Encryption model of network information based on AES algorithm with dimension reduction chaos optimization

Yong Wu

College of Information Science and Engineering, Hennan University of Technology, Zhengzhou 450052, Henan

Defa Hu*

School of Computer and Information Engineering, Hunan University of Commerce, Changsha 410205, Hunan, China

**Corresponding author (E-mail:hdf666@163.com)*

Abstract
According to the standard AES algorithm has low encryption performance in the application of the network information encryption, this paper proposes a network information encryption model which based on AES algorithm with dimension reduction chaos mapping optimization. First, Ant colony algorithm is introduced to dimension, and the pheromone of ant colony algorithm is weighted controls. Then the improved ant colony algorithm is adapted to chaotic mapping to optimize dimension reduction, and enable the chaos optimization algorithm in the current optimal solution, namely the near global optimal ants do chaotic search. Finally dimension reduction chaos mapping is adopted to optimize the safety of AES algorithm. Simulation experiments show that compared standard AES algorithm, the proposed based on AES algorithm with dimension reduction chaos optimization encryption model of network information has good cryptographic properties.

Key words: CHAOS AES ALGORITHM, CHAOTIC MAPPING, WEIGHT CONTROL, NETWORK INFORMATION ENCRYPTION

Introduction

With the coming of information age, people’s work, study and life dependence on information technology has reached the unprecedented level. Now, most countries in the world are highly dependent on the communication network, including the government affairs, national defence, finance, commerce and industry and so on various aspects of social life in [1]. However, the greater our dependence on information technology, the greater the risk caused by the steal information, tampering with data, hacker attacks, the spread of the virus as well as a variety of network attacks, the security of network information transmission faces huge challenges [2] Strengthen the network information security is a priority, ensure the security of information network transmission of the core is to realize information confidentiality, integrity, and authentication.

Along with the rapid development of computer technology, the cryptography has been expanding rapidly, such as DES, 3DES, RSA and so on, but these methods have certain limitations and vulnerability. Lorenz equation is mentioned by John M.Carroll, Jef Verhagen and Perry T.Wong for generate pseudo random sequences, and the sequence as a sequence of password key [3] They have pseudo random test of the chaos sequence , and put forward the sequence within a certain range of parameters have good pseudo randomness, but the points listed here have the chaotic characteristics only in the case of two or three dimensional. In the study of chaotic block cipher, T.Habuts propose that using chaotic inverse system method , such as in the scenario, the use of Tent map of piecewise linear mapping [4]. But the piecewise linear tent map was flawed, so E.Biham with chosen-ciphertext attack and known plaintext attack breached the Habutsu‘s scheme [5]. Also there are researchers introduce some methods of traditional cryptography, such as L.Kocarev and others used the S - box which is just by introducing chaos system to construct the traditional password [6]. Toshiki Habutsu published a "password of chaos", and puts forward the iterative encryption model form is chaotic password is common, this paper raised a hot wave of chaotic cipher research [7]. Su Yong will put forward a kind of Encryption algorithm combining chaos and DES (Data Encryption Standard) , it became the combination of the chaos and traditional cryptography typical [8]. Hu Fengjun put forward a kind of identity authentication scheme based on hyperchaos encryption; encryption effect is verified by image encryption [9]. The scheme is essentially static password an improved scheme, the basic idea is to the authentication information is encrypted, in the process of identity authentication of identity information decrypted. Liao Guangzhong put forward a kind of based on the PPTP (Point to Point Tunnel Protocol) chaotic authentication Protocol, is essentially the chaos dynamic password system. This paper has realized the dynamic password “once a secret”, but not analyzes the characteristics of the hash algorithm. He also put forward the design method of dynamic password chip based on Logistic mapping and implementation is a kind of using the challenge/response mechanism of the dynamic password generator hardware [10]. Liu Z, et published relevant articles about the chaos generated digital sequence, which laid a foundation for constructing chaotic hash function [11]. K.W.Wong proposes an algorithm that combines encryption and Hash function [12].

According to the defects of standard AES algorithm in the application of the network information encryption, this paper proposes an encryption model of network information which based on AES algorithm with dimension reduction chaos mapping optimization.

