this need.

For the most part the common denominator of many current watermarking techniques has been the use of pseudo-noise (PN) sequences in various forms to embed (or scramble) the message.

This lecture is split into two halves. The first half is an overview of the current state of digital watermarking. We include a description of the steganographic channel model, as well as a mechanism for mapping the essentially one dimensional streaming of the conventional communication model to higher dimensions.

The second part of the lecture describes the construction of arrays suitable for embedding as watermarks. We will also explain the contrary requirements of a good watermark and contrast them to the features of spread-spectrum communications.

## 1 Introduction

The use of digital multimedia for profit is pressing for the development of a robust and indelible method of protecting the intellectual property rights of the content creators.

The fields of digital watermarking and steganography have exploded over the last few years as a potentially viable technique as addressing this need.

The use of the spread spectrum technique for digital watermarking first appeared in a patent in 1989[1] where the least significant bit of samples of an audio stream are periodically replaced with a random-looking signature, but very little followed until 1993[2,3]. Since then, increasingly sophisticated algorithms have been developed for embedding messages within digital data in multiple dimensions for audio, image, and video. For the most part the common denominator of these methods has been the use of pseudo-noise (PN) sequences in various forms to embed (or scramble) the message.

---

\* Short title: Array Constructions in Steganography.

This lecture is split into two halves. The first half is an overview of the current state of digital watermarking. We include a description of the steganographic channel model, as well as a mechanism for mapping the essentially one dimensional streaming of the conventional communication model to higher dimensions.

The second part of the lecture describes the construction of arrays suitable for embedding as watermarks. We will also explain the contrary requirements of a good watermark and contrast them to the features of spread-spectrum communications.

## 2 Steganography and Digital Watermarking

Digital steganography can be defined as the subtle perturbation of elements of digital multimedia data. In most cases, the media is composed of digitised samples from the real world. This means there is a base level of quantisation noise in the medium which is one of the places a message can hide.

For information hiding, the main criterion is that the information not be perceptually detectable, but still recoverable by authorised people.

An ideal watermark, on the other hand, will be embedded such that, in addition to undetectability as in information hiding, it is also indelible. So a watermarked image, for example, should be indistinguishable from an unwatermarked version of the same image, but no matter what is done to the image - provided it can still be passed off as an original - it should be impossible to remove the watermark. Such a watermark is said to be robust.

The key concept to watermarking is that a structured probe signal has been embedded in the data that is recoverable even after data manipulation.

This is where the spread spectrum techniques come into play. Its features of redundant signalling, local adaptability, and its resistance to many types of distortion, leads it to be the preferred vehicle for many commercial watermarking technologies in use today.

For brevity, in the remainder of this lecture, the terms watermarking and information hiding will be used interchangeably. The ultimate application will usually make it obvious which one of these is intended.

### 2.1 Forms of Watermarking

As well as the forms usually associated with digital multimedia - audio, static images and video - there are many other areas where watermarking has been used or suggested.

For formatted text, for example, the precise to-the-dot positioning of the letters on a page can be perturbed by a watermark [20].

A more unusual suggestion has been the embedding of an encoded message within the surface of engine castings. One can imagine how difficult it is to file down an engine number if it is present everywhere on the engine!

Information can also be hidden within procedures and protocols. A fairly old covert signalling method is to effectively use the positive- and negative-acknowledge signal in a network protocol as a Morse code.

Since there are multiple ways of implementing equivalent gates on FPGA's, the ultimate choice of gates may itself be a code. Even playing SOS on certain device-enable lines in a PC can modulate the RF emissions of the PC which is detectable by an ordinary radio.

An authentication watermark can be created by making a pair of identical images, then perturbing the position of some pixels in each image differently such that when the two are viewed stereoscopically, a message appears to 'float' out of the image.

One of these images is released to the public, the other is kept privately for authentication purposes. This form is easily defeated however, as will become clear later in the lecture.

## 2.2 Some Terminology

As stated previously, an ideal **robust** watermark is one that resists all distortions and other attempts to remove it.

A **fragile** watermark, on the other hand, can act as a check-sum, so that any change will render it unreadable. This would apply to authentication.

