

# New families of arrays in two dimensions for watermarking applications

O. Moreno, A.Z. Tirkel, U. Parampalli and R.G. van Schyndel

A new construction of arrays for watermarking is presented. The arrays are composed from cyclic shifts of a binary column with good autocorrelation. The sequence of shifts is obtained from a discrete logarithm of an irreducible quadratic over a finite field. This yields a large family of binary arrays with low off-peak autocorrelation and low cross-correlation in many new and desirable sizes.

**Introduction:** Currently, digital image, audio, video and related media are vulnerable to theft, misuse or manipulation. To guard against this, watermarking technology has been developed. One of the first references to this concept is [1]. Watermarking requires sequences and/or multidimensional arrays [2]. New constructions of families of arrays with desirable properties are essential. These properties are: low off-peak autocorrelation, low cross-correlation, balance, large family size, and a variety of suitable sizes. A desirable, but not essential, property is that the arrays be binary. Watermarks can be designed for a single user or multi-user application. Our designs cater for the more general, multi-user environment. A good survey of watermarking techniques is found in [3]. Here, we describe a new family of arrays which satisfy these requirements. Our constructions are based on a method developed in [4]. The essential ingredients are a column sequence with good autocorrelation, and a shift sequence which is applied as a cyclic shift to the column sequences to form a watermarking array. This Letter describes new shift sequences, which are compatible with known column sequences and are available in many sizes, with no bounds on size.

**Construction:** The new shift sequences are produced by mapping polynomials over finite fields using a logarithmic function. The lowest order, the quadratic, yields the best correlation. In that case, the shift sequence  $s_i$  is constructed as follows:

$$s_i = \log_\alpha(Ax^2 + Bx + C) \quad (1)$$

where:

1.  $x = \alpha^i$ ,  $\alpha$  is a primitive element of a finite field  $GF(q)$  and  $q$  is the number of elements, and is a prime power;
2.  $i$  is an index taking on the values  $0, 1, 2, \dots, q-2$ .  $s_i$  takes on the values  $0, 1, 2, \dots, q-2, \infty$ , where  $\infty$  results from the argument of the log function being equal to 0;
3.  $A, B, C$  are suitably chosen entries from  $GF(q)$ ;
4.  $GF(q) = (0, \alpha^0, \alpha^1, \alpha^2, \dots, \alpha^{q-1})$ ;
5. In this context  $\log_\alpha x = j$  implies that  $x = \alpha^j$ . The log mapping is 1:1, i.e. there is a single value of  $s_i$  for each  $i$ .

Let  $A = [a_{i,j}]$  and  $B = [b_{i,j}]$ ,  $0 \leq i < M$ ,  $0 \leq j < N$  be two arrays of size  $M \times N$  over an alphabet. In this Letter we consider the alphabet to be a subset of complex numbers such as  $\{-1, 1\}$ ,  $\{-1, 0, 1\}$ . Two-dimensional correlation function between  $A$  and  $B$  is defined as  $R_{A,B}(k,l) = \sum \sum a_{i,j} b_{i+k,j+l}^*$ , where  $*$  represents complex conjugation and indices are added modulo  $N$  and  $M$  appropriately. A watermarking array is constructed from  $s_i$  as follows: columns with  $\infty$  in them are strings of constant entries.  $\infty$  does not occur if the quadratic is irreducible, occurs twice if it has two distinct factors, and once if it is a square. All remaining columns are cyclic shifts of a known column over roots of unity, with good correlation. Column  $i$  has cyclic shift equal to  $s_i$ . Columns commensurate with this construction are: Sidelnikov sequences [5], Legendre sequences, m-sequences, Hall sequences, and others [6]. This is the first time Sidelnikov sequences have been used in such a construction. The resulting array finds application in watermarking and related areas.  $s_i$  has the distinct difference property: all differences  $(s_{i+k} - s_i)$  appear exactly once.  $(i+k)$  and  $(s_{i+k} - s_i)$  are calculated modulo  $(q-1)$ . Therefore, the watermarking array and any two-dimensional cyclic shift of itself can have at most one column matching: exactly one column for any nonzero horizontal shift, and no columns matching for any non-trivial purely vertical shift. Therefore, the autocorrelation of a watermarking array is the sum of the autocorrelations of one matching column and  $q-2$  mismatched columns. Since the columns are pseudonoise, with small off-peak autocorrelation

