Sequence Families Sets Constructed from Quadratic Congruence Codes for Use in Secure Spread Spectrum Watermarking for Multimedia

C. S. Lim, S. S. Abeysekera and S. K. Amarasinghe

School of Electrical and Electronic Engineering,
Nanyang Technological University, Nanyang Avenue, SINGAPORE 639798.
E-mail: ascslim@ntu.edu.sg, esabeysekera@ntu.edu.sg

ABSTRACT

Digital watermarking for multimedia information has been widely adopted as a measure to detect for copyrights infringements. In many watermarking schemes, often only one watermarking signature is used in the embedding of hidden information. This paper introduces new multiple sequence families with good auto- and cross-correlation properties, which are ideal in the application of digital watermarking. It is also envisaged that this good cross-correlation property of these multiple families of sequences allows for the use of multiple signatures in a watermarking scheme. Multiple signatures increases the robustness of the watermarking scheme and also retrieving for independent signatures is straightforward due to the low cross-correlation property of member sequence.

1. INTRODUCTION

Developments in digital communication and the Internet have seen the growth of digital information beyond bounds. This information being in digital forms also means that they could be replicated and distributed easily in its original quality. In recent years, digital watermarking has been developed and commonly adopted as a means to protect the copyright of the digital contents' owner [1][2][3]. In watermarking, copyrights information is often embedded or hidden in the digital data stream, usually this information is embedded using watermarking signatures. In a watermarking scheme, this additional information is embedded, such that it is imperceptible to the user. The general requirements for watermarking schemes [4] are that, the intended party could retrieve the signatures and therefore the embedded information easily and the ability for it to survive any deliberate attempts to destroy the signatures [5]. In this paper, a new class of multiple families of sequences with good auto- and cross-correlation properties will be introduced. The construction of these sequences, as well as the proofs of their correlation properties will be shown. In the later part, it will be shown how these families of sequences can be advantageous in increasing the security of the embedded signatures when used as digital signatures. It will also be demonstrated how the low cross-correlation property between member sequences allows for easy retrieval of individual signatures.

2. WATERMARK SIGNATURE

In many digital-watermarking schemes, pseudo-random sequences are often used as digital signatures to be embedded into the information data, retrieving of these signatures are usually achieved by an auto-correlator. This section shall illustrate the construction of new multiple families of sequences with good auto- and cross-correlation properties. This new multiple families of sequences are constructed from Quadratic Congruence (QC) Codes and Quadratic Residue (QR) sequences. This construction gives sets of sequence families with good auto- and cross-correlation properties.

2.1 Construction of New Sequence Families Sets

The construction of QC codes [6] is given as,

$$y(k) = ak^2, \quad \text{modulo } p \tag{1}$$

where $k = 0, \ldots, (p-1)$, $1 \le a < p$ and p is an odd prime number. QR sequences [7] of a certain prime length, p, are a class of pseudo-random sequences with the auto-correlation property, $\theta_{bb}(\tau)$, defined as,

$$\theta_{bb}(\tau) = \begin{cases} p, & \tau = 0 \text{ modulo } p \\ -1, & \text{otherwise} \end{cases} \tag{2}$$

where $0 \le \tau < p$.

QR sequences with auto-correlation property defined in (2) exist for prime p, of the form $p = 4k + 3$, where k is any integer. QR sequence, is defined as,

$$b(i) = \begin{cases} 1, & \text{if } i = 0 \text{ modulo } p \\ 0, & \text{if } i \text{ is a quadratic residue modulo } p \\ 1, & \text{if } i \text{ is a quadratic non - residue modulo } p \end{cases} \tag{3}$$

Let $\{b(i)\}_{i=0,\ldots,p-1}$ be the QR sequence of period p, where p is prime number of the form $p = 4k + 3$. Let $\{y(i)\}_{i=0,\ldots,p-1}$ be the single QC code of prime length p, as defined in (1). Then a sequence, $\{z(y(i), b(i))\}$ is defined as,

$$z(y(i), b(i)) = L^{y(i_2)} b(i_1) \tag{4}$$

where $i = i_1 p + i_2$, and $0 \le i_1, i_2 < p$. The symbol $L^l b(i)$ denote the left shift, by l places of sequence b, where

$$L^l b(i) = b(i+l), b(i+l+1), \ldots, b(p-1), b(0), \ldots, b(i+l-1) \tag{5}$$

Now, let's define the sequence family set generated by a single quadratic code as,

$$S = \{s_j(i);\ 0 \le j < p,\ 0 \le i < p^2 - 1\} \tag{6}$$

where $s_j(i) = z(y(i), b(i)) \oplus b(i + j)$ (7)

and $\oplus$ denotes modulo 2 addition and + denotes modulo p addition.