Many **semi-fragile** image watermarks are still recoverable after change, but will reveal the regions of an image that were changed. This might be useful, for example, in newsreel photographs - indeed, digital cameras now exist which embed such a watermark automatically.

Many of the watermarking algorithms initially published required that the original data be available to the detector. It would typically be subtracted from the watermarked data to reveal the watermark itself. These are referred to as **private** watermarks. Watermark detectors that do not need the original have been called **blind** detectors.

When it comes to public or private watermarks, the definitions can get a bit blurry, since the terms public and private watermark detectors have also been used to refer to models analogous to public key encryption systems. In this situation, a publicly accessible watermark detector uses a method quite different to a private detector, so that an attacker cannot infer the watermark structure by, for example, disassembling the public detector. Making such a watermark undetectable using the public detector, does not necessarily make it undetectable to the private detector, which only the originator of the watermark possesses.

An **invertible** watermark is one where the embedding process can be reversed to yield the original data exactly. For the same reason as with public watermarks – security - this is not a desirable feature, and most recent watermarks are not invertible.

Further watermarking terminology can be found in [11].

## 2.3 The Generic Watermarking Channel

The generic watermarking or steganographic channel model resembles the traditional communications channel model in most respects. The principal difference is the visibility criterion. This can be roughly considered analogous to a power limitation requirement, but the human visual system is a much more 'fussy animal' when it comes to watermark detection.

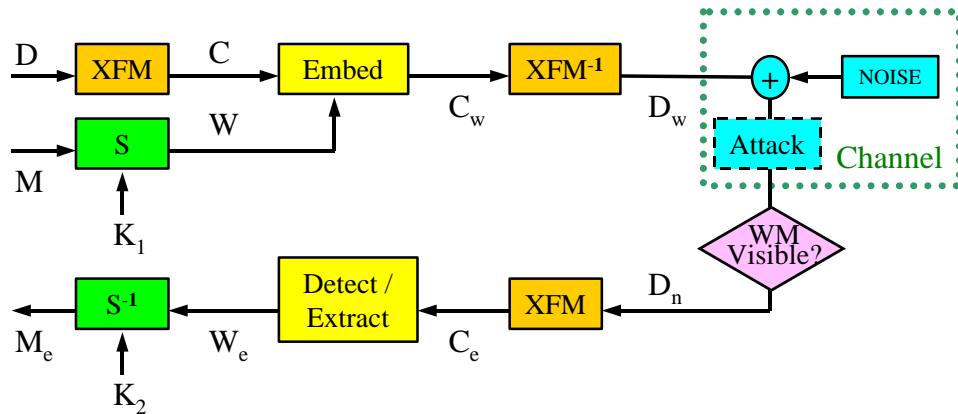


Figure 1: The Generic Watermarking Channel Model

In the above scenario, the multimedia data,  $D$  which is often referred to as the host data, is transformed into some other invertible domain. Typically this is the frequency domain, so the transform is a Fourier or discrete cosine transform.

The message  $M$  is also transformed or encoded. In the case of spread-spectrum signalling, the message is encoded by a spreading function. After the embedding, explored further in figures 2 and 3, the inverse transform is applied to produce the watermarked data,  $D_w$ .

The channel noise was modelled in early versions of watermarking as additive white Gaussian, but more recent efforts use a more general non-linear distortion or attack noise model. This noise modelling is one of the active areas of research in watermarking, but its mitigation is very dependent on the features of a particular watermarking algorithm and individual image statistics, and is beyond the scope of this paper. See [4-6] for more details on attack strategies.

Like the traditional channel model, the detection or extraction process typically involves matched filtering or a correlation.

When the spreading and de-spreading functions use different keys, the watermark is referred to as having a non-symmetric key.

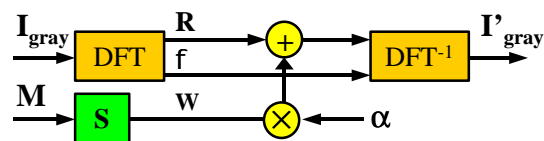


Figure 2: Linear embedding in a monochrome image

In figure 2, the multimedia data is a monochrome image, which is transformed to the frequency domain. The magnitude of the frequency components are perturbed by the watermark, scaled by a constant, alpha, which might be determined manually, based on visibility.