contributions of the mismatched columns are small and sum to a small number, whilst the matching column contributes something of order  $q$ . Therefore, the off-peak autocorrelation values of the array are of order  $q$ , whilst the peak correlation is of order  $q^2$ .

Our construction generates a multiplicity of arrays. Some of the arrays generated by (1) are two-dimensional cyclic shifts of each other (equivalent), and hence have bad correlation. All purely vertical shifts of the array by  $v$  spaces are equivalent, so

$$s_i \equiv s_i + v = \log_\alpha(\alpha^v Ax^2 + \alpha^v Bx + \alpha^v C)$$

Without loss of generality one can make  $\alpha^v A = 1$ , and hence  $s_i = \log_\alpha(x^2 + B'x + C')$  is representative of the equivalence class of all purely vertical shifts, where  $B' = \alpha^v B$ ,  $C' = \alpha^v C$ . All purely horizontal shifts of the array by  $h$  spaces are equivalent to

$$\begin{aligned} s_i &\equiv s_{i+h} = \log_\alpha(\alpha^{2i+2h} + B'\alpha^{i+h} + C') \\ &= \log_\alpha(\alpha^{2i} + \alpha^{-h} B' \alpha^i + \alpha^{-2h} C') + 2h \\ &\equiv \log_\alpha(\alpha^{2i} + \alpha^{-h} B' \alpha^i + \alpha^{-2h} C') \end{aligned}$$

Without loss of generality one can make  $\alpha^{-h} B' = 1$ , and hence  $s_i = \log_\alpha(x^2 + x + C'')$  is representative of the equivalence class of all two-dimensional shifts. Here,  $C'' = \alpha^{-2h} C'$ . Now consider another (inequivalent) array built from  $t_i = \log_\alpha(x^2 + x + D')$ , where  $D' \neq C''$ . The number of matching columns can be obtained by examining  $t_{i+h} - s_i - v = \log_\alpha(x^2 + x + D') - \log_\alpha(x^2 + x + C'') - v$ .

This equation has at most two roots, so that the number of matching columns is at most two. Therefore, the cross-correlation between two arrays is of order  $2q$ , whilst the autocorrelation is of order  $q^2$ . There are  $q-1$  distinct arrays corresponding to the  $q-1$  distinct values of  $C''$ . Each of these can be assigned to a different user. These constructions also find application in modulating radar signals for multi-target recognition [7–10] and in OCDMA [11].

The normalised absolute values of all off-peak auto- and cross-correlations for these watermarking arrays are bounded by approximately  $2/q$  for m-sequence columns and  $4/q$  for Sidelnikov columns. These constructions are new, and available in desirable sizes and alphabets. Such alphabets include selections of complex roots of unity and zero. For example, binary arrays of sizes  $8 \times 8$ ,  $16 \times 16$ ,  $256 \times 256$  are possible. These are desirable in watermarking and other applications, and have not been available before. The arrays are square, balanced (equal numbers of +1's and -1's).

The presence of  $\infty$  in the shift sequence degrades the correlation. Hence, it is desirable to avoid it. This occurs when the quadratic in the shift sequence  $s_i = \log_\alpha(x^2 + x + C'')$  is irreducible. It can be shown that for even characteristics, this occurs when  $T_q^{q^2}(C'') = 1$ , whilst for odd characteristics  $C'' = (1 - \alpha^{2k+1}/2)$  is required. Approximately one half of the quadratics are irreducible, a result which can also be obtained using the Mobius function. The construction can be generalised to higher degree polynomials; this results in a larger family size, but the correlation properties degrade.