Performance Analysis of AES Encryption Algorithm

AES algorithm using the symmetric block cipher system, the encryption and decryption keys are the same. The encryption method is:

$$s'(x) = c(x) \cdot s(x) \bmod (x^4 + 1) \qquad (1)$$

$$c(x) = \{03\} \cdot x^3 + \{01\} \cdot x^2 + \{01\} \cdot x + \{02\} \qquad (2)$$

Among them, $s(x)$ is the original state, $s'(x)$ is after the transformation of state, $\{\}$ is the number of bytes.

$$s'(x) = s'_{0,c} + s'_{1,c} \cdot x + s'_{2,c} \cdot x^2 + s'_{3,c} \cdot x^3 \qquad (3)$$

$$s(x) = s_{0,c} + s_{1,c} \cdot x + s_{2,c} \cdot x^2 + s_{3,c} \cdot x^3 \qquad (4)$$

$s'_{0,c}$ means the constant terms’ coefficient which multiply by $c(x)$ and $s(x)$ and merge $\bmod(x^4 + 1)$. Make use of $x^i \bmod(x^4 + 1) = x^{i \bmod 4}$, we can obtain equation (5).

$$s'(x) = \{02\}s_{0,c} + \{03\}s_{1,c} + \{01\}s_{2,c} + \{01\}s_{3,c} \qquad (5)$$

The rest of the items can be similar, so equation (1) using matrix is expressed as:

$$\begin{pmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{pmatrix} \qquad (6)$$

The column mixing transform is equivalent to the intermediate state data according to the column left multiply by a constant matrix.

To understand the performance of AES password, we make a comparative analysis of it and the RSA key.

RSA algorithm is representative of the public key encryption algorithm, the algorithm using basic knowledge of number theory, its security is based on large integer factoring this math problem, protects against all the passwords so far known attacks, compared with the symmetric key encryption algorithm, increased the function of digital signature. The RSA algorithm has basic characteristics of the public key system, such as:

1) If use PK (public key) to encrypt p (plaintext), then using SK (private key) to decrypt can recover p, namely

$$P = D_{SK}[E_{PK}(P)] \quad (7)$$

2) The encryption key PK can only be used for encryption, cannot decrypt.

$$D_{SK}[E_{PK}(P)] \neq P \quad (8)$$

3) It cannot be deduced from the known PK to SK

4) Encryption arithmetic and decryption operation can swap, namely

$$E_{PK}[D_{SK}(P)] = P \quad (9)$$

As known from the characteristics, in the public key encryption system, PK as a public key can be sent to the users, when the sender A want to send plaintext p to the receiving party B , just look up to the receiving party B's public key PKB from the PK , and use the encryption algorithm E to encrypt plaintext p, can get the ciphertext $C = E_{PKB}(P)$. In the receiving party B after receiving the ciphertext C, using only oneself know the decryption key SKB decryption, can recover the plaintext $P = D_{SKB}[E_{PKB}(P)]$. For any eavesdropper even if intercepted ciphertext C, because do not know SKB, is also unable to recover the plaintext.

RSA system depends on the theoretical basis of the famous Euler's theorem: two positive integers a and n are prime numbers, there are $a^{\phi(n)} = 1(\mathrm{mod}\, n)$, among them, $\phi(n)$ is the number of positive integers that relatively prime to n, and less than n. The cores of the RSA public key technology are as follows:

1) p and q are two large enough of prime number (decimal number more than 100), p and q are confidential.

2) Computing $n = pq$, n is public (to get the p and q by factorings n extremely time-consuming).

3) To get the Euler function of n $z = \phi(n) = (p-1)(q-1)$.

4) Selecting integer e under the condition of $[e, z] = 1$, e and $\phi(n)$ relatively prime, e is public.

5) Computing the d which meets the $de = 1(\mathrm{mod}\, z)$, and d is confidential.

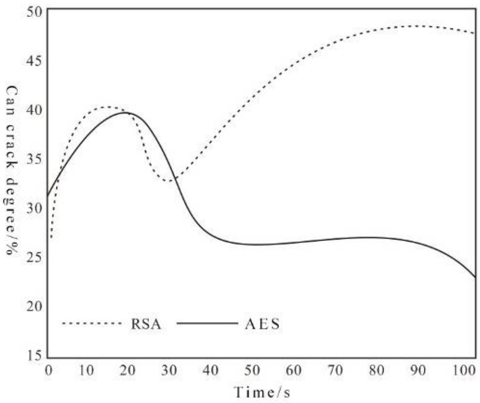

Figure 1. Encryption performance comparison between RSA algorithm and AES algorithm

Seen from the figure 1, compared with RSA encryption algorithm, AES algorithm has good encryption performance, but it cannot achieve high precision encryption requirements.

