A Generalized Continued Fraction-Based Asynchronous Stream Cipher For Image Protection

Atef Masmoudi, William Puech, Mohamed Selim Bouhlel

A GENERALIZED CONTINUED FRACTION-BASED ASYNCHRONOUS STREAM CIPHER FOR IMAGE PROTECTION

A. MASMOUDI[1,2], *W. PUECH*[2], *and M.S. BOUHLEL*[1]

[1]Research Unit: Sciences and Technologies of Image and Telecommunications
Higher Institute of Biotechnology, Sfax TUNISIA
[2]Laboratory LIRMM, UMR 5506 CNRS University of Montpellier II
161, rue Ada, 34392 MONTPELLIER CEDEX 05, FRANCE
atef.masmoudi@lirmm.fr william.puech@lirmm.fr medsalim.bouhlel@enis.rnu.tn

ABSTRACT

In this paper, we are particulary interested by image protection. The conventional encryption standard may be not applicable to images, due to the digital images properties which are characterized with some intrinsic features such as highly pixel redundancy and correlation. We propose a new asynchronous stream cipher based on generalized continued fraction (GCF). The proposed scheme is resistant to statistic attack, differential attack and some other known attacks. Experimental results prove that our scheme is efficient and secure.

1. INTRODUCTION

With the advancements of communication technologies and the fascinating developments in digital image processing, the real-time secure image transmission over public networks such as the Internet and through wireless networks need to be secure. Thus, to make use of the communication infrastructure already developed and to maintain the secrecy, cryptographic techniques need to be applied [1, 2]. Cryptographic approaches are therefore critical for secure multimedia content storage and distribution over open networks such as the Internet and wireless networks.

In this paper, we are particulary interested by image protection. The conventional cryptographic, such as DEA, AES and RSA may not be good candidates, especially for fast and real-time communication applications. In recent years, several stream cipher methods have been proposed. Some of them are synchronous like the chaos-based image encryption system with stream cipher structure [13, 16, 21, 22, 7]. Other are asynchronous, and the advantage of these techniques is that if ciphertext digits are dropped or added, then the decipher stream can self-heal by re-synchronization, and result errors are limited in a few plaintext digits. Furthermore, asynchronous stream ciphers have statistically a better diffusion than synchronous stream ciphers. In this paper, a new asynchronous stream cipher based on the use of the generalized continued fraction (GCF) to modify the pixel's value is proposed.

The rest of this paper is organized as follows. In Section 2, we overview the continued fraction method. In Section 3 the proposed image encryption scheme based on GCF is presented and discussed. Performances and cryptanalysis of the new proposed scheme for image encryption are studied in Section 4. Finally, Section 5 concludes the paper.

2. CONTINUED FRACTION

A continued fraction [8, 14, 17, 20, 18] refers to all expressions of the form:

$$x = b_0 + \cfrac{a_1}{b_1 + \cfrac{a_2}{b_2 + \cfrac{a_3}{b_3 + \cfrac{a_4}{\cdots}}}}, \tag{1}$$

where a_i $(i > 0)$ are the partial numerators, b_i the partial denominators, and the leading term b_0 is the so-called whole or integer part of the continued fraction. Note that the partial numerators and the partial denominators can assume arbitrary real or complex values. There are other notations for a continued fraction in more or less common use. One convenient way to express a generalized continued fraction looks like this:

$$x = b_0 + \frac{a_1}{b_1+}\frac{a_2}{b_2+}\frac{a_3}{b_3+}\cdots. \tag{2}$$

Pringsheim wrote a generalized continued fraction as follows:

$$x = b_0 + \frac{a_1|}{|b_1} + \frac{a_2|}{|b_2} + \frac{a_3|}{|b_3} + \cdots. \tag{3}$$