This form has been referred to as first generation watermarking [7], because the watermark is not adjusted to the image. In fact the detector would simply treat the image as un-correlated noise. These watermarks are relatively easy for an attacker to remove.

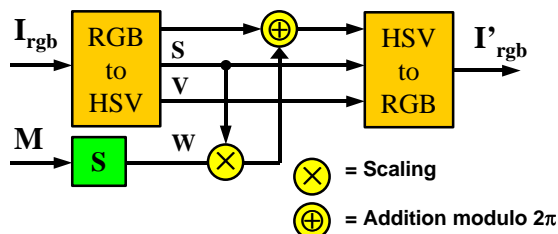


Figure 3: Non-Linear embedding in a colour image

In figure 3, a colour image is transformed to the Hue-Saturation-Value colour model. In this model, the intrinsic colour of the image pixels, the hue, are related to angles on a 'colour wheel', with red at zero degrees, green at 120 degrees and blue at 240 degrees.

Since hue is an angle, an additive perturbation is equivalent to a multiplicative embedding.

In addition, the image saturation scales the watermark intensity, so the watermark is dependent on image characteristics. This is an example of a second generation watermarking process [7], where the watermark is adjusted by image characteristics.

In this particular case, the value or brightness could just as easily have been used to scale the watermark. Both relate to the visibility of the watermark.

Because we are, in effect modulating the hue angle, we could employ a phase or frequency shift keying modulation here [8-10], but in this lecture we will concentrate on spread spectrum modulation.

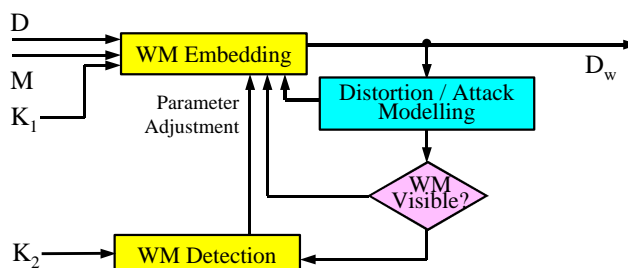


Figure 4: Third-generation Watermark Embedding [7] with Channel Equalisation

More recent watermarking algorithms have involved a degree of pre-distortion. In the model shown in figure 4, the watermark detector is used to adjust the embedding parameters in order to maximise the detection of the watermark for this particular host data.

This means that for different host data, the parameters may be quite different, even if the embedded watermark was identical. The host data, watermark and detector are all available to the embedder, so an optimal equalisation process is possible.

This is the cutting edge of research in watermarking at the moment and is an example of third generation watermarking, where optimal detection is considered as well as visibility.

## 2.4 The Central Objectives of Digital Watermarking

In general, an optimal watermark can be found by maximising one of three parameters: visibility, capacity and robustness - usually at the expense of the other two.

One suggestion [21] for a visibility measure is a weighted peak signal-to-noise-ratio, wPSNR:

$$wPSNR = 10 \log \left( \frac{D}{\|V(D_w - D)\|^2} \right) \text{ where } V = \frac{D}{(D + S_n^2)},$$

V is the 'Noise Visibility Function', and the sensitivity of the measure depends on the local variance. But this is one of many such measures suggested over the years [12].

## 2.5 Observations

Here are some observations that are pretty much standard requirements of a digital watermark today.

A watermark is generally imperceptible, but visible digital watermarks do exist - a cable TV channel logo probably being the most often seen.

If a watermark is invertible, then an attacker can remove it. In most cases this is undesirable and so watermark invertability is most often prevented by involving a quantisation in the embedding process.

In order to ensure that the watermark cannot be removed, we place the watermark using the same frequency components as the image itself. That way, trying to remove the watermark causes maximal damage to the image. This damage is measured as a distortion penalty paid to remove the watermark [13].

If a watermark is not embedded in a transform domain, the biggest danger from attack lies in the desynchronisation of the spread spectrum arrays used to encode the watermark.

This could be done by something as simple as a slight image rotation.

One way to fight this kind of attack is to embed in a transform domain that is invariant to some of these image transformations. O'Ruanaidh [19], for example, created a watermark procedure which is invariant to image rotation, scale and translation.