AES Encryption Algorithm Based on Chaos Optimization

The dimension optimization of the chaotic mapping

Before using the chaotic mapping to optimize the AES encryption algorithm, first, we do optimize to dimension reduction according to the defects of too long operation time of the chaotic mapping.

After reconstruction for the time series $\{X(t)\}$ $t = 1, 2, ..., N$ we obtain phase space state vector:

$$X(t) = \{x(t), x(t-\tau), ..., x[t-(m-1)\tau]\} \quad (10)$$

According to the given data structure mapping function F, make the future state $X(t+1)$ and current states $X(t)$ meet:

$$X(t+1) = F(X(t)) \quad (11)$$

Among them, the criterions of the mapping function F for the minimum value as following equation.

$$\sum_{t=0}^{N} \left\{ X(t+\eta) - F(X(t)) \right\}^2 \quad (12)$$

In the process of phase space reconstruction, if the dimension is low, the general can be directly used to simulate global high order polynomial; And for high dimensional phase space, its computational complexity multiplied, generally USES the typical regression analysis model to minimize the amount of calculation:

$$x(t+1) = \sum_{i=1}^{d} a_i x(t+1-i) + k\varepsilon_t \quad (13)$$

In the equation, ε_t is Gaussian random variable, and obey the standard normal distribution $N(0,1)$; k is stochastic intensity constant factor, usually takes $k=\sqrt{E_d/(N-d)}$; a_i can be obtained by time sequence itself. To ensure that the influence of random input part of the system as small as possible, require that a_i meet minimal system error sum of squares;

$$E_d=\sum_{t=d}^{N}\left[x(t)-\sum_{i=1}^{d}a_i x(t-i)\right]^2 \qquad (14)$$

Partial derivatives and makes the result to zero for a_i,

$$\sum_{i=1}^{d}a_i\left[\sum_{t=d}^{N}\left[x(t-i)x(t-j)\right]\right]=\sum_{t=d}^{N}\left[x(t)x(t-j)\right] \qquad (15)$$

After deformation,

$$\sum_{i=1}^{d}a_i C(i-j)=C(j) \qquad (16)$$

In the equation, $C(i-j)$ and $C(j)$ are autocorrelation function, so obtain coefficient a_i. Ant colony algorithm is introduced to dimension, and the pheromone of ant colony algorithm for weight control.

When there is a new node i into the model, the node i needs to inform its parameters to all neighbour nodes, neighbor node to add a new directory, can jump digital section is set to 1. The initial pheromone of v_{ij} and is relate to comprehensive weighting factor e_i and e_j of the node i and node j. On the initial pheromone of v_{ij} as follows:

$$\tau_{ij}(0)=e_i\cdot e_j \qquad (17)$$

In this paper, after based on a path of initialized pheromone, pheromones are normalized processing, mainly to adjust before after one iteration path pheromone and the weights between the pheromone increment iteration paths.

In improved ant colony algorithm, the ant routing mechanism is for: first according to $tabu_k$ and AT_k to choose the next nodes collection $next_k$, then according to the forwarding probability

$$p_{ij}^{k}(t)=\frac{\tau_{ij}^{\alpha}(t)\cdot\eta_{ij}^{\beta}(t)}{\sum_{u\in next_k}\tau_{iu}^{\alpha}(t)\cdot\eta_{iu}^{\beta}(t)} \qquad (18)$$

Select the next hop nodes j. If $next_k$ is null set, means the selectable hop nodes is null, Ant in the node is “die” and no longer forward.

To control the number of ants in the network, an ant carry a survival time field (T), every node of the field value minus 1. When $T=0$, ants no longer forward. Setting the appropriate value T can be set the scope of the ant routing. The T is small, the search range is small, whereas the T is larger, the ant search scope is bigger.

