

A DIGITAL WATERMARK

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

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

(+) Scientific Technology, 21 Walstab St, E. Brighton, 3187, 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 a legend essential for image interpretation. This capability is envisaged to find application in image tagging, copyright enforcement, counterfeit protection, and controlled access. Two methods of implementation are discussed. The first is based on bit plane manipulation of the LSB, which offers easy and rapid decoding. The second method utilises linear addition of the water mark to the image data, and is more difficult to decode, offering inherent security. This linearity property also allows some image processing, such as averaging, to take place on the image, without corrupting the water mark beyond recovery. Either method is potentially compatible with JPEG and MPEG processing.

1. INTRODUCTION

The art/science of hiding messages is known as steganography [1]. Conventional techniques involve the encryption of a copyright message on one colour of a composite image. The method described in this paper relies on the manipulation of the LSB of any *colour or monochrome* image, in a manner which is undetectable to the eye. The embedded message is decoded and can be removed from this modified image in order to recover the original information. The desirable properties of an electronic water mark are undetectability and accurate recovery of the hidden message. In general, the problem of embedding an invisible watermark and its subsequent extraction falls into the category of matched or adaptive filtering [2]. The authors have developed a simple modification of such a scheme. In order to render the watermark undetectable, encoding with m-sequences was chosen, because of their balance, random appearance and good auto-correlation properties (a single peak with no sidelobes), which simplify the recovery process [3]. In practice, extended m-sequences were employed, being commensurate with the image size (2^n) and exhibiting a null in autocorrelation around the main peak [4]. Two dimensional analogues such as Costas Arrays were studied, but were rejected because of their sparse nature [5]. For simplicity, we have chosen to encode the water mark by the choice of m-sequence phase. (An alternative method could use the choice of m-sequence to determine the data byte). This paper demonstrates the feasibility of such encoding and the accuracy of the message extraction.

2. M-SEQUENCES

M-Sequences can be formed from starting vectors by a Fibonacci recursion relation, which can be implemented by linear shift registers. 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. The autocorrelation function and spectral distribution of m-sequences resemble that of random Gaussian noise. The cross-correlation of m-sequences has been examined mathematically and empirically in [6], [7] and [8]. Certain families of sequences (maximal connected sets) have been known to possess desirable cross-correlation properties [9]. Images encoded with m-sequences or one bit Gaussian noise are statistically indistinguishable from each other and only visually distinguishable from the original if the image contains large areas with a small intensity variation. 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 [10]. The Monash group has performed extensive analysis of m-sequence codes and their correlations [8]. The vulnerability of m-sequences to cracking is characterised by their span ($2n$), which is the dimension of the matrix which must be diagonalised in order to determine the shift register configuration [3]. In the case of the linear addition of the m-sequence to the image LSB, the code cracker must know the image content without errors in order to determine the encoding sequence. The span of these sequences can be increased by forming compound codes (Gold or Kasami) or by performing non-linear mappings, such as in the GMW sequences [3]. The number of available sequences varies according to the operations performed. Also, it is possible to utilise other sequences of the de Bruijn type, such as Legendre sequences, based on residues, and extremely difficult to crack [11].

3. METHODS OF INCORPORATING THE WATER MARK

Our experiments were conducted on 512*512 8 bit gray scale images encoded on a line by line basis with m-sequences 2^9 pixels long. The first method involves the embedding of the m-sequence 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. The above process enables the LSB to carry the watermark information. The watermark can be decoded by comparing the LSB bit pattern with a stored counterpart. The watermark

message can be carried by the choice of sequence (or its complement) and its phasing. A schematic equivalent of the decoder is shown in Fig.1.