**Application to watermarking:** There are many methods of embedding such arrays in media files as watermarks. This depends on the type of media, the purpose of the watermark and the alphabet. Types of media include still image (colour, greyscale, etc), video and audio. Purposes include proof of ownership or copyright, fingerprinting, audit trail, tamper detection, traitor tracing, anonymity, and others. These dictate whether the watermark is embedded in the media directly or whether the media needs to be transformed, using discrete Fourier transform (DFT), discrete wavelet transform, fractal transform, or some other transform, before the watermark is embedded. Various filters may also be used to make the watermark less obtrusive, for example making use of the human visual system or the human auditory system characteristics. In its basic form, the media is transformed (if necessary) and placed into a suitably sized array. If the watermark array is binary, it can be just added to a commensurate sub-array within the media array, with an appropriate scaling factor. For non-binary arrays, the media is transformed into the same non-binary format as in [12]. In our application, the embedding methods of [13], or similar, are suitable. Fig. 1. shows one of the new arrays produced by the construction. The array is built using the shift sequence: 0,4,6,4, - ,6,2,2 obtained from the quadratic  $x^2 + 2x + 1$ . The column sequence is the Sidelnikov sequence: 1,1, -1,1,0, -1, -1, -1.

Black = +1, Grey = -1, White = 0. Fig. 2 shows the autocorrelation of the array from Fig. 1. Fig. 3 shows the cross-correlation of the array from Fig. 1 with another array constructed from the quadratic  $x^2 + x$ , with the shift sequence: 0,4,6,4, - ,6,2,2.

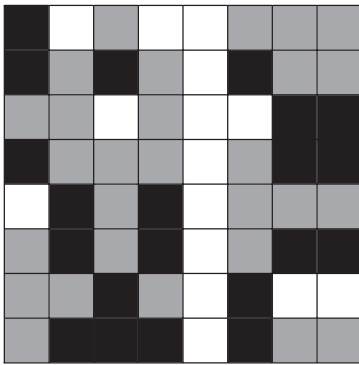


Fig. 1  $8 \times 8$  array using Sidelnikov column

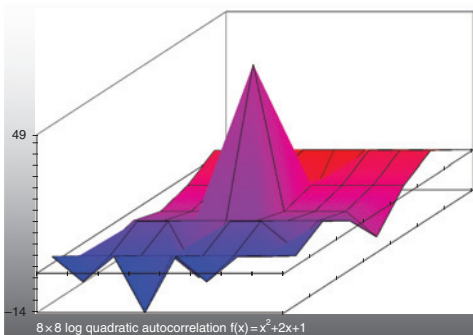


Fig. 2 Autocorrelation of array from Fig. 1

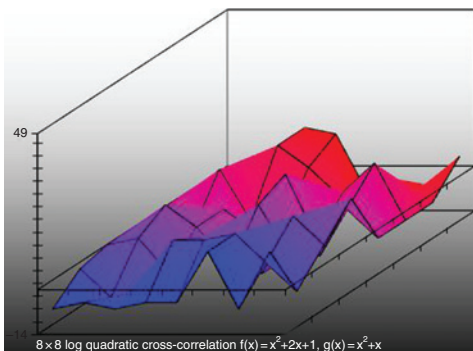


Fig. 3 Cross-correlation between two  $8 \times 8$  arrays

Note the autocorrelation peak in Fig. 2 and the absence of any such peak in Fig. 3, which shows the cross-correlation. An alternate application of the  $8 \times 8$  arrays shown in this example is to embed them as a fragile watermark in the transform domain of an  $8 \times 8$  array of discrete cosine transform (DCT) coefficients. The effects of compression and other tampering of such a block can be detected, if the image under

test shows a reduced autocorrelation peak. The watermark is recovered because of the good auto- and cross-correlation property of our arrays [1, 2].