The standard way is to explicitly resynchronise the image, and this is where the use of 2D arrays can assist.

The watermarking channel differs from the communication channel in a number of important respects.

Probably the most limiting is the usually narrow bandwidth within which the watermark must operate.. Images have only a limited size, and this is often much smaller than the sort of bandwidth encountered in communications. Audio and video watermarking channel have more samples to perturb, so the problem is not so great there.

The embedded watermark strength is always constrained subject to some visibility criterion that may not be straight-forward to model, and along with storage quantisation, this leads to another significant source of detection uncertainty.

Noise modelling is a currently active area for third generation watermarking for the same reason.

And finally, the multi-dimensionality and a-causality of the watermarking channel allow some types of distortions to occur which are not often encountered in communications [6].

<b>Distortions</b>	<b>Attacks</b>
<b>1D Audio:</b> resampling, reordering, rescaling, truncation, (non)linear filtering, DA/AD, requantisation, apply noise, addition of echos.	<b>Collusion:</b> Estimate watermark using many copies of the same image, each differently watermarked, frame averaging
<b>2D Image:</b> non-uniform geometric warping, rotation, intensity / histogram modification, mosaicing.	<b>Confusion:</b> Make it impossible to detect watermark (loss of synchronisation)
<b>3D Video:</b> Frame: reordering, deletion, duplication, average, interpolation, compression, jitter.	<b>Ownership Deadlock:</b> Super-impose counterfeit watermark with equal detection probability (which WM was first ?)
<b>Lossy Compression:</b> Reducing redundancy using perceptual rules may distort the watermark.	

Figure 5: Distortions and some attack strategies

Figure 5 shows a reasonably comprehensive list of distortions that any good watermark algorithm should be able to resist to some degree.

Unfortunately, in addition to these, the watermark algorithm must also be resistant to deliberate attack - only some of which are shown on the right.

It is competing against these odds that make the development of the ultimate watermark so interesting.

### 3 2D Array Constructions

Two-dimensional array constructions can and have also been used in more conventional signalling.

We will essentially look at 2 commonly used 2-dimensional constructions from 1-dimensional sequences - product arrays and array folding, and then we will introduce a third construction method.

The sequence and array parameters can be formed from the keys  $K_1$  and  $K_2$  in figure 1, which can then be used to encode the message.

### 3.1 Eligible 1D Seed Sequences

Most of the sequences listed in figure 6 originate from CDMA communications where inter-symbol interference (or the minimisation of cross-correlation between different members of a set of sequences) plays a significant role.

For digital watermarking, there are applications where good cross-correlation is specifically not wanted and the ideal behaviour should be pathological.

**Binary:** M-sequence, GMW, Gold, Kasami, No, Legendre, Twin-Primes, Hall, and Kerdock and other codes.

**Complex:** M-sequence, Legendre, DSP, FZC and other Chirp Sequences, Opperman & Vucetic near-perfect periodic sequences, and CAP and other general orthogonal sequence families where the sequence alphabet and the cross-correlation between members is not controlled.

*Figure 6: 1D seed sequences*

For example, trying to embed a second authentication watermark on an already watermarked image should ideally result in obvious damage to the image - perhaps as a highly visible moire pattern.

The binary sequences is usually bipolar ( $\pm 1$ ) and while optimal for modulation in a mean-squared sense, suffer from the fact that there is always some inter-symbol interference. This is because sequences lengths are almost always odd, and so symbols don't add to zero. The correlations are thus never perfect.

The complex watermarks, on the other hand have greater message capacity, but even though the correlations can be perfect, the inter-symbol distance is reduced, so these methods are often less robust.

#### 3.1.1 Cyclic All-pass Sequence

From the list of complex sequences in the previous slide, we will look at two varieties in a little more depth.

The chirp-like cyclic all-pass sequence [14] is an easy-to-generate instance of a general class of orthonormal sequences that possess the ideal auto-correlation property needed for signal extraction.