Example: Let p = 11, with the QR sequence of length 11, given as, 10100011101. The QC code with p = 11, from (1), is {0, 1, 4, 9, 5, 3, 3, 5, 9, 4, 1}.

Therefore sequence $z(y(i),b(i))$, defined in (4) can be viewed as an array, *Array*($z(y(i),b(i))$, with the i^{th} columns of the array being essentially the QR sequence of length 11, shifted cyclically by, $y(i)$ positions indicated by the QC code.

The sequence $z(y(i),b(i))$ is obtained by reading off the array row-wise. From (7), the term $b(i+j)$ could be viewed as a $p \times p$ array where its rows are basically the sequence b, shifted cyclically by j position, therefore the sequence $s_j(i)$ is obtained by the modulo 2 addition of the two arrays and reading off the resultant array row-wise.

2.2 Correlation Properties Analysis

Figure 1 and Figure 2, shows the auto- and cross-correlation function of the sequences in the family in the above example respectively.

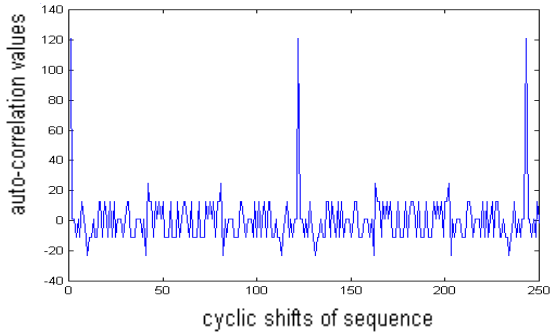

Figure 1: Auto-correlation function of the sequences in the family, S, with the sequences of period, p^2 = 121.

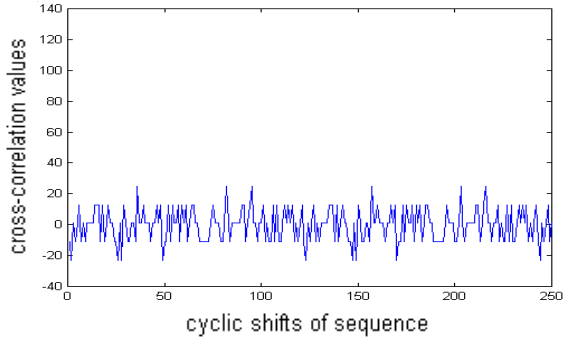

Figure 2: Cross-correlation function of the sequences in the family, S, with the sequences of period, p^2 = 121**.**

From the figures, it is demonstrated that this construction generates families of sequences with its correlation function bounded by, $2p+3$, where p is the prime period and length of sequence $b(i)$ and code $y(i)$.

Proofs: To prove the results, following theorem is required.

Theorem 1: The modulo-2 addition of *Array*($z(y(i),b(i))$) and any of its row-wise cyclically-shifted versions results in at most 2 columns of all binary '0's.

The columns of, *Array*($z(y(i),b(i))$), are essentially the sequence $b(i)$ shifted by $y(i)$ positions, columns of all binary '0's arise when the i^{th} column's $y(i)$ of the shifted *Array*($z(y(i),b(i))$), coincides with the i^{th} column's $y(i)$ of the unshifted *Array*($z(y(i),b(i))$). The following expression describe the code $y'(i)$, of *Array*($z(y(i),b(i))$) after shifted cyclically row-wise by τ positions.

$$y'(i) = y(i+\tau) + c \tag{8}$$

where i = 0, …., $p-1$, τ any integer between $0 \le \tau < p^2$ and c is the integer value of $((i+\tau) \bmod p^2)/p$. For a coincidence to occur, we have

$$y(i) - y'(i) = 0 \tag{9}$$

If τ = 0, c = 0, we have the trivial coincidence function at zero shift, if τ = 0 mod p, $c \neq 0$, then situation at (9) will never occur, meaning 0 coincidences. However if $\tau \neq 0$ mod p, then

$$y(i) - [y(i+\tau) + e] \quad \text{for } (i+\tau) < p(e+1) \tag{10}$$

and $$y(i) - [y(i+\tau) + e + 1] \quad \text{for } (i+\tau) \ge p(e+1) \tag{11}$$

with i = 0, …., $p-1$ and e the integer value of τ/p.

