SECURITY AND SYNCHRONIZATION IN WATERMARK SEQUENCE

Litao Gang, Ali N. Akansu and Mahalingam Ramkumar

ECE. Dept., New Jersey Institute of Technology
New Jersey Center for Multimedia Research
University Heights, Newark, NJ 07102.
{lxg8906, ali, mxr0096}@njit.edu

ABSTRACT

In a mature watermarking and steganography application, the security should lie in the unknow random keys not in the embedding algorithms. In this paper, the problem of the selection of watermarking random sequences is investigated. In the widely used Spread Spectrum modulation schemes, a white sequence and a Low-Pass (LP) type sequneces are analyzed, including its security level and synchronization requirements. It is found that the white independent is more secure but not robust against LP attack. Also it is not energy efficient. Actually The random sequence selection is usually the tradeoff between these factors. To be resilient to the removal attacks, the watermark spectrum should be similar to the spectrum of the cover signal. A watermarking sequence with fixed amplitude spectrum shape and random phase is proposed in the last part of the paper and its properties are discussed in detail.

1. INTRODUCTION

Watermarking or steganography provides a possible solution to multimedia copyright protection and piracy tracking. Similar to an encryption system, it is believed a mature watermark system should be employed with a public algorithm and a private key. The key is usually used to generate a random sequence. An attacker tries to "guess" a sequence close enough to the watermark sequence and remove it. This attack is referred to as "guessing" attack in this paper.

One of the influential algorithms is the Spread Spectrum (SS) modulation. Cox *et al.* are among the first to employ it in practice [3] [4]. The SS-based schemes have been widely used in practice, in video [5], audio [2] and images [3]. In this paper, we concentrate on watermark embedding in the time/spatial domain.

In Section 2, the guessing attack is analyzed on the white Gaussian sequence and AR(1) sequence. Results shows that the white sequence is more secure against the attack.

One of most important concerns in SS modulation is synchronization. In Section 3, misalignment effect on the white sequence and AR(1) sequence is discussed. Analysis demonstrates the white sequence is more sensitive to synchronization than the latter.

AR(1) sequence is just a simple specific case of colored sequence. It has some advantage over white sequence. The latter is not energy efficient, since most cover signals are of low-pass type. This can give a smart attacker some advantage if he combines low-pass filtering and the guessing attack.

To be energy efficient, the spectrum of the watermark signal should be proportional to the cover signal [6]. In Section 4, we proposed a watermark sequence generated by the random phase and analyzed its security.

In the last section, some conclusions are summarized.

2. SECURITY OF GAUSSIAN PN SEQUENCE

2.1. White Gaussian Sequence

The white Gaussian sequence is widely used in various watermarking schemes [1] [4] . In a white sequence $\mathbf{x}$, $x_i \sim N(0, \sigma_x^2)$ and x_i is i.i.d.

In a public scheme scenario, an attacker knows the parameters σ_x and sequence length N, but does not know the random seed. In the guessing attack, a random sequence $\mathbf{y}$ is generated. The "closeness" between $\mathbf{x}$ and $\mathbf{y}$ is measured by correlation

$$q = <\mathbf{x}, \mathbf{y}> = \sum_{i=0}^{N-1} x_i y_i, \tag{1}$$

If the correlation output is larger than a fixed threshold γ, the attacker assumes that $\mathbf{y}$ is sufficiently close to $\mathbf{x}$ and stops. By subtracting the sequence $\mathbf{y}$, a good proportion of the watermark energy could be removed.

As a linear combination of $\mathbf{y}$, output q is Gaussian distributed

$$q \sim N(0, \sigma_x^2 \sum_{i=0}^{N-1} x_i^2). \tag{2}$$

The exact value of q is dependent on the individual signature sequence $\mathbf{x}$. However, for a large value of sequence length N, we have

$$E[q^2] = \sigma^2 \sum_{i=0}^{N-1} x_i^2 \approx N {\sigma_x}^4. \tag{3}$$

The successful attack probability is

$$P(q > \gamma) = Q(\frac{\gamma}{\sqrt{N}{\sigma_x}^2}), \tag{4}$$

auto-regression where $Q(.)$ is the Gaussian pdf tail integral function. Some numerical result for white sequence (corresponding to $\rho = 0.0$) is shown in Table 1.

White sequences are quite secure against this guessing attack. This conclusion is justified by the intuition the white sequence is the most "unpredictable". The signature sequence has a flat spectrum whereas most cover signals are of low-pass type. Most high frequency energy could be removed by low-pass filtering. For example, in a typical audio signal, most energy is concentrated between 0 – 6KHz. For an audio signal sampled at 48KHz, by suppressing frequency components over 6KHz, a smart attacker can remove 75% of the white watermark signal energy without much noticeable distortion. In that sense, the white sequence, although secure, is less energy efficient.

