MATEC Web of Conferences **31**, 15002 (2015)
DOI: 10.1051/matecconf/20153115002

A Novel Image Cryptosystem Based on S-AES and Chaotic Map

Lan BAI [1,a]

[1] *Chien-Shiung Wu Honors College, Southeast University, Nanjing, 210096, China*

Abstract. This paper proposes a novel scheme based on simplified advanced encryption standard (S-AES) for image encryption. Modified Arnold Map applied as diffusion technique for an image, and the key and dynamic S-box of encryption is generated by PWLCM. The goal is to balance rapidity and security of encryption. Experimental implementation has been done. This light encryption scheme shows resistance against chosen-plaintext attack and is suitable for sensor networks and IoT.

1 Introduction

Nowadays, the importance of data security is ever-growing in many fields of common life. As transmission of images through portable terminals and wireless networks becomes daily routine for people, the security of images becomes big concern of people. Consequentially, people demands efficient image encryption methods. Because of the large size of image, asymmetric cryptosystems, such as RSA[1], can hardly be directly used for image encryption. Besides, a number of symmetric image algorithms are developed, and AES is one of the most unbreakable one of them. However, the full execution of AES needs at least 10 iterations, and each of them consists of 4 functions. Therefore, AES is too heavy and slow to be adopted in sensor networks, Internet of Things and Zigbee[2]. S-AES (Simplified AES) is the reduced algorithm of AES[3]. The rapidity of S-AES meets the demands of the usages mentioned above, while S-AES is not secure enough.

In this paper, a novel symmetric key image algorithm is proposed to overcome the problems above. Based on chaotic maps, we introduce random phenomenon to enhance the weak function Substitution and the creation of initial key. For more robustness of the scheme, chaos is added to diffuse the image.

This paper is organized as followed: in the next section, AES and S-AES is briefly reviewed. In section 3, the theory of the chaotic maps that be used in our scheme is introduced. In section 4, the proposed algorithm is presented. In section 5, we analyse experimental results and the security of out algorithm, and in the last part, the conclusion is given.

2 AES and S-AES

AES is a new generation symmetric encryption algorithm proposed to supersede DES[4]. It was adopted by the USA government and now used worldwide. AES encrypts data in block of 128 bits, while it has flexible key sizes of 128, 192 and 256 bits, and their numbers of rounds for repetition are 10, 12 and 14 respectively. S-AES is simplified version of AES. The block and key size of S-AES are 16 bits, and it takes only 2 rounds for full encryption. A round of AES and S-AES consists of four basic transformations: Substitution, Shiftrows, Mixcolumns, and Addroundkey. The difference is that Substitution, Shiftrows and Mixcolumn of AES is by byte while S-AES is by nibble.

Substitution: A nonlinear function which substitutes each nibble of the block according to the S-box.

Shiftrows: A function which turns the block from

$N_0 \quad N_2$
$N_1 \quad N_3$
To
$N_0 \quad N_2$
$N_3 \quad N_1$.

Mixcolumns: A function that makes linear combination of each input nibble. It can be seen as the matrix map: $\begin{bmatrix} N_0 & N_2 \\ N_1 & N_3 \end{bmatrix} \mapsto \begin{bmatrix} 1 & x^2 \\ x^2 & 1 \end{bmatrix} \begin{bmatrix} N_0 & N_2 \\ N_1 & N_3 \end{bmatrix}$.

Addroundkey: A function that makes xor with the expansion of the initial key.

The security offered by full rounds AES is breakable. However, the long execution time of AES makes it hard to be adapted to Internet of things and Zigbee. S-AES was developed following the structure of AES, but S-AES is light and can be implemented easily. However, as the algorithm become less complex, the robustness of S-AES degenerates. To improve the security and robustness of S-AES in image encryption, we use chaos.

3 Chaos

Chaos is a nonlinear process with sensitivity to a small change to initial condition and parameters. [5]The

[a] Corresponding author: bailan0506@gmail.com

property of chaos can enhance the confusion and diffusion of Cryptographic algorithms.Two chaotic maps will be applied to in our scheme, Modified Arnold Map and PWLCM (Piecewise Linear Chaotic Map).