In this paper we propose to use the following notation:

$$x = b_0 + K_{i=1}^{\infty}\frac{a_i}{b_i}, \tag{4}$$

where the K stands for Kettenbruche, the German word for continued fraction. A simple continued fraction is a continued fraction where all the value $a_i = 1$:

$$x = b_0 + K_{i=1}^{\infty}\frac{1}{b_i}. \tag{5}$$

Theorem 1 *Let f_n denote the result of evaluating equation (1) with coefficients through a_i and b_i. Then:*

$$f_n = \frac{A_n}{B_n}, \tag{6}$$

where A_n and B_n are given by the following recurrence:

$$\begin{array}{cc} A_{-1} = 1 & B_{-1} = 0 \\ A_0 = b_0 & B_0 = 1 \\ A_j = b_j A_{j-1} + a_j A_{j-2} & B_j = b_j B_{j-1} + a_j B_{j-2} \end{array}$$
$$j = 1, \cdots, n$$

The fractions (6) are referred to as general convergents.

Continued Fractions [6] have become used in various areas. For exemple, they have been used for computing rational approximations to real numbers and for solving various well known equations. R. M. Corless, in his paper [10], presents the connection between chaos theory and CF. The process of generating successive fractional parts of a real number is given by a the Gauss map [11] which is a non-linear equation. Gauss presents the following map from [0,1) to [0,1), called Gauss map, to find the CF representation of a real number:

$$G(x) = \begin{cases} 0 & \text{if } x = 0 \\ \frac{1}{x} \bmod 1 & \text{otherwise} \end{cases} \quad (7)$$

The notation "mod 1" means taking the fractional part. The operation of generating the infinite list of CF representation from a real number using Gauss map is a chaotic process. The best general method for evaluating continued fractions seems to be the modified Lentz's method [12]. In detail, the modified Lentz's algorithm is presented in algorithm (1), where Th is a threshold related to the floating-point precision.

Algorithm 1

begin
$f_0 \leftarrow b_0$
if $(b_0 = 0)$ **then**
  $f_0 \leftarrow tiny$
end if
$C_0 \leftarrow f_0$
$D_0 \leftarrow 0$
for $j \leftarrow 1, \cdots n$ **do**
  $D_j \leftarrow b_j + a_j D_{j-1}$
  if $(D_j = 0)$ **then**
    $D_j \leftarrow tiny$
  end if
  $C_j \leftarrow b_j + a_j / C_{j-1}$
  if $(C_j = 0)$ **then**
    $C_j \leftarrow tiny$
  end if
  $D_j \leftarrow 1/D_j$
  $\Delta_j \leftarrow C_j D_j$
  $f_j \leftarrow f_{j-1}\Delta_j$
  if $(|\Delta_{j-1}| < Th)$ **then**
    exit
  end if
end for
end

The algorithm (1) assumes that you can terminate the evaluation of the continued fraction when $|f_j - f_{j-1}|$ is sufficiently small. There is at present no rigorous analysis of error propagation in Lentz's algorithm. However, empirical tests suggest that it is at least as good as other methods.

3. PROPOSED ENCRYPTION SCHEME

Assuming that a gray scale plain image and its corresponding cipher image are represented by $X = \{X_1, \cdots, , X_N\}$ and $Y = \{Y_1, \cdots, , Y_N\}$, respectively. N is the number of pixels in both original and encrypted image. Each element of X and Y is an $8 - bit$ value representing the gray level of that pixel.

Algorithm 2

begin
for $j \leftarrow 1, \ldots, N$ **do**
  $S \leftarrow 0$
  for $\alpha \leftarrow 1, \ldots, k \; div \; p$ **do**
    $R_\alpha \leftarrow K_{i=1}^{p} \frac{Y_{j-p(\alpha-1)+i} + 1}{c_{p(\alpha-1)+i} + 1}$
    $S \leftarrow S + R_\alpha$
  end for
  $Y_j \leftarrow X_j \otimes (\sum_{i=1}^{5} (d_{1,i} d_{2,i} d_{3,i})_s) \; mod \; 256$
end for
end