- **Cyclic All-Pass (CAP) Sequence (Ramkumar)**

1. Generate  $S_p = \text{random} \in \{0..1\}$ , length  $p$ , seed  $K_1$
2. Form sequence:

$$T = \{0, S_1, S_2, \dots, S_p, 0, -S_p, -S_{p-1}, \dots, -S_1\}, p = \text{even integer}$$

3. Take the Fourier Transform:  $H_k = \frac{1}{p} \sum_{j=0}^{p-1} e^{2\pi i T_k} e^{2\pi i j/p}$

- $|R_{HH}| = (p,0)$ ,  $R_{GH} = \text{unconstrained (not important for WM)}$ ,  $G \neq H$
- Large number of sequences possible, determined by a random seed,  $K_1$

Figure 7: Generating a Cyclic All-pass Sequence

Like most sequences in this class, the cross-correlation between different sequences is unconstrained, so it is difficult to model the probability of false detection. Note, however that the correlational properties inherent in the higher dimensional constructions can be used to overcome this limitation.

### 3.1.2 Distinct-Sums Property Sequences

Hall and Tirkel introduced a new chirp-like sequence that also has ideal auto- and cross-correlation properties.

For a complex sequence of length  $p$ ,  $p$  being a prime number, there is a set of  $p-1$  possible sequences in the family. Each of these sequences has a perfect auto-correlation and ideal cross-correlation with other members in the set.

Indeed, a Kronecker product of this sequence with other chirp-like sequences also yields very good correlation properties. A combination of these effectively allows a very large family of sequences to be developed, so the message capacity has the potential be large.

- **Distinct-Sums-Property (DSP) Sequence (Hall/Tirkel)**

1. Generate a roots of unity ramp:

$$S(k) = \exp(2\pi i k/p), k = 0, \dots, p-1, p = \text{prime}$$

2. Shuffle  $S$  to form the sequence  $T_m$  using parameter  $m \in \{1, 2, \dots, p-1\}$ :

$$T_m(k) = S(n_k), n_k = (n_{k-1} + mk) \bmod p, n_0 = 0, k = 1 \dots p-1$$

- $|R_{TT}| = (p,0)$ ,  $|R_{TU}| = (\sqrt{p}, \sqrt{p})$ ,  $U \neq T$ ,  $U, T \in \text{Same family of sequences for length } p$
- $p-1$  different sequences possible. Because of ramp, all angles equally represented.
- Kronecker product of DSP/CAP/FZC seq, length  $p$ , with another seq, length  $q$ , also gives good auto-correlation but NOT good cross-correlation with a different combination, but the same length,  $pq$ , ---> **ISI not good, sufficient for watermarking?**
  - $|R_{TT}|$ : (peak:  $pq$ , off-peak: 0 for all but  $q$  values on both sides of peak
  - **Allows synchronisation on multiple scales.**

Figure 8: Generating a Distinct-Sums Property Sequence

For direct-sequence insertion however, these product forms allow multiple scales to be examined at once. For watermarking, multi-scale embedding is better achieved by applying the watermark in the Wavelet transform domain.

As with the cyclic all-pass sequences, modelling the probability of false detection can be difficult, and is being studied presently.

## 3.2 2D Constructions

### 3.2.1 Product Arrays and Array Folding

The simplest two-dimensional construction is a product array [15]. This is just a vector product of a row and column sequence vector to produce a P by Q matrix.

Sequence folding [15] has been used in coded aperture imaging and communications for a long time. More recently it has been used in image watermarking almost from the beginning [16] as a means of utilising the properties of a 1-dimensional M-sequence over local image blocks.

### 3.2.2 Distinct-Sums Arrays

This new construction method, related to the DSP sequence generation outlined before, uses the first principles of difference-sets to obtain the ideal correlation properties as an intrinsic part of the construction method, instead of only relying on the properties of the component sequence.

A sequence  $S_p = \{S_1, S_2, \dots, S_p\}$ ,  $p = \text{prime}$ , has the distinct sum property if:

$S_1+S_2, S_2+S_3, \dots, S_{p-1}+S_p, S_p+S_1$  are all distinct, and also

$S_1+S_2+S_3, \dots, S_{p-1}+S_p+S_1, S_p+S_1+S_2$ , and so on for  $k = 4 \dots p-2$  consecutive sums

To make an array, the seed sequence is placed in each row, phase shifted progressively by a value  $m \times (\text{row number}-1)$  relative to the previous row, where  $m=1..p-1$ . The relative shift sequence then possesses the DSP property.