Low-pass (LP) type random signature can keep most energy after low-pass filtering attack. As a case study, in the next paragraphs, we analyze a simple colored PN sequence – AR(1) random process.

2.2. AR (1) PN Sequence

The first order AR(1) sequence $\mathbf{x}$ can be expressed as

$$x_i = \rho x_{i-1} + u_i, \tag{5}$$

where

$$\rho = \frac{E[x_i x_{i-1}]}{\sigma_x^2}, \tag{6}$$

and $u_i \sim N(0, (1-\rho^2)\sigma_x{}^2)$, u_i is i.i.d.

The attacker tries to generate a matching sequence $\mathbf{y}$ randomly based on the same AR(1) model (suppose he knows ρ).

Correlation output (1) is also used to measure the successfulness of this attack. It can be easily shown that $E[q] =< \mathbf{x}, \mathbf{y} >= 0$.

The variation of correlation output q is

$$E[q^2] = E[(x_0y_0 + x_1y_1 + ... + x_{N-1}y_{N-1})^2] \tag{7}$$

Using

$$E[y_i y_{i-j}] = \sigma^2\rho^j \tag{8}$$

and

$$E[x_i x_{i-j}] \approx \sigma^2\rho^j, \tag{9}$$

Equation (7) can be reduced to

$$E[q^2] = N + 2(L-1)\rho^2 + 2(L-2)\rho^4 + ... + 2\rho^{L-1}. \tag{10}$$

After some algebraic steps, the final result can be obtained as

$$\sigma_q^2 = E[q^2] = 2[\frac{N-\rho^{2N}}{1-\rho^2} - \frac{\rho^2-\rho^N}{(1-\rho^2)^2}] - N. \tag{11}$$

For a sufficiently large value of sequence length N, the above can be further expressed as

$$\sigma_q^2 \approx \alpha N, \tag{12}$$

where

$$\alpha = \frac{2}{1-\rho^2} - 1. \tag{13}$$

Similarly the successful guessing attack probability is

$$P(q > \gamma) = Q(\frac{\gamma}{\sigma_q}) = Q(\frac{\gamma}{\sqrt{\alpha N}\sigma_x^2}). \tag{14}$$

Compared with (4), for a same threshold value γ in order to achieve the same security level, the AR(1) sequence length should be increased by a factor α. For example, for the $\rho = 0.8$ case, $\alpha = 4.56$, AR(1) sequence length 456 has the same robustness as the white sequence length 100.

Table 1. shows the successful attack probability for different ρ and N values.

The result reveals that the LP type signal is more vulnerable to the guessing attack due to the correlation between x_i. However, it has some desirable properties, one is the relaxed synchronization requirement at decoder.

	N=30	N=100	N=400
$\rho = 0$	$2.16 \cdot 10^{-8}$	$7.62 \cdot 10^{-24}$	$2.75 \cdot 10^{-89}$
$\rho = 0.5$	$3.98 \cdot 10^{-4}$	$4.57 \cdot 10^{-10}$	$8.66 \cdot 10^{-35}$
$\rho = 0.8$	$1.00 \cdot 10^{-2}$	$1.10 \cdot 10^{-5}$	$1.08 \cdot 10^{-17}$

Table 1: Sequence Security Comparison ($\gamma = N\sigma_x^2$)

3. SYNCHRONIZATION EFFECT ON DETECTION

In SS modulation, it is well known the decoder is extremely sensitive to synchronization. Su *et al.* first addresses this problem in [7]. As we will see, the LP type sequence is less sensitive to synchronization, which is often a desirable property in practice.

3.1. White Gaussian Sequence

Suppose a signal $\mathbf{x}$ is transmitted through a Gaussian channel,

$$r_i = x_i + z_i, \tag{15}$$

where z_i is the channel noise, $z_i \sim N(0, \sigma_z^2)$.

If the sequence is perfectly matched, the output SNR can be shown to be

$$SNR = \frac{S^2}{E[Z^2]} = \frac{(\sum x_i{}^2)^2}{\sigma_z^2 \sum x_i^2} \approx \frac{N\sigma_x^2}{\sigma_z^2}. \tag{16}$$

However if the received sequence $\mathbf{r}$ and $\mathbf{x}$ is not perfectly matched, $SNR \approx 0$. The watermark verification completely fails.

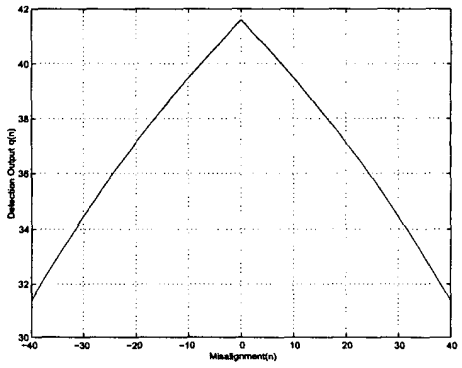

Figure 1: AR(1) Correlation Output vs. Misalignment

3.2. AR(1) Random Sequence

For an AR(1) sequence generated by (6), although the output SNR degrades if **r** and **x** are not perfectly synchronized, there is still some signal energy residue in the correlation detector output.