Let K be a key of length k bytes C_i, $k = C_1, C_2, \cdots, C_k$. The unit of encryption is the pixel (1 byte). The proposed encryption scheme consists in the fact that for each pixel of the plain image, the encryption value depends upon the original pixel, the value of the key K, and k pixels previously encrypted. For each pixel X_i of the original image, we calculate the value of the pixel Y_i of the encrypted image using the algorithm 2 with $j \in [1, \cdots, N]$ where N is the number of pixels in both original and encrypted image, k is the length of the key, $\alpha \in [1, \cdots, k \; div \; p]$ where p is the number of C_i and Y_i used to form a generalized continued fraction with the partial numerators are Y_i and the partial denominators are C_i. R_α is the result of evaluation of the continued fraction using the algoritm 1 and S is the sum of all R_α.

The sum S is a double value and we choose its first 15 significant digits, $S = 0.d_1 d_2 d_3 \ldots d_{15}$. Divide the 15 digits into five integers with each integer consisting of three digits $(d_{1,i} d_{2,i} d_{3,i})_s$, $i \in [1 \cdots 5]$.

Next we propose to calculate the sum of these integers $\sum_{i=1}^{5} (d_{1,i} d_{2,i} d_{3,i})_s$, do mod 256 operation and do XOR operation of the generated byte with one byte of pixel X_i from the original image. Finally, out put the calculation result Y_i to the encrypted image.

In Section 4, the proposed stream cipher is analyzed using different security measures. These measures include visual test, key sensitivity test, histogram analysis, correlation analysis of adjacent pixels and differential analysis.

4. EXPERIMENTAL ANALYSIS

In this section, we present some security analysis of the proposed image encryption scheme, including the most important ones like key sensitivity test, statistical analysis, and differential analysis [9, 5].

4.1 Visual testing

A number of images are encrypted by the proposed method, and visual test is performed. Three examples are shown in Fig.1 (a), (c) and (e), where each image is in 8-bit grey-level with 256×256 pixels. Fig.1 (a) is the Lena plain-image, Fig.1 (c) is a black image with 128×128 white bloc and Fig.1 (e) is a medical image. All images were encrypted with the encryption key $K = A0DEACB6A2B0401DB5F076CC277ABC4A$ expressed in

hexadecimal format and consists of a 128 bits. By comparing the original and the encrypted images in Fig. 1, there is no visual information observed in the encrypted images. The encrypted images are visual unknowable with a big difference from original images.
The encrypted image should be greatly different from its original form. there are two measures using to quantify the above requirement, noted NPCR and UACI [3, 4].
Let $C_1(i,j)$ and $C_2(i,j)$ be the ith row and jth column pixel of two images C_1 and C_2. We define a two-dimensional array D, having the same size as C1 and C2.

- NPCR (Number of Pixel Change Rate): The NPCR is used to measure the number of pixels in difference of two images. The NPCR can be defined as

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\%, \quad (8)$$

where W and H are the width and height of the image and $D(i,j)$ is defined as follows:
If $C_1(i,j) = C_2(i,j)$ then $D(i,j) = 1$, otherwise $D(i,j) = 0$.

- UACI(Unified Average Changing Intensity): The UACI measures the average intensity of differences between the two images. The UACI is defined as

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right] \times 100\%. \quad (9)$$

It is clear that in order to resist difference attack, the NPCR value should be small enough, and the UACI value should be large enough to a ideal cipher system. Experimental results for NPCR and UACI between original and encrypted image are shown in Table 1.