Then, the improved ant colony algorithm is adopted to optimize the chaotic mapping, after search optimal individual ants pheromone update for equation (19).

$$\begin{aligned}c_i&=\varepsilon_i p_{1i}\\&=(1-\varepsilon_i)p_{2i}\end{aligned} \qquad (19)$$

p_{1i} as the optimization probability of the ants initial value p, ε_i random number in $[0,1]$.

$$c_i'=c_i+\varepsilon_i\lambda_i\exp[-\gamma(t-1)^{\beta}/\omega] \qquad (20)$$

t is the current number of iterations, is maximum step of interval i of variable x_i. β and ω are the parameters of the attenuation rate control nonlinear step length. ε_i and γ are random numbers on $[0,1]$.

$$\tau(c)=1/n\sum_{i=1}^{n}[\varepsilon_1\tau_{p1}+(1-\varepsilon_i)\tau_{p2}] \qquad (21)$$

After using chaotic sequence to produce several test point traverse the entire search interval, initial colony according to each region of the area of the optimal value to determine the initial pheromone, the algorithm can also make use of the chaos system to produce a large number of test point work as an ant, ant colony based on information in different areas of the work content through the chaos algorithm in optimal ants are randomly selected by the corresponding argument around again to search, find out the new optimal solution. So, find the global optimal solution in a specified number of iterations.

Therefore, the chaotic mapping based on improved ant colony algorithm, the basic steps are as follows:

1) Initialize the set number N of iterations and optimal number of ants m.

2) Put m ants in search range, path to search for each variable.

3) To perform global search process, completely bureau to a search path analysis, the ants and pheromone update path.

4) Pick out the global optimal ants.

5) Into the ant colony optimization and local search process, make the ants quantity along with the increasing of the number of iterations and contraction after attenuation to the global search, and update the pheromone.

6) Enable chaos optimization algorithm in the current optimal solution, namely the near global optimal ants do chaotic search, if found due to the current best solution of the solution, replacing the original optimal solution.

7) If the m ants have not finished analysis, skip to step (3).

8) Pheromone update to the passed route of every ant.

$$\tau_k \leftarrow \rho \cdot \tau_k + \Delta\tau_k, \Delta\tau_k \leftarrow 0 \tag{22}$$

9) If iteration, skip to step (2).

10) All the end of the iteration, the output value mapping.

AES encryption algorithm based on dimension reduction of chaotic mapping

Then, the dimensionality reduction chaotic mapping is used to AES algorithm to optimize the safety and encryption, specific methods as shown in the figure below.

Then, the dimensionality reduction chaotic mapping is used to AES algorithm to optimize the safety and encryption, specific methods as shown in the figure below.

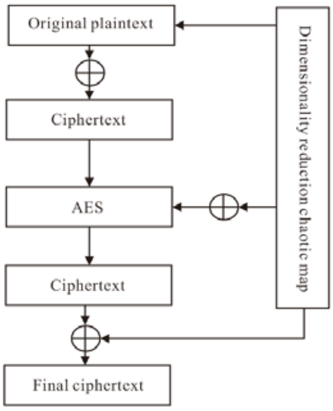

Figure 2. AES encryption algorithm based on dimensionality reduction chaotic map

As shown in the figure, the improved algorithm is divided into four steps:

1) First, the chaotic mapping iterative n times ($n > 200$), make chaotic system into stable attractor.

2) According to the bit, y_n and y_{n+1} xor this original plaintext, generate the initial ciphertext. 1.

3) Xor $x_n - x_{n+21}$ and $m_n - m_{n+21}$, we get chaotic sequence $k_n - k_{n+21}$ and AES encryption for ciphertext 1. With chaotic sequence directly instead of extended keys, the resulting ciphertext 2.

4) According to bit, xor ciphertext 2 and z_n , z_{n+1}, generate the final ciphertext.

Such a clear grouping encryption to complete, if to continuous encryption, it only need $n+22$ to replace n, repeat step (2) ~ (4).

Decryption steps are inverse operation of encryption: first, generate ciphertext 2 with xor cipher and z_n z_{n+1}; then $k_n - k_{n+21}$ used as extension key, to decrypt the ciphertext 2, generating ciphertext 1; finally ciphertext 1 xor with y_n and y_{n+1}, restore the original plaintext.