**Conclusion:** This Letter presents a new array construction, based on cyclic shifts of a column sequence. The shift sequence is obtained using a log quadratic map over a finite field. The large family of arrays has good auto- and cross-correlation, making it applicable to digital image watermarking.

© The Institution of Engineering and Technology 2010

2 August 2010

doi: 10.1049/el.2010.2122

One or more of the Figures in this Letter are available in colour online.

O. Moreno (Gauss Research Laboratory Inc., PO Box 21613, San Juan, 00931, Puerto Rico)

A.Z. Tirkel (Scientific Technology, 8 Cecil St, East Brighton, 3187, Australia)

E-mail: atirkel@bigpond.net.au

U. Parampalli (Department of Computer Science, University of Melbourne, 3000, Australia)

R.G. van Schyndel (School of Computer Science and IT, RMIT University, Melbourne, 3000, Australia)

## References

- 1 Tirkel, A.Z., Rankin, G.A., Van Schyndel, R.M., Ho, W.J., Mee, N.R.A., and Osborne, C.F.: 'Electronic water mark'. DICTA'93, Macquarie University, Sydney, Australia, pp. 666–673
- 2 Tirkel, A.Z., van Schyndel, R.G., and Osborne, C.F.: 'A two-dimensional digital watermark'. DICTA'95, Brisbane, Australia, December, 1995, pp. 378–383
- 3 Hartung, F., and Kutter, M.: 'Multimedia watermarking techniques', *Proc. IEEE*, 1999, **87**, (7), pp. 1079–1107
- 4 Tirkel, A.Z., Osborne, C.F., and Hall, T.E.: 'Steganography – applications of coding theory'. IEEE Information Theory Workshop, Svalbard, Norway, 1997, pp. 57–59
- 5 Sidelnikov, V.M.: 'Some k-valued pseudo-random sequences and nearly equidistant codes', *Probl. Inf. Transm.*, 1969, **5**, (1), pp. 12–16
- 6 Tirkel, A.Z., and Hall, T.E.: 'Matrix construction using cyclic shifts of a column'. ISIT'05, Adelaide, SA, Australia, 2005, pp. 2050–2054
- 7 Kumar, P.V., and Moreno, O.: 'Prime-phase sequences with periodic correlation properties better than binary sequences', *IEEE Trans. Inf. Theory*, 1991, **37**, (3), Part 1, pp. 603–16
- 8 Moreno, O., Zhang, Z., Kumar, P.V., and Zinoviev, V.A.: 'New constructions of optimal cyclically permutable constant weight codes', *IEEE Trans. Inf. Theory*, 1995, **41**, (2), pp. 448–55
- 9 Moreno, O., Golomb, S.W., and Corrada, C.J.: 'Extended sonar sequences', *IEEE Trans. Inf. Theory*, 1997, **43**, (6), pp. 1999–2005
- 10 Moreno, O., and Maric, S.V.: 'A new family of frequency hop codes', *IEEE Trans. Commun.*, 2000, **48**, (8), pp. 1241–1244
- 11 Moreno, O., Games, R.A., and Taylor, H.: 'Sonar sequences from Costas arrays and the best known sonar sequences with up to 100 symbols', *IEEE Trans. Inf. Theory*, 1993, **39**, (6), pp. 1985–7
- 12 van Schyndel, R., Tirkel, A.Z., and Svalbe, I.D.: 'A multiplicative color watermark'. IEEE-EURASIP Workshop on Non-Linear Signal and Imaging Processing, Antalya, Turkey, 1999, pp. 336–340
- 13 Svalbe, I.D., Tirkel, A.Z., and van Schyndel, R.: 'Discrete angle watermark encoding and recovery'. ICPR Int. Conf. on Pattern Recognition, Barcelona, Spain, August 2000, Vol. 4, pp. 246–250