2004 International Symposium on Nonlinear
Theory and its Applications (NOLTA2004)
Fukuoka, Japan, Nov. 29 - Dec. 3, 2004

A Chaos-Based Error Detection Code For Data Communication

H.S. Kwok and Wallace K.S. Tang

Department of Electronic Engineering, City University of Hong Kong,
Tat Chee Avenue, Kowloon, Hong Kong
Email: hskwok, kstang@ee.cityu.edu.hk

Abstract– In this paper, a novel chaos-based error detection coding scheme is proposed. The checksum is generated by a discrete chaotic map so that transmission errors can be detected. Additional advantage in using chaos for error detection code is that a keyed feature can be easily embedded and the generated code is ready to use for message authentication in data communication, such as IEEE802.11 wireless communication. The design of the algorithm is presented and the performance analyses on error detection and authentication are discussed.

1. Introduction

Error detection codes or error controlling codes have been widely used in various areas, such as high-speed computer memory storage, digital audio/video transmission, data communication and so on [1]. By introducing the redundancy to the original data, error in the transmitted message can be detected or even corrected. The most popular scheme is cyclic redundancy check (CRC) [2].

The usage of CRC has recently been extended for the purpose of authentication in wireless communication, in particular IEEE802.11 protocol [3]. Although CRC is strong in error detection, it may not be good enough to resist the attacks, such as impersonation and substitution, due to its linearity property. Its weaknesses have been found and reported in [4, 5], and various ways are possible in altering a message without being detected.

In this paper, a novel chaotic error detection code (CEC) is proposed. With the distinct properties of a chaotic map, such as ergodicity, quasi-randomness, sensitivity to initial conditions and system parameters, the proposed CEC not only provides the required error detection ability but also serves the authentication purpose in data communication. Although many cryptosystems have been developed based on the diffusion and confusion properties of chaotic systems in the past decade [6], its use in error detection and authentication code is firstly studied in this paper.

The organization of this paper is as follows. The CRC is briefly revisited in Sect. 2. In Sect. 3, the design of CEC is explained in detail. Served as an error detection code, its performances in detecting single-bit, double-bit and burst errors are reported in Sect. 4. The security provided by the CEC is studied in Sect. 5. Finally, conclusion is given in Sect. 6.

2. Cyclic Redundancy Check

The CRC is one of the main techniques in providing the error detection in data communication. Based on some standard generator polynomials, *g(x)*, such as

CRC-12 : $x^{12}+x^{11}+x^3+x^2+x^1+1$

CRC-16 : $x^{16}+x^{15}+x^2+1$

CRC-CCITT : $x^{16}+x^{12}+x^5+1$

ETHERNET : $x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^8+x^7+x^5+x^4+x^2+x+1$

valid codeword can be obtained by the following equation:

$$v(x) = u(x)g(x) \qquad (1)$$

where $v(x)$ and $u(x)$ are the polynomials representing the $(m+c)$-bit codeword and m-bit message, respectively; $g(x)$ is a pre-defined c-degree polynomial given before. Based on the fact that the codeword *v(x)* should be divisible by $g(x)$, error can be detected if that's not the case.

There are many characteristics that make CRC attractive, and they are summarized as follows:

1) all single bit errors can be detected;
2) most double bit errors can be detected;
3) all odd number of bit errors can be detected;
4) all burst errors with *length* ≤ *degree of* $g(x)$ can be detected.

Recently, CRC is further adopted in the Wired Equivalent Privacy (WEP) in IEEE 802.11b wireless network for verifying the data integrity. Although CRC is powerful in error detection, using it as a secure code is not recommended. According to some researches [4, 5, 7], it is possible to modify the message without being detected by CRC in WEP. Therefore, in this paper, a novel way is proposed in designing a secure error detection code for authentication purpose.

3. Chaos-Based Error Detection Code

3.1. Discrete Chaotic Map

Chaotic maps are usually described in difference equations or recurrence relations. Despite of their simple forms, complex dynamics that fall between stochastic and deterministic behavior are reported. The chaotic features, such as ergodicity, quasi-randomness, sensitivity dependence on initial conditions and system parameters,

are suggested to be advantageous for the construction of cryptosystems [6]. Over the past decade, we can witness many attempts to apply the chaotic dynamics and many chaos-based cryptosystems have been proposed [6].

In this paper, an entire new application is suggested. A chaos-based error detection code, called CEC, is proposed and designed to achieve error detection and also data authentication.

A two-dimensional discrete chaotic map, the Arnold's Cat Map [8], is adopted in the coding scheme. A generalized discrete Cat Map [9] can be formulated as

$$s_{k+1} = f_p(s_k) = A_p s_k \bmod 2^l \tag{2}$$

where $s_k = [x_k, y_k]^T$, $p = (a, b)$ and $A_p = \begin{bmatrix} 1 & a \\ b & 1+ab \end{bmatrix}$ with x_k, y_k, a, b being integers in $[0, 2^l - 1]$. An important feature of the map in (2) is that its determinant is equal to 1 and so it is area-preservative or one-to-one mapping.