**Example:** For the 5-element sequence below relative phase offsets are:  $m \times (0,1,2,3)$ , for each of  $m = 1..4$

Readily extendable to higher dimensions

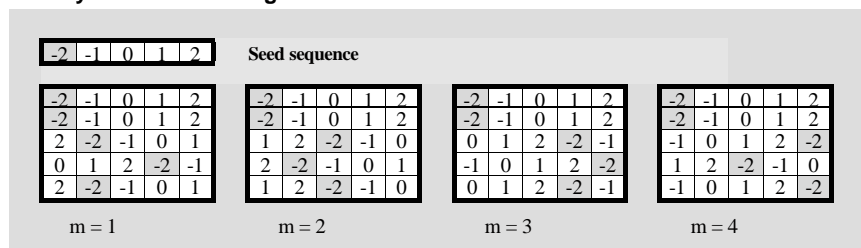


Figure 9: Generating a Distinct-Sums Array

One can thus use any random sequence in this construction method and obtain an ideal correlation in the direction in which the construction is applied, which in this case is vertical. The only requirement is that the sequence is balanced (that is, it sums to zero) and be of prime length.

In practise however, the noise tolerance of this construction is usually insufficient in itself, and the performance is dramatically improved if the constituent sequence also has ideal or near-ideal correlation property.

The particular benefit of this method is the availability of a free parameter 'm', which can be used for message embedding.

The cross-correlation of DSA's with different 'm' values is also near perfect [17].

The DSA construction also possesses the weak window property which can be employed in circumstances where automatic watermark detection may not work - for example, where parts of an image are destroyed and you must use the remaining part to establish the watermark presence. In addition, distinct sum arrays have a large linear span and, combining this method with array folding presents a significant cryptographic security.

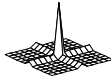
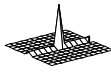
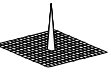
Table 1: Summary of 2D Construction Features for Image of Dimensions $p \times q$					
Response Shape	Sequence	Peak	Row of Peak	Column of Peak	Background
<b>Product Arrays</b>					
	Legendre	$(p-1)(q-1)$	$-(p-1)$	$-(q-1)$	1
	M-Sequence	$(p-1)(q-1)$	$-(p-1)$	$-(q-1)$	1
	Frank-Zadoff-Chu	$pq$	0	0	0
	Distinct Sums Array	$pq$	0	0	0
	Cyclic All-Pass Random	$pq$	0	0	0
	Random	$pq$	- (a)	- (a)	- (a)
<b>Distinct Sum Arrays</b>					
	Legendre	$p(q-1)$	$-p$	0	0
	M-Sequence	$pq$	$-(p-1)$	-1	-1
	Frank-Zadoff-Chu	$pq$	0	$p$ , iff $p = q$	$p$ , iff $p = q$
	Distinct Sums Array	$pq$	0	$p$ , iff $p = q$	$p$ , iff $p = q$
	Cyclic All-Pass Random	$pq$	0	$p$ , iff $p = q$	$p$ , iff $p = q$
	Random	$pq$	$p-1$	- (a)	- (a)
<b>Folded Arrays (Seq length = Image Area = <math>n</math>)</b>					
	Legendre	$pq$	$\sqrt{pq}$ (b)	$\sqrt{pq}$ (b)	$\sqrt{pq}$ (b)
	M-Sequence	$pq$	0	0	0
	Frank-Zadoff-Chu	$pq$	0	0	0
	Distinct Sums Array	$< pq$	0	$< 2\sqrt{n'}$ (b)	$< 2\sqrt{n'}$ (b)
	Cyclic All-Pass Random	$pq$	0	- (a)	- (a)
	Random	$pq$	- (a)	- (a)	- (a)
(a) Results are random (normally distributed with mean = $\sqrt{pq}$ ) (b) Approximate, since folding needs composite length, and these sequences can only have prime lengths. Sequence was truncated to $n' = pq < n$ such that $p-q$ is minimised and $p, q$ are co-prime.					