With the definition of $y(i)$ from (1), by solving the expression (10) and (11) for i, it is straightforward that each expression has only one solution for i. Therefore summing up both (10) and (11), we can show that there can be at most 2 coincidences.

From the construction of the sequence families, the sequence $s_j(i)$ defined in (7) can be rewritten as

$$s_j(i) = Array(z(y(i),b(i))) \oplus Array(L^j b(i)) \tag{12}$$

The correlation of j^{th} and k^{th} sequences of the family defined in (6) can be given as,

$$\theta_{s_j,s_k}(\tau) = \sum_{i=0}^{p^2-1} (-1)^{s_j(i) \oplus s_k(i+\tau)} \tag{13}$$

where τ indicates the integer number of shifts, $0 \le \tau < p^2$. From (13), it is obvious that to obtain the correlation values, we only need to compute, $s_j(i) \oplus s_k(i+\tau)$.

$$s_j(i) \oplus s_k(i+\tau) = Array(z(y(i),b(i))) \oplus Array(L^j b(i)) \oplus Array(L^{\tau_1} z(y(i),b(i))) \oplus Array(L^{k+\tau_2} b(i)) \tag{14}$$

where and $0 \le \tau_1 < p$ and $0 \le \tau_2 < p$.

From theorem 1, we know that $Array(L^{\tau_1} z(y(i),b(i)))$ has at most 2 columns of all binary '0's for $\tau_1 \neq 0$. From the construction of sequence families, it is observed that the columns of $Array(z(y(i),b(i)))$ and $Array(L^{\tau_1} z(y(i),b(i)))$, where a coincidence has not occur for the later, are essentially the sequence $b(i)$, also the columns of $Array(L^j b(i))$ and $Array(L^{k+\tau_2} b(i))$ are either all the binary '1's or '0's, where their rows are the sequence $b(i)$. Therefore through a straightforward computation of possible cases, the non-trivial correlation values are given as $\{2p+3, p+2, 1, -p, -2p-1\}$.

2.3 Generation of Sequence Family Set

Figure 3 below shows the basic block diagram for the generation of the new sequence family set.

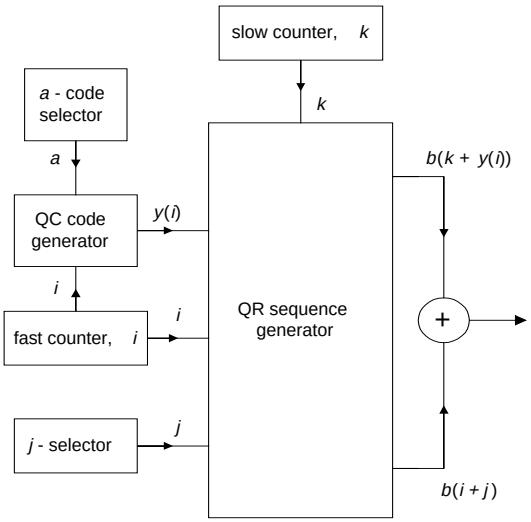

Figure 3: Block Diagram for Sequence Generation

From the block diagram illustrated, it can be observed that generation of sequence families can be achieved by a single architecture. Selection of member sequences can be accomplished by switching *j* and selection of families by switching *a*.

3. APPLICATION OF NEW SEQUENCE FAMILY SET IN DIGITAL WATERMARKING SYSTEM

In most digital watermarking system, only one digital signature is employed. In a general watermarking scheme, careful selection of the signature length is necessary for the detection of signature embedded in the data stream (e.g. in an audio stream).

For the selection of the signature length, consider the output of the auto-correlator at the detector, which is given by,

$$(a(i)+\alpha\cdot s(i))\otimes s(i) \quad (15)$$

where $a(i)$ is the audio data, $s(i)$ is the signature and α is a suitable scaling factor. From the above function, it can be deduced that the detector's Peak Power Level (PPL) is largely influenced by the signature peak auto-correlation and given by,

$$\text{PPL} = \alpha^2 L^2 \quad (16)$$

where L is the signature sequence length. Also the detector's Noise Power Level (NPL) can be shown to be,

$$\text{NPL} = A\cdot L \quad (17)$$

where A is the audio signal power. Therefore for detection of signature peak, we have from (16) and (17),