Table 1: Pixel difference between original and encrypted image

test item	test results
NPCR	0.4150
UACI	30.0102

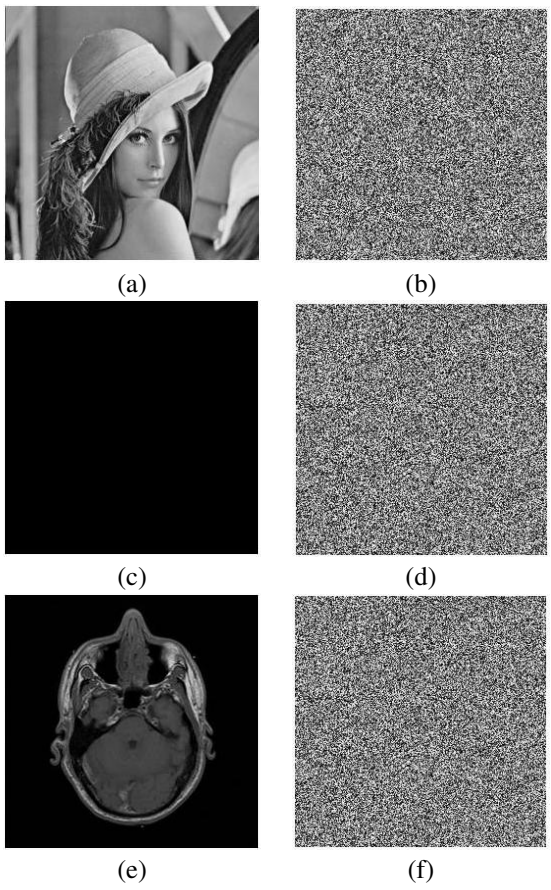


Figure 1: Image encryption experimental result:(a) Lena plain-image, (b) encrypted image of (a), (c) black image, (d) encrypted image of (c) , (e) medical image, (f) encrypted image of (e).

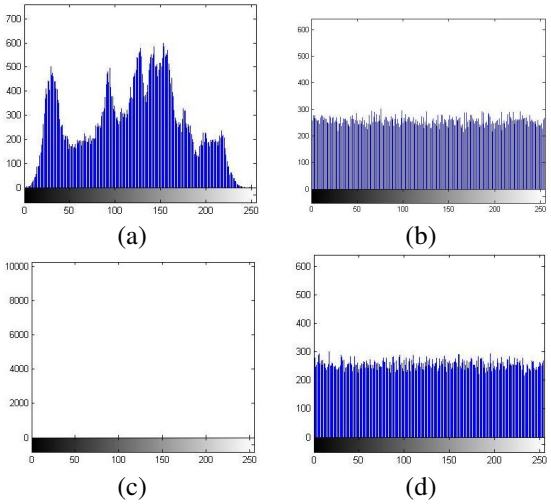


Figure 2: Histograms of original images and encrypted images.

4.2 Statistical analysis

a) ***Histograms of encrypted images:***
With a statistical analysis [19] of the original and encrypted images, their grey-scale histograms are shown in Fig.2. The standard Lena image of size 256×256 and 256 grey levels is employed in this test. It is shown in Fig.2 (a). A 256×256 image composed of all black pixels (pixel value 0) is taken an example of homogenous image Fig.2 (e). Fig.2 (d) and Fig.2 (h) show the histograms of two encrypted images which are significantly different from the histograms of the original images (Fig. 2 (b) and Fig. 2 (f) respectively) . From the Figure we can see the uniformity distribution of gray-scale of the encrypted images. Hence, the proposed algorithm does not provide any clue to employ any statistical analysis attack on the encryption image.

b) ***Correlation of adjacent pixels:***
For an ordinary image, each pixel is usually highly correlated with its adjacent pixels either in horizontal, vertical or diagonal directions. However, the proposed en-

cryption scheme should generate a cipher image with low correlation of adjacent pixels [22]. Taking the horizontal correlation as an example, for each pixel of the image, a duplet $(x_i\ ,\ y_i)$, can be found, where yi is the horizontal adjacent pixel of x_i. Obviously, there may be more than one duplet for each pixel, and the horizontal correlation coefficient is computed as Eq.13.