3.2. Design of CEC

Assuming *M* is a packet with *m*-bit long, *C* is the CEC checksum with *c*-bit long and *K* is the secret key. The procedures for generating *C* from *M* are as follows:

For any message *M*,

1. If *m* is not divisible by *c*, append sufficient number of zeros, say *r* zeros, at the end of *M*. The padded message, *M'*, is with *m'*=(*m*+*r*) bit length where *mod(m',c)=0*.
2. Partition *M'* into data blocks such that each block, s_i, is in *c*-bit long, where $\bigcup_{i=1}^{q} s_i = M'$, $s_i \cap s_j = \varnothing$ $(i \neq j)$ with $q = \frac{m'}{c}$ is the total number of blocks.
3. A group of parameters, $P = \{p_1, p_2, \cdots, p_q\}$ is to be generated, where $p_i = (a_i, b_i)$ is the parameter of f_{p_i} in the *i*-th Cat map, as defined in (2). Firstly, the secret key *K* is decoded into 2 pairs, where the first pair specifies a Cat map and the next pair is considered as an initial point. With this initial point, *q* surrounding points are selected to be the initial values of the derived Cat map. Through iterations (in our design, 1000 iterations are used.), *P* can then be obtained with $p_i \neq p_j$ ($i \neq j$) due to the one-to-one mapping property.
4. Each data block, s_i, is transformed to s_i' with the *i*-th Cat map where $s_i' = f_{p_i}^t(s_i)$ with some positive integer *t* (*t=100* in our case), and $f_{p_i}^t(s_i) = f \circ f_{p_i}^{t-1}(s_i)$.
5. The checksum *C* is obtained by XOR all the blocks in $S' = \{s_1', s_2', \cdots, s_q'\}$, i.e. $s_1' \oplus s_2' \oplus \cdots \oplus s_q'$.
6. Append *C* to *M* to form a codeword *W* of (*m* + *c*)-bit long for transmission.

According to the above procedures, each data block will be transformed by a distinct Cat map, whose parameters are key-sensitive. If the number of iterations, *t*, is sufficient, the relationship between the original and the transformed data blocks will be confused. With such a keyed property, the attacks, such as impersonation and substitution, can be resisted since the key is unknown to the forger.

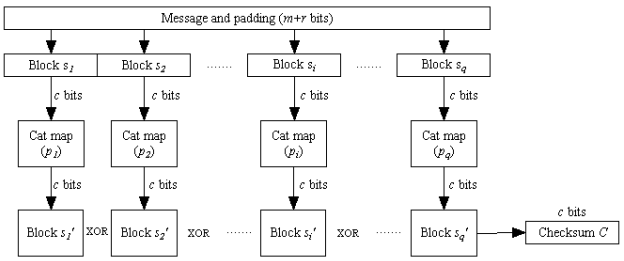

Fig. 1. The block diagram of the proposed CEC.

The generated codeword *W* is then sent through a communication channel. When it is received, the transmission error and the integrity of the message can be verified with the following procedures:

1. Remove the last *c* bits from *W* and label it as *C*.
2. Label the first *m* bits of the received message as $\hat{M}$.
3. Generate the checksum $\hat{C}$ with $\hat{M}$ and the secret key *K*, by the procedures described before.
4. Compare the calculated checksum $\hat{C}$ with the received checksum C. The codeword, *W*, is considered to be valid if $\hat{C} = C$.

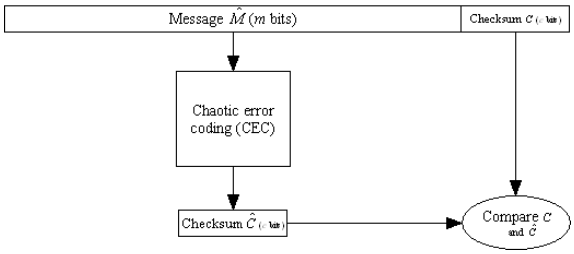

Fig. 2. Block diagram of the CEC message authentication.

4. Error Detection Analysis

The effectiveness of the proposed CEC in error detection is analyzed under the conditions of single bit, double bit and burst errors in the transmitted codeword.

4.1. Single Bit Error

For single bit error, one bit in a particular single block, s_i, is changed. Due to the one-to-one mapping of discrete Cat map, the transformed result of this block, s_i', will be altered while the other s_j' $(i \neq j)$ remains the same. As a result, the checksum will be different from the original one after the XOR function. Hence, the

probability of detecting single bit error is 100%.