$$\alpha^2 L^2 >> A\cdot L$$

$$L >> A/\alpha^2 \quad (18)$$

Using multiple digital signatures one could improve the overall security and robustness of the watermarking scheme. In the multiple families of sequences proposed in the earlier section, it is proven and demonstrated that the families of sequences have got good cross-correlation properties and that member sequence of the family can be generated easily by switching the parameter *j*, as indicated in Figure 3. Therefore such a family will be ideal for the watermarking scheme whereby a different digital signature within the family can be embedded into the information data stream at a different point in time. Also by dictating the unique sequence at which *j* switches, this gives an added level of security, switching *a* allows for the selection of families. Embedding multiple digital signatures into an information data stream improves the robustness of such a system, as multiple distinct signatures are used, the survival chances for these signatures are higher when subject to deliberate signature attacks. The good cross-correlation properties between these distinct signatures ensure that the signatures won't interfere with each other when retrieved with an auto-correlator. This will be elaborated in section 4.

In the case of multiple sequences, *p* sequences of length p^2 are used as signatures and this *p* signatures carries one bit of embedded information, detection is by cumulative addition of *p* signatures. With multiple signatures, equations (16-17) will be modified as follows:

$$\text{PPL} = \alpha^2\cdot(p^2)^2\cdot p \quad (19)$$

$$\text{and NPL} = A\cdot p\cdot p \quad (20)$$

$$\text{Therefore we get, } p^3 >> A/\alpha^2 \quad (21)$$

4. PERFORMANCE EVALUATION

Consider the following simulated experiment. In the simulation, member sequences of length 1849 are generated from a QR sequence and QC code of prime length 43. This family was used as digital signatures to be embedded into the information data. The generated signatures were passed through a 10 kHz bandwidth low-pass filter before embedding into the audio data stream (audio data stream was from a bowed string instrument sampled at 44.1 kHz). The 10kHz filter was chosen so that the watermark could be well hidden in the data stream with least susceptibility to an attack. Figure 4 shows both the original audio data and the audio data embedded with the signatures. Figure 5 shows both the spectra of original and embedded with signatures audio data and Figure 6 show the detection of distinct signatures. This signature detection is achieved by means of an auto-correlator. Due to the good cross-correlation property between the member sequences, it can be observed from the results obtained that these signatures do not interfere with each other in detection.

Note that in embedding the watermark, the squared scaling factor, α^2 is chosen to be 10^{-5} dB after examining the original audio data spectra in Figure 5. The average audio power within 10 kHz bandwith is computed to be 10^{-1} dB. In this simulation where multiple signatures from the generated family are used, according to equation (21) we have, $p^3 >> 10^4$, and thus $p >> 22$. Therefore, *p* was chosen to be 43 and p^3 = 79,507. Note that if a single sequence (as in conventional methods) was used, according to equation (18), *L* need to be much greater than 10^4, i.e. chosing *L* to be larger by a factor of 8 results in a single sequence of length 80,000. *It is elaborated here that from a hardware implementation point of view, generating and detection of 43 multiple sequences of length 1849 from a family is much simpler and easier as well as more robust than using a single sequence of length 80,000.*

