Chaotic signal masking based on orthogonal polynomials

S V Belim¹ 2 and S Yu Belim¹

¹Omsk State Technical University, 11 Mira ave., 644050, Omsk, Russia
²Siberian State Automobile and Highway University, Omsk, Russia

Abstract. The article discusses the approach to encoding information based on families of orthogonal polynomials. The discrete signal is represented as a superposition of orthogonal polynomials. This approach allows to transmit the useful signal in a chaotic container without matching the parameters of the noise generators. Different orthogonal functions families are considered: trigonometric functions and, Lagrange polynomials. The parameters of orthogonal polynomials families have been studied to increase the stability and stealth of the signal. The computer experiment is made. The average number of decoding errors is calculated depending on the numerical integration step. Orthogonal polynomials require significantly larger calculations to decode the message.

1. Introduction

The main purpose of chaotic signal masking is to hide the fact of message transmission. The signal is encapsulated in a chaotic container. The chaotic component is subtracted when the signal is received. In the simplest case, chaotic noise $x(t)$ is added to the transmitted message $m(t)$. The result is a mixed signal $m'(t)=m(t)+x(t)$. The chaotic noise $u(t)$ is subtracted after receiving the mixed signal. The result is a message $m''(t)=m'(t)-u(t)$. The received message $m''(t)$ is equivalent to that transmitted $m(t)$ if $u(t)=x(t)$. The message is transferred without mistakes if two generators of noise are coordinated and develop an identical chaotic signal. The main problem of chaotic masking schemes is the noise generator coordination protocol. Noise intensity far exceeds the useful signal. In modern chaotic masking systems noise level exceeds signal level by 35-60 dB [1].

The transmission of additional parameters is used to match noise generators. The parameter matching process is carried out to synchronize the chaos generators. The quality of the signal transmission is significantly reduced when transmitted over noisy channels. Random noise cannot be subtracted from the mixed signal. The second major problem is the out-of-sync of generators when errors occur [2–4]. Out-of-sync occurs when the parameter exchange protocol is violated. In a chaotic masking scheme, the message is transmitted by an analog signal. Digital signals are easily detected.

The use of orthogonal chaotic signals is one possible approach to a chaotic masking scheme. Этот подход называется DCSK (Differential Chaos Shift Keying) [5]. Orthogonal chaotic signals are
produced by conventional noise generators. Various orthogonal transformations are applied to these signals: Hilbert [6-8], Gram-Schmidt [9-11] or Walsh [12-14]. This approach is characterized by low throughput. One frame contains one bit. In articles [15,16] random masking scheme with coding of a signal based on a family of orthogonal functions is suggested. A computer experiment was conducted with simple trigonometric functions. This article provides a comparative study the various orthogonal functions families for encoding the transmitted message.

2. Encoding scheme

Digital messages consisting of zeros and ones are encoded in this scheme. Let the message is broken into frames $M$. We will consider coding one frame. All frames are encoded in the same way. The length of one frame is $n$ bits.

$$M = b_0 b_1 ... b_n.$$ 

Design a function for the message

$$F(t) = \sum_{i=0}^{n} c_i f_i(t).$$

In this function, the coefficients $c_i$ are calculated based on the bits of the message $b_i$.

$$c_i = 2b_i - 1 \ (i = 1, ..., n).$$

For $b_i=0$ we have $c_i=-1$. For $b_i=1$ we have $c_i=1$. $f_i(t) (i=1, ..., n)$ – the family of orthogonal functions in interval $[a, b]$, $t$ – time axis. The condition of the orthogonality is

$$\int_{a}^{b} w(t) f_i(t) f_j(t) dt = \delta_{ij},$$

$$\delta_{ij} = \begin{cases} 0, & i \neq j, \\ 1, & i = j. \end{cases}$$

$w(t)$ - weight function.

The message decoding is based on the functions orthogonal property. By calculating the projections of function $F(t)$ on the functions $f_i(t)$, we will determine original message bits. Let ‘s define the auxiliary coefficients $d_i$. 

2
\[ d_i = \int_{a}^{b} w(t) F(t) f_i(t) dt. \]

Substituting in this relation the expression for function \( F(t) \) we gives the equality between \( d_i \) and \( c_i \).

\[ d_i = \sum_{j=0}^{n} c_j \int_{a}^{b} w(t) f_j(t) f_i(t) dt = \sum_{j=0}^{n} c_j \delta_{ij} = c_i. \]

We use these equals for chaotic signal masking. We add the chaotic signal \( G(t) \) to the useful message \( F(t) \).

\[ G(t) = F(t) + H(t). \]

We divide the mixing signal \( G(t) \) into orthogonal functions \( f_i(t) \).

\[ e_i = \int_{a}^{b} w(t) G(t) f_i(t) dt. \]

By substituting the expression for \( G(t) \), we get the ratios for the coefficients \( e_i \) and \( d_i \).

\[ e_i = d_i + h_i, \]

\[ h_i = \int_{a}^{b} w(t) H(t) f_i(t) dt. \]

For a true random signal \( H(t) \), the coefficients \( h_i \) must be zero.

\[ h_i = 0 \ (i = 0, \ldots, n). \]