The second method uses LSB addition for embedding the water mark. As a result, the decoder is more complex, as shown in Fig.2. The decoding process makes use of the unique and optimal auto-correlation function of m-sequences. The process requires the examination of the complete bit pattern, and in its current implementation, must therefore be performed off-line, which is 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 partial correlation of the image data with the encoding sequence. This may be suppressed by a deliberate compression of the image dynamic range followed by a compensating mapping of the lookup table, which leads to gray scale quantisation effects. Analysis of the image histogram indicates that a 3 bit dynamic range compression (from 8 bits down to 5 bits) should permit threshold detection to be successful. Alternatively the application of a longer sequence of length 2^{15} or better filtering or detection algorithms should have a similar effect. Since the auto-correlation peak is typically very sharp, (superimposed on a significant, but slowly varying background) it is possible to employ simple filtering techniques to extract it. Various length impulse response filters were tested in single and multi-pass configurations. The differential filter (with kernel -1,-1,4,-1,-1) was found to yield optimum results for 512*512 images with a 9-bit M-sequence. The separation of the image crosscorrelation histogram into image and message peaks shown in Fig. 3(a) and (b) demonstrate the feasibility of using thresholding on the cross-correlation values as a simple and rapid technique of message decoding. The possibility of false positives and false negatives was also investigated in terms of the effect the image content has on the auto-correlation function. The effects of adding two distinct messages to the same image each encoded using a different m-sequence and then added to the image was investigated in terms of their effect on each other and their recovery ability. Such an image could contain two water-marks: one for the hospital, and one for the radiologist. Fig 4. shows some images to which the water mark has been added. The composite image of Fig 4(a) has been changed to that of Fig 4(b) with the addition of the water mark, with a enlarged detail shown in 4(c). The cross-correlation after filtering of this image is shown with (above) and without (below) the watermark in Fig 4(d). The peaks are visible as a series of single white dots in the lower right portion of the figure, whose position determines the message letter (in this case the message is "aabbccAABBCC " repeated four times). This suggests that the water mark is undetectable only in circumstances where low-level gaussian noise is expected. Typically this does not include computer generated images.

4 APPLICATIONS

The objectives of this project are to investigate the feasibility of embedding undetectable watermarks for the purposes of image integrity verification, tagging and copyright infringement protection and controlled image access. The anticipated applications include

medical images, commercial photographs and videos, sensitive documents such as patents, artwork, and computer generated images.

5. FUTURE WORK

The authors are investigating LMS adaptive filter extraction algorithms to determine an optimum technique with minimal image dependence. We will explore the effects on the watermark due to cropping and distortions such as skew, rotations, translations etc, and countermeasures against these. These may include bit-swapping or diagonal raster folding of sequences into m-arrays [12]. These operations are facilitated by our choice of extended m-sequences of length 2^n . The desirability of tamper-resistant watermarks could be a function of the application. Some implementations may be better served by retaining a distorted watermark as evidence of the illegal act! This aspect requires further study.

6. CONCLUSIONS

This paper examines the feasibility of embedding a digital water mark on test images. The main problems found with adding the water mark is in retaining the dynamic range of the original image and the auto-correlation output. The paper discusses a method which would avoid the sacrifice of the LSB for the insertion of the sequence, and the ramifications on image processing and compression. The techniques used and contemplated for watermark coding and detection are all compatible with hardware implementation in standard size programmable gate array IC's. Such implementation would be capable of on-line, real time algorithm execution.

7.ACKNOWLEDGEMENT

The authors would like to express their gratitude to Mr. G.A.Rankin for his assistance in developing a program to generate and analyse the auto and cross-correlations of m-sequences and related codes, which has proved invaluable in this project.

8. REFERENCES

- [1] E.Sapwater and K.Wood "Electronic Copyright Protection", Photo-Electronic Imaging, vol 37, No.6, (1994), p.16-21.
- [2] B.Widrow. "Adaptive Signal Processing." Englewood Cliffs, N.J. Prentice Hall. 1985.
- [3] M.K. Simon, J.K.Omura, R.A.Scholtz, B.K.Levitt. "Spread Spectrum Communications" Volume III. Rockville Md. Computer Science Press. 1985.
- [4] U.-C.G.Fiebig. "Auto- and Crosscorrelation Properties for Extended m-Sequences and Related Sequences" IEEE ISSTA Symposium, Oulu, Finland, July 4-6, 1994. p.406-410.
- [5] S.W.Golomb, H.Taylor. "Construction and Properties of Costas Arrays". Proc.IEEE, vol.72, p.1143-1163. Sept 1984.
- [6] 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.

- [7] 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.
- [8] A.Z.Tirkel, N.R.A.Mee, C.F.Osborne, G.A.Rankin "Cross-Correlation Properties of M-Sequences" Paper Submitted to IEEE Transactions on Information Theory.
- [9] A.Z.Tirkel, C.F.Osborne, N.Mee, G.A.Rankin, A.McAndrew. "Maximal Connected Sets - Application to Microcell CDMA".International Journal of Communication Systems.1994.vol 7, p.29-32.
- [10] 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.
- [11] S.Kitabayashi, T.Ozawa, M.Hata. "Property of the Legendre Subsequence" Communication on the Move. ICCS/ISITA '92. Singapore. vol 3. p.1224-1228.
- [12] F.J.McWilliams and N.J.A.Sloane. "Pseudorandom Sequences and Arrays". Proc.IEEE(76), vol 64, p.1715-1729.