3.1 Modified Arnold Map

Classical Arnold map is a two-dimensional invertible chaotic map[6] for a NxN image. We will apply the Modified Arnold Map Based on Arnold map to make diffusion to the Images. The Modified Arnold Map is defined as:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} \equiv \begin{bmatrix} 1 & c \\ d & cd+1 \end{bmatrix}^{s} \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} e \\ f \end{bmatrix} (mod\ N) \qquad (1)$$

(*x,y*) is the original pixel position in an $\mathrm{N} \times \mathrm{N}$ image and (*x',y'*) is the transformed position after the map. *c, d, s, e, f* are integers in $\{0,1,2,\cdots,N-1\}$.

The inverse of Modified Arnold Map is defined as:

$$\begin{bmatrix} \mathrm{x} \\ \mathrm{y} \end{bmatrix} \equiv \begin{bmatrix} 1 & \mathrm{c} \\ \mathrm{d} & \mathrm{cd}+1 \end{bmatrix}^{-\mathrm{s}} \left(\begin{bmatrix} \mathrm{x}' \\ \mathrm{y}' \end{bmatrix} - \begin{bmatrix} \mathrm{e} \\ \mathrm{f} \end{bmatrix} \right) (\mathrm{mod\ N}) \qquad (2)$$

To be concise, we use MAM(Image,c,d,e,f,s) and IMAM(Image,c,d,e,f,s) to denote the Modified Arnold Map and its inverse, respectively.

3.2 PWLCM

PWLCM is one of simplest chaotic map[7], so that it can be applied in cryptosystem of sensor networks and IoT without too much time cost of the encryption. The algorithm is described as:

$$c_{n+1} = F(c_n) = \begin{cases} {c_n}/{\mu} & 0 \le c_n \le \mu \\ {(c_n - \mu)}/{(0.5-\mu)} & \mu \le c_n < 0.5 \\ F(1-c_n) & 0.5 \le c_n < 1 \end{cases} \quad (3)$$

The initial condition ranges from $c_n \in [0,1)$, and the control parameter ranges from $\mu \in (0,0.5)$. PWLCM will be used as pseudo random number generator to enhance the performance and security of S-AES.

4 Proposed Scheme

The proposed encryption scheme consists of two main stages. The first stage is image pixels diffusion through Modified Arnold Map. The second stage is encryption by chaotic S-AES.

In chaotic S-AES, the S-box and the creation of initial keys are modified by PWLCM described above.

The function Substitution has a weak point because the S-box is a constant matrix, and the matrix is open to adversary. We replace this S-box with a dynamic one using PWLCM generator. At every execution of S-AES, the S-box will be generated once. The chaotic generator has initial state c_0 and parameter μ, which can be viewed as additional secret keys for the new algorithm. Every iteration gives a number $\mathrm{R}(i)$. After each iteration, the first 32 bits of c_n will be extracted. We will divide the 32 bits into 8 nibbles place them in the new S-box. So, it takes 2 iterations to create a new S-box.

The sub-key of each round of S-AES is the expansion of the initial key. The initial key should be a random one in case that adversary gets either sub-key or the initial one. Since S-AES is a symmetric key algorithm, both side of communication needs to ensure they have the same initial key before encryption. We use another PWLCM generator with different initial state c_0' and parameter μ' to generate pseudo random numbers as initial keys during every execution of S-AES. So, only the seeds of generator, c_0' and μ', need to be exchange before encryption, instead of all initial keys. The cost of communication can be saved.

Modified Arnold Map is implemented to scramble the image. The S-box and the creation of initial keys have been modified into random manners. So it becomes hard for attackers to predict the behavior of the cryptosystem. Fig.1 shows the full process of our scheme.