The distribution of the bit difference in the checksum due to the single bit error is studied. A hundred sets of messages are randomly generated, each with 1600-bit long. For each message, 32-bit checksum is generated based on a randomly-generated secret key. Performing an exhaustive test, all 1600 combinations of one-bit error are evaluated for every message and the resultant distribution of the bit difference in the checksum is shown in Fig. 3. The obtained mean, variance, maximum and minimum values of the bit difference are 15.886, 8.293, 29 and 4, respectively. It can be observed that the mean is close to the half of the checksum length, which is the best in terms of error detection.

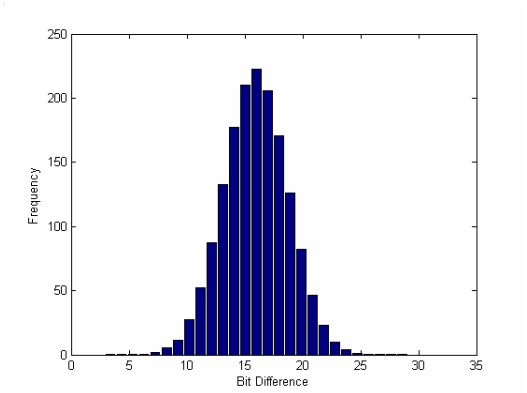

Fig. 3. Distribution of the bit difference of the checksum with single-bit error

4.2. Double Bit Error

For a double bit error, there are two possible cases:

1) *Both error bits fall in the same data block*: Similar to the case of single bit error, the checksum will be changed and such error is 100% detectable.
2) *The two error bits fall in two different data blocks*: In this case, the error may not be detectable if the two corresponding transformed blocks, s'_i and s'_j ($i \neq j$), have the same changes in the bit pattern.

Assuming that

1) the distribution of the bit difference for a single bit error is normal with the mean and variance obtained in Sect. 4.1, and
2) the probability distribution of the patterns for each kind of bit difference is uniform,

the probability of the error detection for the case (2) can be estimated as 99.999999976694%.

The distribution of the bit difference under the situation of double bit error is obtained with a test similar as before. A hundred sets of message are randomly generated and all the combinations of double bit error are injected into every message. The bit differences of the resultant checksum and the original one are recorded, and the distribution is depicted in Fig. 4. The mean, variance, maximum and minimum value of the distribution are 15.994, 8.011, 30 and 0, respectively. Once again, the mean is about half of the bit length of the checksum. If it is assumed that the distribution in Fig. 4 is normal, the probability of the error detection for double bit error is 99.99994%, which is close to our previous calculation.

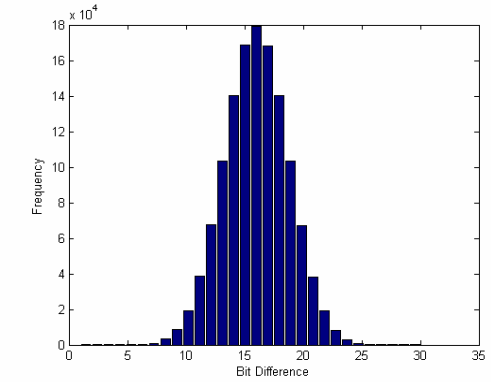

Fig. 4. Distribution of the bit difference of the checksum with double bit error

4.3. Burst Error

For burst error, it is assumed that the bit length of the burst error is less than or equal to the bit length of a data block. Then, there are two possible cases:

1) *The error bits caused by burst error fall in a single data block*: Similar to the case of single bit error, there will always be some changes in the checksum, and hence this situation is 100% detectable.
2) *The error bits caused by burst error fall in two data blocks*: Similar to the second case in double bit error, it may not be detectable if the two corresponding transformed blocks, s'_i and s'_j ($i \neq j$), have the same changes in their bit patterns.

Again, the distribution of the bit difference caused by 32-bit burst error is plotted in Fig. 5. The mean, variance, maximum and minimum value of the distribution are 15.993, 7.992, 28 and 5, respectively. Under the assumption of normal distribution, it is estimated that any burst error can be detected with a probability of 99.99994%.