Table 1 presents a summary of the useful combination of some of the more popular sequences constructed as arrays. Note how the chirp sequences all respond in a similar manner to the constructions. Also note that the Legendre sequence has a perfect response to the DSA constructions

### 3.2.3 Results

In figure 10, 4 binary bipolar watermarks were added together to produce the watermark shown. This watermark has values of -3, -1, 1 and 3

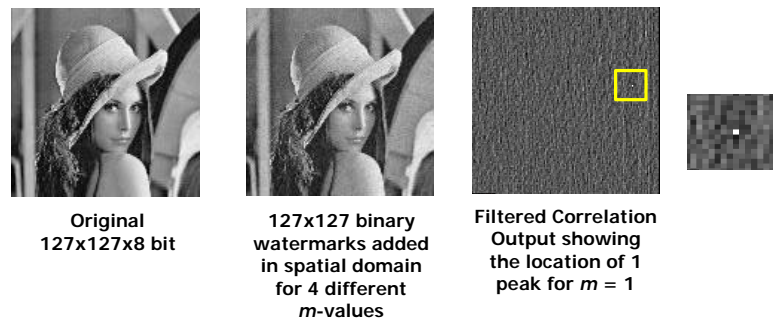


Figure 10: 'Lena' with 4 DSA watermarks added with parameter  $m = \{1,2,3,4\}$

These 4 watermarks are then added directly to the image with clipping where required. To improve recovery, we perform a local 3 by 3 Laplacian operation to the output of the watermark correlation. The peak location can be used to encode a message.

A 127 by 127 image was chosen as the smallest practical limit for image capacity. The 16,129 pixels that make up this image can thus store 7 bits by 7 bits by 2 bits, or 16 bits of information for this very simple watermark implementation. The storage capacity quadruples for every doubling of image side length.

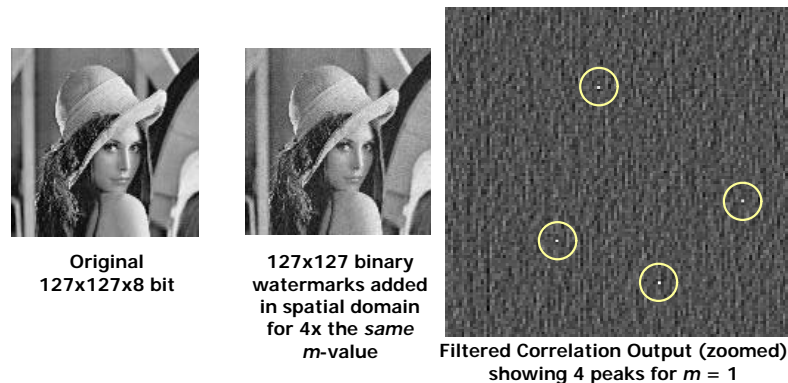


Figure 11: 'Lena' with 4 DSA watermarks added with parameter  $m = 1$ , but different phase shifts

In this case, we generated another sum of 4 watermarks, but these had the same 'm' value, so a cross-correlation reveals them all. The peak locations can now be used as a registration mask.

In these images, we concentrated on showing the effects of using the 2D masks. A commercial grade watermark would include a number of measures to improve robustness, but these are too involved to show in these lectures. The references included discuss some of these measures more fully.

## 4 Conclusion

After a brief background on digital watermarking, we looked at the watermarking channel model in terms of similarities and differences with the communication channel model and showed that the perceptibility aspect is the major difference.

We looked at how higher dimensional arrays can be constructed from 1D sequences, while maintaining their correlational properties, and introduced the distinct-sums property sequences and arrays, as well as comparing some of these constructions.

## References

- [1] L. F. Turner (1989), *Digital Data Security System*, Patent IPN WO 89/08915
- [2] A. Z. Tirkel, G. A. Rankin, R. M. van Schyndel, W. J. Ho, N. R. A. Mee, C. F. Osborne (1993), *Electronic Water Mark*, DICTA-93, Macquarie University, Sydney, December 1993, pp.666-672.
- [3] R. G. van Schyndel, A. Z. Tirkel, C. F. Osborne (1994). *A Digital Watermark*, First IEEE International Conference Image Processing, Houston TX, November 15-17, 1994, vol II, p.86-90.
- [4] F. A. P. Petitcolas, R. J. Anderson, M. G. Kuhn, *Attacks on Copyright Marking Systems*, 2<sup>nd</sup> Workshop in Information Hiding, Portland, OR, 15-17 April, 1998, pp 218-238.