As a result, the coefficients \( e_i \) will be equal both \( d_i \) and \( c_i \).
For implementing this scheme, it is necessary to perform automatic integration. The simplest approach is to implement numerical integration on the receiving side. To do this, one of the numerical integration schemes must be implemented. The transmitting side generates an analog signal. The receiving side determines the value of the signal at discrete times with a step $k$.

$$G_j = G(a + jk), \ (j = 0, \ldots, s, s = \left\lceil \frac{b-a}{k} \right\rceil).$$

The $e_i$ coefficients are then determined using the numerical integration rectangle method.

$$e_i = \sum_{j=0}^{s} w(a + jk) G_j f_i(a + jk).$$

For the coefficients $d_i$ and $h_i$ will be write similar equalities.

$$d_i = \sum_{j=0}^{s} w(a + jk) F_j f_i(a + jk).$$

$$h_i = \sum_{j=0}^{s} w(a + jk) H_j f_i(a + jk).$$

$$F_j = F(a + jh), \ (j = 0, \ldots, s, s = \left\lceil \frac{b-a}{h} \right\rceil).$$

$$H_j = H(a + jh), \ (j = 0, \ldots, s, s = \left\lceil \frac{b-a}{h} \right\rceil).$$

Random noises are possible in the communication channels. Numerical integration has calculation errors. Therefore, a large number of coefficients $h_i$ will be different from zero. A threshold scheme must be used to calculate the original message coefficients.
\[ c_i = \begin{cases} 1, & e_i \geq 0, \\ 0, & e_i < 0. \end{cases} \]

The integral calculation accuracy depends on the selected step \( k \). But as step \( k \) decreases, the amount of computation increases. The message rate is reduced.

3. Computer experiment

The message transmission errors rate was calculated in a computer experiment. Two orthogonal functions families were tested.

The first orthogonal functions family was based on simple trigonometric functions.

\[ f_j(t) = \sqrt{2} \cos(\pi jt). \]

The weighting function is \( w(t) = 1 \) for this functions family. Orthogonality interval is \([0,1]\).

The second orthogonal functions family was based on Lagrange polynomials.

\[ f_0(t) = 1, \quad (j + 1) f_{j+1}(t) = (2j + 1) x f_j(t) - df_{j-1}(t). \]

The weighting function is \( w(t) = 1 \) for this functions family. Orthogonality interval is \([-1,1]\).

An example the relationship between a useful signal and a masking signal is shown in Figure 1.

One byte messages between 0 and 255 were encoded. Random noise was generated based on a linear congruent generator. The useful signal amplitude was equal one. The noise amplitude was equal 100. The sampling step \( k \) varied from 0.0001 to 0.001. The Hamming distance was calculated between the original and decoded message. The average Hamming distance for all messages was determined.
Figure 1. Masking (black) and useful (red) signal. Amplitude of nose equal is 100.

The average Hamming distance dependence on the sampling step for the three test orthogonal functions families for noise amplitude 100 is shown in figure 2.

![Graph](image)

Figure 2. The average Hamming distance dependence on the sampling step for the three test orthogonal functions families at a noise amplitude of 100. (a) Trigonometric functions. (b) Lagrange polynoms.

From the graph, it can be concluded that orthogonal polynomials are inferior to simple trigonometric functions. Decoding errors when using orthogonal polynomials are significantly greater.

4. Conclusion

In this article the chaotic signal masking scheme based on orthogonal functions families is investigated. A computer experiment has shown that the use a simple trigonometric functions is preferable in this scheme. Orthogonal polynomial families have less resistance to external noise.
References

[1] Downes P T 1993 SPIE 2038 227
[2] Perez G and Cerderia H A 1995 Phys Rev Lett 74 1970
[3] Short K M 1996 International Journal of Bifurcation and Chaos 6 2 367
[4] Ponomarenko V I and Prokhorov M D 2002 Phys Rev E 66 026215
[5] Kolumban G, Vizvari G K, Schwarz W and Abel A 1996 Proc. Intern. Workshop on Non-linear Dynamics of Electronic Systems 92
[6] Galias Z and Maggio G M 2001 IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications 48 12 1510
[7] Kaddoum G 2016 IEEE Trans. Commun. 64 1 249
[8] Yang H, Tang W K S and Chen G 2016 IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications 63 1 146
[9] Wren T J and Yang T C 2010 IET Communications 4 6 739
[10] Wang L, Cai G and Chen G 2015 IEEE Transaction on Wireless Communications 14 9 5197
[11] Kaddoum G, Soujerti E, Arcila C and Eshteiwi K 2015 IEEE Transactions on Circuits and Systems II: Exp. Briefs 62 9 901
[12] Xu W K, Wang L and Kolumban G 2011 International Journal of Bifurcation and Chaos 21 3 799
[13] Huang T, Wang L, Xu W and Lau F C 2016 IET Communications 10 10 1189
[14] Escribano F J, Kaddoum G, Wagemakers A and Giard P 2016 IEEE Trans. Commun. 64 5 2066
[15] Belim, S.V and Rakitskiy Y S 2019 Informatsionno-Upravliaiushchie Sistemy 2 76
[16] Belim S V and Larionov I B 2020 Journal of Physics: Conf. Series. 1441 012034