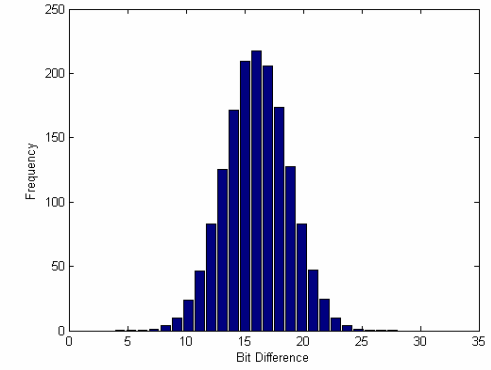

Fig. 5. Distribution of the bit difference of the checksum with burst error

4.4. Comparison with CRC

As observed in the above experiments, the distributions of the bit difference in all the studied cases are close to normal distribution with mean equal to the half of the bit length of the checksum. It indicates the randomness of the checksum which is obviously favorable for security purpose. In conclusion,

1) The probability in detecting any single bit error is 100% which is as powerful as the traditional CRC.
2) Double bit error detection probability is estimated to be 99.99994% which is good enough in practice, though worse than CRC.
3) Burst error detection probability is 99.99994%. The result is inferior to CRC which is 100% in this case.
4) The mean of the bit difference is half of the bit length of the checksum which is favor for error detection especially when the bit error is occurred in the checksum instead of the data blocks.

5. Security Analysis

In this section, some security analyses on the proposed CEC scheme are performed. Firstly, the correlation between the secret key and the Cat map parameters is studied. A number of keys, K_i are randomly generated and used to form the corresponding parameters P_i. The correlation coefficient between K_i and P_i is then calculated to study their linear relationship. It is known that the smaller the correlation coefficient is, the weaker the linear relationship. From our study, the mean correlation coefficient is found to be 0.01596, which is comparable with the correlation coefficient (0.011085) of randomly-generated data using the *rand()* function in C-language.

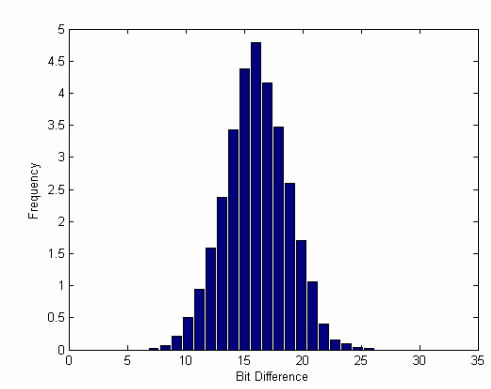

Fig. 6. Distribution of the bit difference of the checksum with one-bit change in the secret key.

Secondly, the relationship between the secret key and the calculated checksum is verified. By altering a single bit in the secret key, the distribution of the bit difference in the checksum is shown in Fig. 6. It can be observed that it is close to a normal distribution, and the mean, variance, maximum and minimum value of the distribution are 16.041, 7.962, 26 and 4, respectively.

To avoid attackers, there should not be any linear relationship between the secret key and the checksum, otherwise, the resistance against attacks will be greatly reduced. The correlation coefficient between key and the checksum is calculated as 0.009837, which again demonstrates their weak linear relationship.

6. Conclusions

In this paper, a novel chaos-based error detection code scheme is proposed for error detection and data authentication. The effectiveness of this proposed scheme is analyzed. Although its capability of error detection may not be as good as CRC, it outperforms CRC since the distribution of the bit differences is normal, having the mean equal to half bit length of the checksum. In addition, the embedded keyed-feature is important for the data authentication, in particular useful for wireless communication.

Acknowledgements

The work described in this paper was fully supported by a grant from the Research Grants Council of the Hong Kong Special Administrative Region, China (Project No. CityU 1157/03E).

References

[1] D.J. Costello, Jr., J. Hagenauer, H. Imai and S.B. Wicker, "Applications of error-control coding," *IEEE Trans. Information Theory*, vol. 44, no. 6, pp. 2531-2560, Oct 1998.

[2] T. V. Ramabadran, S. S. Gaitonde, "A tutorial on CRC computations"**,** *IEEE Micro,* vol.8, issue 4, pp.62-75, Aug. 1988.

[3] IEEE, *Wireless LAN Medium Access Control (MAC) and Physical Layer Specifications*, IEEE standard 802.11 1999 Edition, 1999.

[4] N. Borisov, I. Goldberg and D. Wagner; "Intercepting mobile communications: The insecurity of 802.11," *ACM Int. Conf. on Mobile Computing and Networking***,** Jul. 2001.

[5] J. R. Walker, "Unsafe at any key size; an analysis of the WEP encapsulation," *IEEE Document* 802.11-00/362, Oct. 2000.

[6] L. Kocarev, "Chaos-based cryptography: A brief overview," *IEEE Circuits and Systems Magazine*, vol.1, issue 3, pp.6-21, 2001.

[7] J. Williams, "The IEEE 802.11b security problem. I**,"** *IT Professional*, vol.3, issue 6, pp.96–95, Nov 2002.

[8] V. I. Arnold and A. Aver, *Ergodic problems of classical mechanics*, Benjamin, New York, 1968.

[9] G. Chen, Y. Mao and C. K. Chu, "A symmetric image encryption scheme based on 3D chaotic maps," *Chaos, Solitons and Fractals*, vol.21, pp.749-761, 2004.