The Algorithm Simulation

To verify the effectiveness of the improved algorithm proposed in this paper, simulation experiments on it. The encryption and decrypt of image for example, the standard AES algorithm and the improved AES algorithm proposed in this paper are test image encryption and decryption operations. The result is shown below (figure 3 as the original image, figure 4 for the encrypted image, figure 5 is decrypted image)

Figure 3. Encryption original image

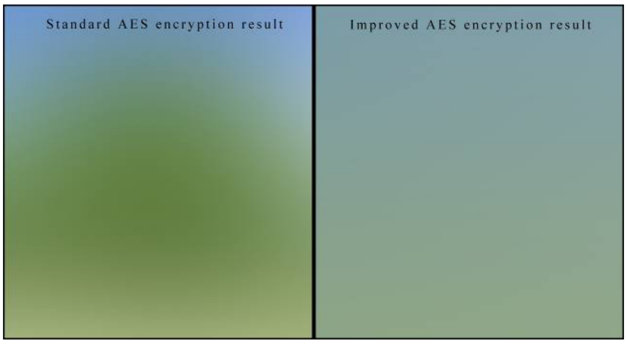
Standard AES encryption result
Improved AES encryption result

Figure 4. The result of two algorithms for the original image encryption

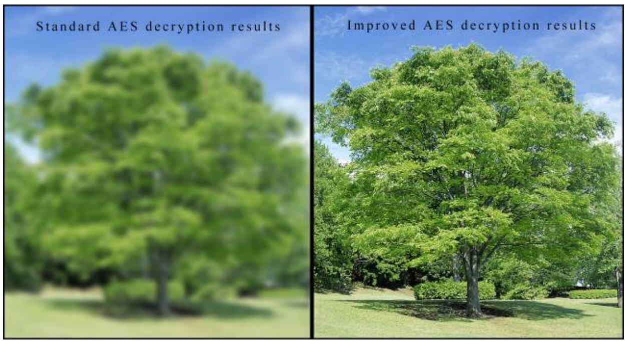
Standard AES decryption results
Improved AES decryption results

Figure 5. The results of two algorithms for decrypting the encrypted image

Seen from the simulation results, the proposed improved AES algorithm has better performance of the network information encryption.

Conclusions

Because the computer network has diversity form connection, inhomogeneity terminal distribution and openness and connectivity network features, the network is vulnerable to hackers, geek, malware and other malicious attacks. So the security and confidentiality of information on the Internet is a vital problem. According to the defects of standard AES algorithm in the network information encryption, this paper proposes a network information encryption model based on AES algorithm with optimization of dimension reduction chaos mapping. The simulation results show that the proposed improved model has better performance of encryption.

References

1. Yang Hong (2014) Research on Fusion Encryption Technology of Blended Security Network. *Bulletin of Science and Technology*, 30(10), p.p.175-177.
2. Tan Xueqin (2014) Design and Implementation of Encryption Positioning Module Based on Mobile Communication. *Tv Engineering*, 38(23), p.p.132-135.
3. Liu Yibo (2014) Network interconnection model based on trusted computing. *Journal of Computer Applications*, 34(7), p.p. 1936-1940.
4. LI Shuang (2014) Attribute-Based Public Encryption with Keyword Search. *Chinese Journal of Computers*, 37(5), p.p.1017-1024.
5. Qiu Guoqing (2014) AES algorithm-based encryption scheme for ZigBee networks. *Application of Electronic Technique*, 40(4), p.p.56-58.
6. Xiong Jinbo (2014) A Secure Self-Destruction Scheme for Composite Documents with Attribute Based Encryption. *Acta Electronica Sinica*, 24(4), p.p.366-376.
7. Xiong JinBo (2014) A Secure Self-Destruction Scheme with IBE for the Internet Content Privacy. *Chinese Journal of Computers*, 37(1), p.p.139-150.
8. Liu Zheli (2013) “Format-Preserving Encryption for PNG Image”. *Journal of Beijing Institute of Technology (Natural Science Edition)*, 33(12), p.p.1263-1268.
9. Hu Fengjun, Zhao Yanwei (2013) Comparative research of matching algorithms for stereo vision. *Journal of*

Computational Information Systems, 9(13),p.p.5457-5465.
10. Hu Fengjun (2013) A rapid eye-to-hand coordination method of industrial robots. *Journal of Information and Computational Science*, 10(5), p.p.1489-1496.
11. Lin Qing (2013) Simulation of Image Encryption Algorithm Based on Orthogonal Basis Function Neural Network. *Computer Simulation*, 30(10), p.p.416-421.
12. HE Yuan.(2013) Block encryption algorithm based on chaotic S-box for wireless sensor network. *Journal of Computer Applications*, 33(4), p.p.1081-1084.