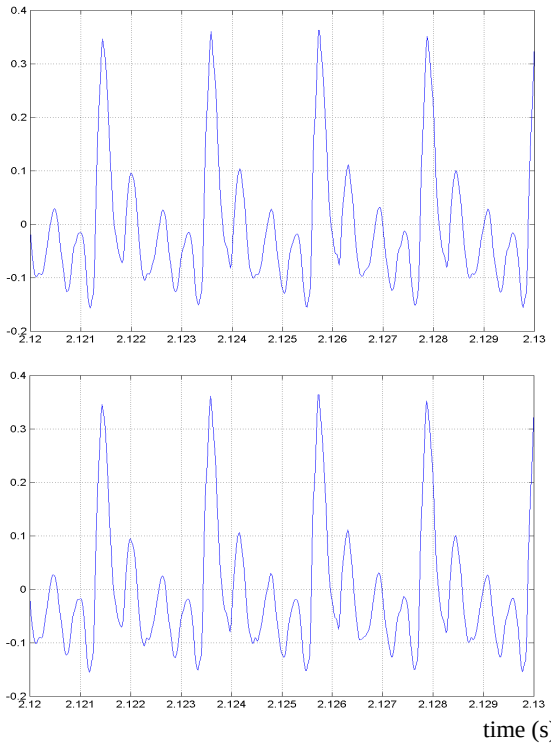

Figure 4: Original audio (top) and signature embedded audio (bottom) data stream

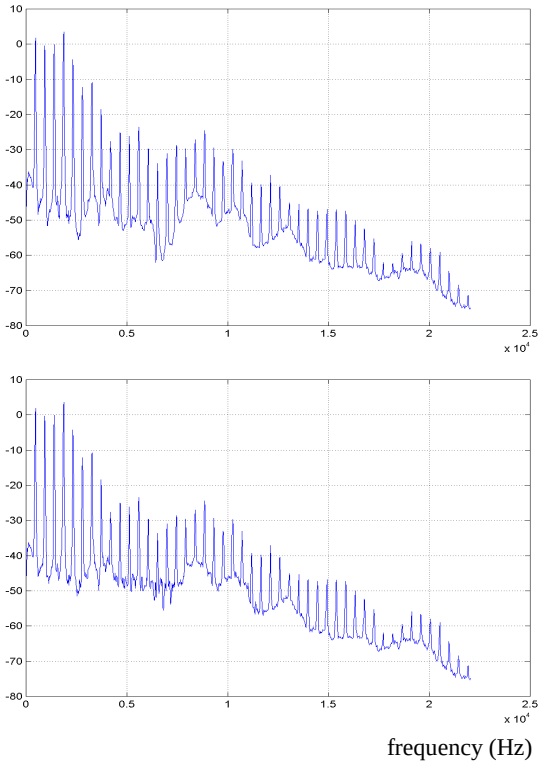

Figure 5: Original (top) and signature embedded audio (bottom) signal spectra

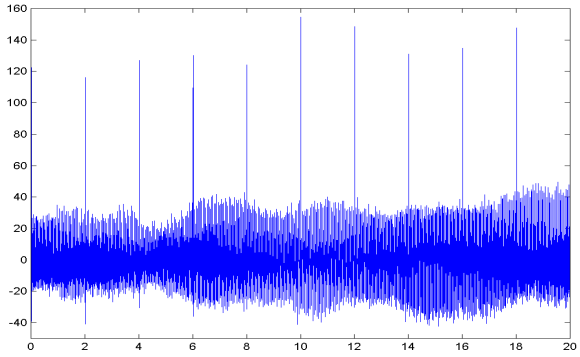

Figure 6: Signature detection with correlator (time index is in multiples of sequence length.)

5. SUMMARY

This paper introduces the construction and proofs of a new family of sequences with good correlation properties. Simulation shows that digital watermarking scheme can benefit by using such multiple families of sequences where the security and robustness of the watermarking scheme can be improved. Watermarking techniques are a widely researched area, often the success of a watermarking scheme depends upon the physical effects of embedding additional information on the original information data, which should be imperceptible to the user, the security of the system and the robustness of the watermarks. Sequences with ideal pseudo-random properties are usually employed as solo signature in digital watermarking scheme. However, it commonly known that sequences with ideal pseudo-random properties do not usually have good cross-correlation property and this make them unsuitable for multiple signatures watermarking scheme. This paper introduces multiple sequence families with good correlation properties and shows the ability of such sequence families in improving the overall security and robustness of a watermarking scheme. It is demonstrated that single hardware architecture is sufficient for the generation of sequence families and the retrieval of these signatures in a watermarking scheme can be carried-out easily, due to the low cross-correlation between member sequences.

6. REFERENCES

[1] M. Swanson, M. Kobayashi and A. Tewfik, "Multimedia Data Embedding and Watermarking Technologies", *Proc. of the IEEE*, 1998, vol. 86, pp. 1064-1087.

[2] L. Boney, A. Tewfik and K. Hamdy, "Digital Watermarks for Audio Signals", *Proceedings of Multimedia '96, Piscataway, NJ: IEEE Press*, 1996, pp 473-480.

[3] K. Matsui and K. Tanaka, "Video-Steganography", *in Proc. IMA Intellectual Property Project*, 1994, vol. 1, pp 187-206.

[4] I. Cox, J. Kilian, F. Leighton and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia", *IEEE Trans. Image Processing*, 1997, vol. 6, pp 1673-1687.

[5] M. Swanson, B. Zhu, A. Tewfik and L. Boney, "Robust Audio Watermarking using Perceptual Masking", *Signal Processing, Elsevier Science*, 1998, vol. 66, pp 337-355.

[6] E. Titlebaum, J. Bellegarda and S. Maric, "Ambiguity properties of Quadratic Congruential Coding", *IEEE Trans. AES*, vol. 27, 1991, pp. 18-29.

[7] D. Everett, "Periodic digital sequences with pseudonoise properties", *G.E.C Journal*, vol. 33, 1966, pp. 115-126.