In the case **x** and **r** is synchronized, AR(1) sequence performs as well as the white sequence. In the case they are misaligned by M sample slip shift, the filter output SNR can be calculated as

$$SNR_M = \frac{(N-M)^2\sigma_x^2\rho^2}{N\sigma_z^2}. \quad (17)$$

Fig. 1 shows the SNR value at different misalignment. The sequence length is $N = 100$, $\rho = 0.8$, $\sigma_x = \sigma_z$. Obliviously the AR(1) sequence is less sensitive to synchronization than the white sequence.

4. RANDOM SEQUENCE DESIGN

4.1. Sequence Spectrum Shaping

In the above discussion, we have studied two examples, a white sequence and LP type sequence. The AR(1) sequence is just a special case of a colored sequence. A more general colored sequence can be generated by a AR(M) model,

$$x_i = \sum_{j=1}^{M} h_j x_{i-j} + w_i, \quad (18)$$

where w_i is white Gaussian noise and i.i.d. And x_i is Gaussian distributed and independent with w_i.

The above AR(M) colored sequence can be interpreted as the white sequence shaped by a LP filter.

Although the white sequence is more secure than a LP type sequence. That is true only when no attack is present. The low-pass filtering attack can remove the watermark energy in high frequency bands without much visual artifacts. A smart attacker can combine the low-pass filtering and guessing attack therefore compromise its security to the level in the LP sequence. In another word, the watermarking energy in a whole spectrum is not well-spent, resulting in energy inefficiency.

Su *et al.* [6] points out in the face of Wiener filtering, the spectrum of the watermark signal should be proportional to that of the cover signal. Under this case, the filtering is nothing but a scaling operation. That implies no gains achieved in this attack.

In practice, watermark signal power spectrum $X(\omega)$ may not be exactly proportional to the cover signal spectrum $N(\omega)$. But should be very close to $N(\omega)$. Since the cover signal spectrum $N(\omega)$ is usually in the public domain, $X(\omega)$ is also public. The randomness mainly lies in the phase.

4.2. Random Phase Sequence

The random phase sequence can be easily generated in DFT domain. Suppose the N-point DFT transform of the watermark signal $x(n)$ is $|X(k)|$. A random phase sequence θ_i is generated by a private key. θ_i is i.i.d., $\theta_i \sim U(0, 2\pi)$, satisfies the odd symmetry property

$$\theta_k = \begin{cases} 0 \text{ or } \pi & k = 0, \frac{N}{2} \\ \theta_k & k = 1, 2, .. \frac{N}{2} - 1 \\ -\theta_{k-N/2} & k = \frac{N}{2}+1, \frac{N}{2}+2, ..., N-1 \end{cases}$$

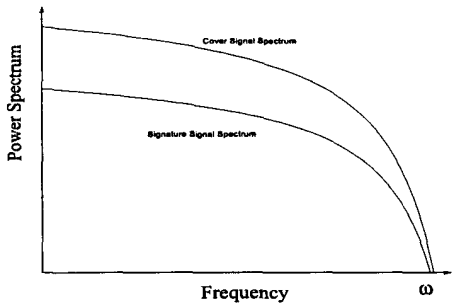

Figure 2: Watermark Spectrum Against Wiener Filtering

The embedding and extraction could be done in time or DFT domain.

The watermark sequence is generated as $x(k) = exp(\theta_k)$. In order to analyzed its security against the guessing attack, for simplicity, we suppose the cover signal spectrum is brick-shape as depicted in Fig. 3.

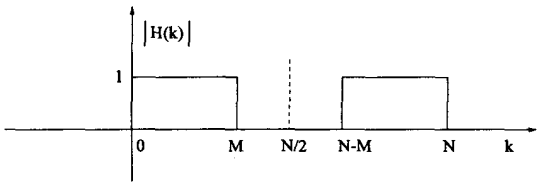

Figure 3: Brick-shape LP Watermark Spectrum

Suppose the attacker randomly generate a phase sequence β. The correlation between these two vectors are

$$q = \sum_{k=0}^{M-1} (e^{j(\beta_k - \theta_k)} + e^{-j(\beta_k - \theta_k)}) = 2\sum_{k=0}^{M-1} cos(\beta_k - \theta_k), \quad (19)$$

Both θ_k and β_k are uniformly distributed in the range $[0, 2\pi)$. The mathematical expectation of $t_k = cos(\beta_k - \theta_k)$ is

$$E[t_k] = \int_0^{2\pi} cos(\beta_k - \theta_k)\frac{1}{2\pi}d\beta_k = 0. \quad (20)$$

The deviation of t_k is

$$E[t_k^2] = \int_0^{2\pi} cos^2(\beta_k - \theta_k)\frac{1}{2\pi}d\beta_k = \frac{1}{2}. \quad (21)$$

For a large number of M, q is approximately Gaussian distributed. Its distribution can be shown to be $q \sim N(0, M)$.

