### ELECTRONIC WATER MARK

- A.Z.Tirkel(+) G.A.Rankin(\*) R.M.van Schyndel(\*) W.J.Ho(\*) N.R.A.Mee(\*)
- C.F.Osborne(\*)
- (+) Scientific Technology, 21 Walstab St, E. Brighton 3187, Australia.
- (\*) Department of Physics, Monash University, Clayton 3168, Australia.

## ABSTRACT

This paper discusses the feasibility of coding an "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 even a legend essential for image interpretation. This capability is envisaged to find application in image tagging, copyright enforcement, counterfeit protection, and controlled access to image data. Two methods of implementation are discussed. The first is based on bit plane manipulation of the LSB, which offers easy and rapid decoding commensurate with streaming type image processing. The second method utilises linear addition of the water mark to the image data, and is thus more difficult to decode, and therefore offers inherent security.

## 1 INTRODUCTION

The desirable properties of an electronic water mark are undetectability and accurate recovery. The technique chosen involves m-sequences and derived codes, because of their random appearance, and good autocorrelation properties. These codes can be employed to manipulate the LSB of the image data, without any apparent image degradation or detectability by a casual viewer. The water mark data can be encoded by the choice of m-sequences and their phases.

The first method involves the use of m-sequence derived codes embedded on the LSB of the image data. The original 8 bit gray scale image data is capable of compression to 7 bits by adaptive histogram manipulation. If this process is followed by a compensating mapping to restore the dynamic range, the resulting image is practically indistinguishable from the original. Examples of this feature will be demonstrated in the presentation. The above process enables the LSB to carry the watermark information with no errors. Hence, it is easy to decode, by comparing the bit patterns with stored counterparts and consulting a look-up table. The data is carried by the choice of sequence (or its complement) and its phasing. The number of bytes capable of storage in this manner is shown in TABLE I as a function of image size and sequence length. This is based on the fact that for a sequence of length  $2^n-1$ , there are  $2^n-1$  disticnt phase snifts. There are phi(n)/n such sequences, and an equal number of complements. The decoder is shown in Fig.1.

The second method uses LSB addition for embedding the water mark. As a result, the decoder is significantly more complex, as shown in Fig.2. The decoding process makes use of the unique and optimal auto-correlation function of m-sequences, shown in Fig.3. The process requires the examination of the complete bit pattern, and therefore be performed off-line, which is must its principal disadvantage. However, it is intrinsically more secure, since a potential code breaker has to perform the same operations, without any a priori knowledge. The decoding process is not completely error free due to the partial correlation of the image data with the encoding sequence. The dependence of error probabilities on sequence length, and the local variance of image intensity is shown in Fig.4. This graph is based on thresholds which have been chosen to render the probability of false detection equal to that of a missed detection. The above information is pertinent, where only one m-sequence is used for the water mark by encoding its phase. If an ensemble of sequences is to be employed, their crosscorrelation needs to be taken into account. In this m-sequences are not optimal, as shown respect, in Table.. The RMS correlation is constrained due to a second moment identity. Unfortunately the same does not apply to the peak value, which is paramount in determining error probabilities. However, the authors have developed a sieve to constuct sets of m-sequences with constrained crosscorrelations (4).

## 2 M-SEQUENCES

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 sequences thus formed (or the polynomials by which they can be generated) form a finite field called Galois Field. In particular, the autocorrelation function (and hence spectral distribution) of m-sequences resemble that of random Gaussian noise. In