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{10}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2 \tag{11}$$

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))(y_i - E(y)) \tag{12}$$

$$\gamma_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{13}$$

where N is the total number of duplets (x_i, y_i) obtained from the image, and $E(x)$ and $E(y)$ are the mean values of x_i and y_i, respectively. Table 2 shows all the three correlation coefficients of Lena image and those of its encrypted image. Fig. 3 shows the correlation distribution of two horizontally adjacent pixels in the plain-image and that in the ciphered image. These correlation analysis proves that the our encryption algorithm satisfy zero correlation.

Table 2: Correlation coefficients of adjacent pixels in the two images

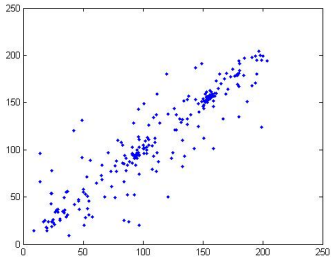
	plain-image	ciphered image
horizontal	0.9411	0.0028
vertical	0.9702	0.0005
diagonal	0.8960	-0.0004

4.3 Key sensitivity test

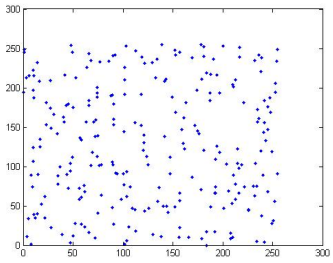
According to the basic principle of cryptology, a cryptosystem should be sensitive to the key. Thus, we propose the following tests [15].

a) Assume that a 128-bits ciphering key is used. A typical key sensitivity test has been performed, according to the following steps:
First, a 256×256 Lena plain-image is encrypted by using the test key *A0DEACB6A2B0401DB5F076CC277ABC4A*.
Then, the least significant bit of the key is changed, so that the original key becomes, say *A0DEACB6A2B0401DB5F076CC277ABC4B* in this example, which is used to encrypt the same image. Finally, the above two ciphered images, encrypted by the two slightly different keys, are compared. The numerical result shown in Table 3 demonstrating that the image encrypted by the first key and the image encrypted by the second key have 99.58% pixels different from each other, although there is only one bit difference in the two keys. Fig. 4 shows the test result.

Correlation of horizontal adjacent two pixels for original image

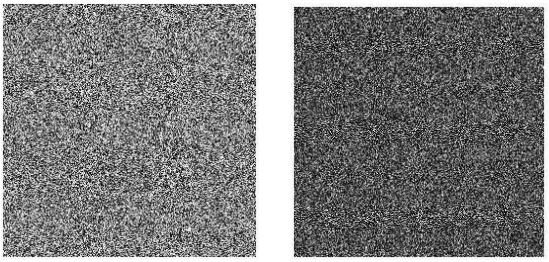


Pixel gray value on location (x,y)
(a)
Correlation of horizontal adjacent two pixels for encrypted image



Pixel gray value on location (x,y)
(b)

Figure 3: Correlations of two horizontally adjacent pixels in the plain-image and in the cipher-image: (a) correlation analysis of plain-image, (b) correlation analysis of cipher-image.



(a) (b)

Figure 4: Key sensitivity test 1: a) Encrypted image with key = *A0DEACB6A2B0401DB5F076CC277ABC4B*, b) Difference between the two encrypted images (a) and Fig. 1.b.

Table 3: Pixel difference between image encrypted by keys with 1-bit difference

test item	test results
NPCR	0.4120
UACI	33.4578

b) In addition, to testing with slightly different encryption keys, decryption using key with only 1-bit difference is also performed. Fig. 5 clearly shows that the image encrypted by the key *A0DEACB6A2B0401DB5F076CC277ABC4A* is not correctly decrypted by using the key *A0DEACB6A2B0401DB5F076CC277ABC4B* there,

which has only one bit difference between the two keys. Thus, having a perfect approximation of the encryption key makes decryption impossible.

(a) (b)

Figure 5: Key sensitivity test 2: c) Decrypted image with key = *A*0*DEACB*6*A*2*B*0401*DB*5*F*076*CC*277*ABC*4*A*, d) Decrypted image with key = *A*0*DEACB*6*A*2*B*0401*DB*5*F*076*CC*277*ABC*4*B*.