The successful guessing attack probability is

$$P(q > \gamma) = Q(\frac{\gamma}{\sqrt{M}}). \quad (22)$$

For example, for different values of M=30, 60 and 100, the successful attack probabilities are $4.74 \cdot 10^{-15}$, $1.04 \cdot 10^{-45}$ and $3.16 \cdot 10^{-28}$ respectively.

The impact of misalignment can be analyzed in a similar fashion. It can be seen without misalignment, the signal component in the correlation detection output is $2M$. Our

mathematical analysis shows that with $p(p \neq 0)$ sample slip shift, the correlation output can be shown to be

$$y_p = 1 + \frac{cos\frac{2\pi p}{N}(M-1) - cos\frac{2\pi p}{N}M}{1 - cos\frac{2\pi p}{N}}. \quad (23)$$

Fig. 4 shows the output vs. misalignment. The sequence length is $M = 30$ and $N = 200$.

The sequence length N and sequence bandwidth (represented by M) are two important parameters. Larger N implies enhanced security against guessing attack, and smaller M lowers the security level, but also relaxes the synchronization requirement.

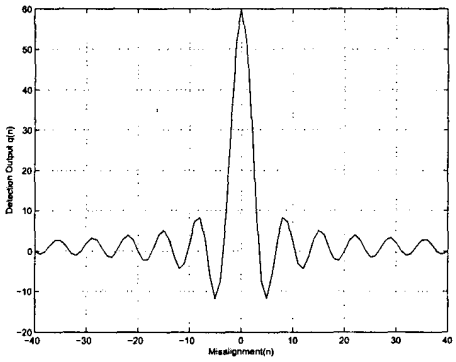

Figure 4: Correlation Output vs. Misalignment

5. EXPERIMENTS AND CONCLUSIONS

It is intuitive to conclude that the white random sequence is more secure since it is independent. However it is not very robust against low-pass filtering attacks as much of its energy is removed after the attack. The watermarking sequence with a colored spectrum is more robust to the attack and is also more energy efficient.

From above analysis and simulation studies it can be concluded that the spectrum of the watermark signal should be close to the spectrum of the cover signal. This prevents easy removal based on the different statistical properties of these two signals, for example, Wiener attack. Compared with Gaussian sequence, the main advantage of the random phase sequence is its flexibility. It provides a trade-off between security and synchronization requirements.

In the random phase sequence, the sequence frequency shape is fixed, only the phase is random. Every sequence has the same energy. In practice, it may not be necessary to keep the sequence spectrum strictly brick-shape. Various visual models could also be applied to further control the distortion visibility. Our experiments with images and audio signals demonstrate its robustness against low-pass filtering and compression.

In this paper, we analyzed the security and synchronization of white and colored sequence. The colored sequence is superior to a white sequence due to its energy efficiency. The wider the bandwidth of the sequence, the more secure it is against guessing attack, but more sensitive to synchronization. The random phase sequence is an effective sequence in watermarking applications.

6. REFERENCES

[1] W. Bender, D. Gruhl, N. Morimoto, and A. Lu. "Technique for data hiding". *IBM System Journal*, 35(3-4):313–336, 1996.

[2] L. Boney, A. H. Tewfik, and K. N. Hamdy. "Digital watermarks for audio signals". *Proc. IEEE International Conference on Multimedia Computing and Systems*, pages 473–480, June 1996.

[3] I. Cox and M. L. Miller. "A review of watermarking and the importance of perceptual modeling". *Proceeding of Electronic Imaging*, Feb. 1997.

[4] I. J. Cox, Joe Kilian, Tom Leighton, and Talal Shamoon. "A Secure, robust watermark for multimedia". *Workshop on Information Hiding'96*, May 1996.

[5] F. Hartung and B. Girod. "Watermarking of uncompressed and compressed video". *Signal Processing*, 66(3):283–301, May 1998.

[6] J. K. Su and B. Girod. "Power-spectrum condition for energy-efficient watermarking". *Proc. ICIP'99*, Oct. 1999.

[7] J. K. Su, F. Hartung, and B. Girod. "A channel model for a watermark attack". *Proc. SPIE, Security and Watermarking of Multimedia Contents, Electronic Imaging '99, San Jose, CA*, 3657:159–170, Jan. 1999.