the case of binary noise, the run length distributions and cross correlations look like those of finite Bernoulli trials such as coin tossing. The similarity becomes closer as the sequence length increases. In fact, images encoded with m-sequences and one bit Gaussian noise are shown to indistinguishable from the original and from each be other. In any case, in many imaging systems the LSB is corrupted by hardware imperfections or quantisation noise and hence its sacrifice is of limited significance. The exact choice of code depends on the amount of data to be embedded, the errors involved in image transmission, and the degree of security required. TABLE I illustrates the tradeoffs between code length and properties. The code span is determined by the number of code bits required to be known in order to uniquely deduce the recursion relation. For m-sequences the span is unacceptably short. However, this situation can be remedied by the inclusion of a non-linear look-up table. A translation through this look-up table results in a non-linear code. One particular class of such codes includes the GMW codes. These have a large span whilst retaining the desirable properties of their parent m-sequences. In the case of non-linear codes, it is the rank of the matrix whose entries require diagonalisation in order to complete decoding. Therefore it is a measure of code security against unauthorised detection. Spans beyond 1000 are readily achievable, and for practical purposes these sequences are impossible to crack. In this respect the proposed system resembles traditional public key encryption systems. Other methods of increasing the span and the data content include modulo addition of two or more selected sequences using 2 selection rules devised by Gold and Kasami. (This is equivalent to multiplication of their generator polynomials). The properties of these compound sequences are presented in TABLE II. It is apparent that from a logistic point of view, the large Kasami sequences or the Gold codes offer the best compromise. Additionally, these codes can be generated using only several bytes of information, and hence are ideal for systems which require dynamically adaptive encryption keys. The crosstalk is related to the cross correlation between m-sequences. This, together with image transmission errors determine the threshold for proper code detection. A strategy of computing and optimising these thresholds is presented. A low crosstalk offers greater immunity to transmission errors or the tolerance of lower threshold values, and speedier recognition of the hence correct data. Α traditional problem associated with any digital coding system is that of synchronisation. In this respect, msequences offer an intrinsic advantage because of their two valued autocorrelation property. This makes them ideal

for synchronisation, along with their relatives, the Barker codes. In terms of decoding speed, and consistency it is possible to make use of the unique property called characteristic phase. The preference of codes of Mersenne prime length is a result of their abundance, and superior peak crosstalk properties. The table was compiled on the assumption that each available m-sequence and its complement are symbols of a complex alphabet, which is decoded into standard format by a mapping in a look-up table. The Monash group has performed extensive analysis of m-sequence codes and their correlations. Some of these results have been used to construct the table, whilst others will be discussed in the presentation. Finally, examples of various codes embedded on typical images are presented and analysed. The paper concludes with an analysis of a method which would avoid the sacrifice of the LSB for the insertion of the sequence, and the ramifications on image processing and compression.

### TABLE I

CODE LENGTH	DATA BYTES	CROSSTALK (dB)		SPAN
		MEAN	PEAK	
127	290	-10.5	-4.9	14
8,191	176	-19.6	-10.7	26
131,071	120	-24.1	≥ - 14.3	34
262,143 <sup>@</sup>	60	-27.1	≈ -4.7	36
524,287	215 <sup>#</sup>	-22.6	?	38

# M-SEQUENCE CODE PROPERTIES

<sup>#</sup> Signifies that only a partial sequence can be accommodated. Hence the inferior crosstalk

suppression.

<sup>®</sup> Signifies longest full sequence. Non Mersenne prime length!

## TABLE II

CODE FAMILY	LENGTH	DATA BYTES	CROSSTALK		SPAN
			MEAN	PEAK	
GOLD	262,143	2,048	-27.1	-24.1	72
KASAMI (SMALL)	262,143	4	≤ -30.1	-27.1	72
KASAMI (LARGE)	262,143	1,048,580	?	-24.1	84
GMW (SHORT)	16,383	94	°•	?•	448
GMW <sup>*</sup> (LONG)	268,435, 455	37,044	?	?	28,67 2

## PROPERTIES OF SELECTED M-SEQUENCE DERIVED CODES

\* Signifies that only 0.1% of the sequence length is accommodated. This corresponds to only 9.1 spans. Additionally, a generator of these sequences requires memory size of  $2^{25}$  or 34 MBytes. In contrast, the short GMW sequence generator requires only 34 KBytes!

#### REFERENCES

1) A.Z.Tirkel, C.F.Osborne, N.Mee, G.A.Rankin, A.McAndrew. Maximal Connected Sets - Application to Microcell CDMA. Submitted to the International Journal of Digital and Analog Communications 1993.

2) Sarwate D.V., Pursley M.B. " Crosscorrelation Properties of Pseudorandom and Related Sequences" Proc. of the IEEE vol.68, no 5. May 1980. pp 593-619.

3) Niho Y. " Multi-valued Cross-correlation Functions Between Two Maximal Linear Recursive Sequences" Ph.D. Dissertation, Department of Electrical Engineering. University of Southern California 1972.

4) A.Z.Tirkel, N.R.A.Mee, C.F.Osborne, G.A.Rankin "Cross-Correlation Properties of M-Sequences" Paper Subitted to IEEE