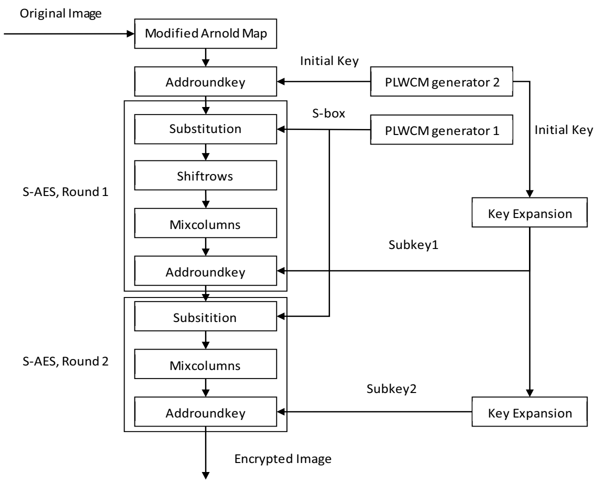

Fig.1 The full process of proposed scheme

5 Experimental Analysis

Experimental results are shown to discuss the security and efficiency of our scheme in this section.

5.1 Results of proposed scheme

We use LENA, the gray plain image with a size of 256x256 to implement our encryption scheme.

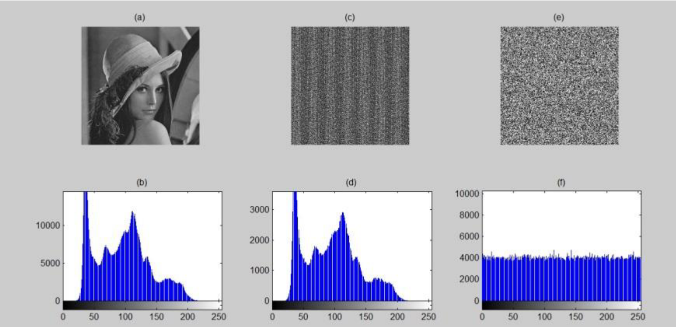

Fig.2 (a-b) plain image and the histogram of LENA; (c-d) LENA after diffusion by Modified Arnold Map and the histogram; (e-f) LENA after encryption by proposed scheme and the histogram

Fig.2 shows that the encrypted image is visually indistinguishable. The histogram analyses how pixels in an image are distributed by plotting the number of pixels at each intensity level [8]. It is obvious that the histogram of encrypted image is distributed uniformly, like white noise.

5.2 General Security Analysis

S-AES maintains the essential structure of AES which is unbreakable till now. Also, the initial value c_0 and parameter μ of PWLCM is actually the key of the improved algorithm. c_0 can be any value in $[0,1)$ and μ can be an value in $(0,0.5)$. The only restriction of the values is precision of computers. The key space is large enough to avoid attacks, and the chaotic map guarantees the key sensitivity. Moreover, because of the diffusion made by Modified Arnold Map, even if the adversary obtains a part of the original image, no other parts can be acquired since he or she can hardly get the key. Therefore, our scheme can resist chosen-plaintext attack.

6 Conclusion

In this paper, we propose an improvement for S-AES by combination of Modified Arnold Map and PWLCM. We make use of chaotic maps not only in diffusion of pixels of images, but also in the encryption procedure. We do not make the algorithm too complex so that we enhance the robustness of S-AES while the efficiency of encryption does not decrease a lot. Our scheme is suitable for sensor networks and Internet of things.

References

1. R.L. Rivest, A. Shamir, and L. Adleman, A Method for Obtaining Digital Signatures and Public Key Cryptosystems, Comm. ACM, 21(2):120-126, 1978.
2. N.Challita, Enhancement of S-AES using chaos for the support of biomedical applications , 2nd International Conference on Advances in Biomedical Engineering, 175-178, 2013.
3. J. Buchmann, Introduction to Cryptography, Berlin, Germany, Springer, 2004.
4. M. Musa, E. Schaefer, and S. Wedig, A simplified AES algorithm andits linear and differential cryptanalyses, Cryptologia, 27:148–177, 2003.
5. L.Kocarev, Chaos-based cryptography: a brief overview，Circuits and Systems Magazine, IEEE, 1(3):6-21, 2001.
6. V. Arnold, and A. Avez, Ergodic Problems in Classical Mechanics, Addison-Wesley, 1989.
7. B. Bakhache, J. Ghazal, and S. El Assad, Improvement of the securityof ZigBee by a new Chaotic Algorithm, Systems Journal, IEEE, January 2013.
8. M.Asiml, V.Jeotil, On Image Encryption: Comparison between AES and a Novel Chaotic Encryption Scheme, ICSCN 2007, IEEE, 65-69, 22-24, 2007