5. CONCLUSION

In this paper, the well-known generalized continued fraction has been used to design a secure symmetric image encryption scheme. We have detailed some numerical analysis of our approach. The experimental tests which have been performed demonstrating the high security of the new image encryption scheme. This scheme can be used for real time Internet image encryption and transmission application.

Acknowledgment

This work is in part supported by VOODDO (2008-2011), a project of ANR and the region of Languedoc Roussillon, France.

REFERENCES

[1] AES. Announcing the Advanced Encryption Standard. *Federal Information Processing Standards Publication*, 2001.

[2] Schneier B. Applied cryptography. *Wiley, New York, USA*, 1995.

[3] Guanrong Chen, Yaobin Mao, and Charles K. Chui. A symmetric image encryption scheme based on 3D chaotic cat maps. *Chaos, Solitons and Fractals*, pages 749–761, 2004.

[4] Chiaraluce F and Ciccarelli L. A new chaotic algorithm for video encryption. *CIEEE Trans Consum Electron*, 2002.

[5] Jakimoski G and Kocarev L. Analysis of some recently proposed chaos-based encryption algorithms. *Phys Lett A*, 2001.

[6] A.Y. Khintchin. Continued Fractions. *Noordhoff, Groningen*, 1963.

[7] Zhang LH, Liao XF, and Wang XB. An image encryption approach based on chaotic maps. *Chaos, Solitons and Fractals*, 2005.

[8] L. Lorentzen and H. Waadeland. Continued Fractions with Applications. *North Holland*, 1992.

[9] A lvarez G, Montoya F, Romera M, and Pastor G. Cryptanalyzing an improved security modulated chaotic encryption scheme using ciphertext absolute value. *Chaos, Solitons and Fractals*, 2005.

[10] Corless R. M., Frank G. W., and Monroe J. G. Chaos and continued fractions. *Physica D, North-Holland*, 46:241–253, 1990.

[11] R. Mafir. Ergodic Theory and Differentiable Dynamics. *Springer, Berlin*, 1987.

[12] W. H. Press. Numerical Recipes in C : the art of scientific computing, chapter 5, (especially 5.2 Evaluation of continued fractions). *Cambridge, Cambridge University Press*, pages 169 – 173, 1992.

[13] Li S and Mou X. Improving security of a chaotic encryption approach. *Phys Lett A*, 2001.

[14] R. B. Seidensticker. Continued fractions for high-speed and high-accuracy computer arithmetic. *in Proc. 6th IEEE Symp. Comput. Arithmetic*, 1983.

[15] Maniccam S.S and Bourbakis N.G. Lossless Image Compression and Encryption using SCAN. *Pattern Recognition*, 34:1229–1245, 2001.

[16] Yang T. A survey of chaotic secure communication systems. *Int J Comp Cognit*, 2004.

[17] D. Teichroew. Use of Continued Fractions in High Speed Computing. *rican Mathematical Society*, 1952.

[18] J. Vuillemin. Exact Real Computer Arithmetic with Continued Fractions. *INRIA Report 760. Le Chesnay, France: INRIA*, NOV. 1987.

[19] Puech W and Rodrigues J.M. A New Crypto-Watermaking Method for Medical Images Safe Transfer. *In Proc.EUSIPCO'04*, pages 1481–1484, Vienna,Austria September 2004.

[20] H. S. Wall. Analytic Theory of Continued Fractions. *Chelsea*, 1973.

[21] Kwok-Wo Wong, Bernie Sin-Hung Kwoka, and Ching-Hung Yuena. An efficient diffusion approach for chaos-based image encryption. *Chaos, Solitons and Fractals*, 2008.

[22] Wu XG, Hu HP, and Zhang BL. Analyzing and improving a chaotic encryption method. *Chaos, Solitons and Fractals*, 2004.