- [5] F. Hartung, J. K. Su, B. Girod (1999), *Spread Spectrum Watermarking: Malicious Attacks and Counter-Attacks*, SPIE Security and Watermarking of Multimedia Contents, P. W. Wong & E. Delp (Eds), Vol 3657, 25-27 January, 1999, pp 147-158.
- [6] J. K. Su, F. Hartung, B. Girod (1999), *SA Channel Model for a Watermark Attack*, SPIE Security and Watermarking of Multimedia Contents, Vol 3657, 25-27 January, 1999, pp 159-170.
- [7] I. J. Cox, M. L. Miller, A. L. McKellips (1999), *Watermarking as Communications with Side Information*, Proceedings of the IEEE, Vol 87(7), 1999, pp 1127-1141.
- [8] R. G. Mobasserri (1999), *Exploring CDMA for Watermarking of Digital Video*, SPIE Security and Watermarking of Multimedia Contents, P. W. Wong & E. Delp (Eds), Vol 3657, 25-27 January, 1999, pp 96-102.
- [9] J. R. Smith and B. O. Comisky, *Modulation and Information Hiding in Images*, 1<sup>st</sup> Workshop in Information Hiding, Cambridge, England, Springer-Verlag, May 1996
- [10] J. Hernandez, F. Perez-Gonzalez, J. Rodriguez, G. Nieto (1998), *Performance Analysis of a 2D Multipulse Amplitude Modulation Scheme for Data Hiding and Watermarking of Still Images*, IEEE Journal on Selected Areas of Communication, Vol 16, No 4, May, 1998, pp 510-524.
- [11] B. Pfitzman (1996), *Information Hiding Terminology*, 1<sup>st</sup> Workshop in Information Hiding, Cambridge, England, Springer-Verlag, May 1996, pp 347-350.
- [12] C. J. van den Branden-Lambrecht, J. E. Farrell (1996), *Perceptual Quality Metric for Digitally Coded Colour Images*, Proceedings of the European Signal Processing Conference, Trieste, Italy, September 10-13, 1996.
- [13] J. K. Su and B. Girod, *Power-Spectrum Condition for Energy-Efficient Watermarking*, Proc. IEEE International Conference on Image Processing '99 (ICIP-99), Kobe, Japan, Oct. 1999.
- [14] M. Ramkumar (1999), *Data Hiding in Multimedia*, PhD Thesis, New Jersey Institute of Technology, Kearny, NJ, USA, November 1999.
- [15] F. J. MacWilliams, N. J. A. Sloane (1976), *Pseudo-Random Sequences and Arrays*, Proceedings of the IEEE, Vol 64, No.12, Dec.1976, pp. 1715-1729.
- [16] M. D. Swanson, B. Zhu, A. H. Tewfik (1998), *Multi-resolution Scene-based Video Watermarking Using Perceptual Models*, IEEE Journal on Selected Areas of Communication, Vol 16, No 4, May, 1998, pp 540-550.
- [17] A. Z. Tirkel, T. E. Hall, C. F. Osborne (1998). *A New Class of Spreading Sequences*, ISSSTA'98, Sun City, South Africa, September 1998, Vol 1, pp. 46-50.
- [18] 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*, SPIE Security and Watermarking of Multimedia Contents, P. W. Wong & E. Delp (Eds), Vol 3657, 25-27 Jan 1999, pp 354-364.
- [19] J. J. K. Ó Ruanaidh and T. Pun (1998), *Rotation, Scale and Translation Invariant Spread Spectrum Digital Image Watermarking*, IEEE Signal Processing, Vol 66(3)
- [20] S. H. Low, N. F. Maxemchuk, A. P. Lapone (1998), *Document Identification for Copyright Protection Using Centroid Detection*, IEEE Transactions on Communications, Vol 6(3), March 1998, pp372-383.
- [21] S. Voloshinovskiy, S. Pereira, T. Pun, *Watermark Attacks*, Erlangen Watermarking Workshop 1999, Slides available at <http://www.Int.de/~watermarking/speakers/pun/>