American Journal of Signal Processing 2015, 5(1): 13-21
DOI: 10.5923/j.ajsp.20150501.03

A Novel Cryptographic System with Adjustable Secret Key Space for Color Image Security Using Nonlinear Adaptive Filter

Hung-I Hsiao*, Junghsi Lee

Department of Electrical Engineering, Yuan Ze University, Taiwan

Abstract In this paper, we propose a novel chaos-based cryptographic system for enhancing color image security by using chaotic amplitude phase frequency model nonlinear adaptive filter. The advantage of the proposed scheme is that it possesses the ability of "adjustable secret key space" in order to get the enough security strength to protect color image. Furthermore, the experimental results and security analyses demonstrate that the proposed method has a fine security performance. The "adjustable secret key space" can overcome the security strength issue for obtaining enough secret key length, which can use external signal to adjust the required secret key space without changing the original cryptographic infrastructure.

Keywords Color image encryption, Adjustable secret key space, Chaos

1. Introduction

The discussions of the image security depict its importance shown in [1, 2]. To achieve the purpose of safe transmission and access of image, we propose a new cryptographic system which possesses the ability of adjustable secret key space, and the proposed scheme is designed by chaotic amplitude phase frequency model (APFM) nonlinear adaptive filter [3].

Among the modern encryption methods, Data Encryption Standard (DES) [4] and Advanced Encryption Standard (AES) [5] are the most typical. Besides, many chaotic encryption methods [6-8] have been researched in recent years. The chaos-based encryption schemes are the most noticeable due to the chaos excellent characteristics such as the sensitivity to initial conditions, and semi-randomness behaviors; the chaos excellent properties make the chaos-based cryptography possess nice randomness in encrypted image [9].

However, in the above-mentioned encryption methods, they can not use external signal to adjust the required secret key space in order to obtain sufficient security strength. For example, DES is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST) in 1977. DES's most serious weakness is the small secret key length, only 56 bits, causing all secret key space of DES to be 2^{56} [10]. This weakness could make the ciphers fragile to be brute-force attacked, so DES is later replaced by AES.

AES, the current encryption standard which is a symmetric-key block cipher published by NIST in 2001, has three different secret key lengths: 128, 192, and 256 bits, i.e., the corresponding secret key spaces are 2^{128}, 2^{192}, and 2^{256}, respectively [11]. Clearly, the secret key length and its corresponding secret key space decide the security strength of the cryptographic system.

Table 1 shows the recommendations of security-strength time frames published by NIST Special Publication 800-57 in 2012 [12], which is a schedule of the security strength for different secret key lengths that provide five types of lengths including 80, 112, 128, 192, and 256 bits. As shown in Table 1, because the two types of security strength, 80 and 112 bits, are not strong enough to protect data, both of the secret key lengths are placed in the "Disallowed" after 2013 and 2030, respectively. On the contrary, the secret key lengths 128, 192, and 256 bits are "Acceptable" from 2011-2031 and beyond, and the minimum of the secret key length for "Acceptable" is 112 bits of security strength, which is acceptable until 2030. We can find that the change of time frame is an important factor for obtaining the enough security strength of secret key length.

* Corresponding author:
hsiaohuinn@gmail.com (Hung-I Hsiao)
Published online at http://journal.sapub.org/ajsp

Table 1. Security-strength time frames

Security Strength		Application	2011 through 2013	2014 through 2030	2031 and Beyond
Secret key length	Corresponding secret key space				
80 bits	2^{80}	Applying (e.g., encryption)	Deprecated	Disallowed	Disallowed
		Processing (e.g., decryption)	Legacy use	Legacy use	Legacy use
112 bits	2^{112}	Applying (e.g., encryption)	Acceptable	Acceptable	Disallowed
		Processing (e.g., decryption)			Legacy use
128 bits	2^{128}	Applying (e.g., encryption) /Processing (e.g., decryption)	Acceptable	Acceptable	Acceptable
192 bits	2^{192}		Acceptable	Acceptable	Acceptable
256 bits	2^{256}		Acceptable	Acceptable	Acceptable

Based on the above discussions, we propose a new cryptographic system possessing adjustable secret key space, which also means that the secret key length is adjustable, and it is designed by chaotic APFM nonlinear adaptive filter whose input signal can control the size of secret key space. That is, the proposed scheme can use external signal to adjust the required secret key space without altering the original cryptographic infrastructure, so the security strength is sufficient to protect color images even it is way beyond the indicated time frames given in Table 1.

The rest of this paper is organized as follows. Section 2 introduces the concepts including chaotic APFM nonlinear adaptive filter. Furthermore, the proposed color image encryption/ decryption algorithm is described in Section 3. The experimental results are depicted in Section 4. Security analyses are subsequently presented in Section 5. Finally, Section 6 concludes the paper.

2. Chaotic APFM Nonlinear Adaptive Filter

The equation of APFM nonlinear adaptive filter is as follows: [13]

$$\begin{cases} \dot{A} = -2\mu_1 A \sin^2\phi + 2\mu_1 \sin\phi u(t) \\ \dot{\omega} = -\mu_2 A^2 \sin(2\phi) + 2\mu_2 A \cos\phi u(t) \\ \dot{\phi} = \omega + \mu_3 \dot{\omega} \\ y(t) = A\sin\phi \end{cases}, \quad (1)$$

where A, ω, ϕ, and $u(t)$ refer to amplitude, frequency, phase angle of the desired component, and input signal, respectively. The parameters μ_1, μ_2, and μ_3 are the filter step sizes for controlling the speed of the filter, $y(t)$ is the filter output, and

$$u(t) = \sum_{i=1}^{n} (a_i \sin(\omega_i t + \delta_i)). \quad (2)$$

We could properly set the parameters μ_1, μ_2, μ_3, a_i, ω_i, δ_i, for $i = 1, 2, ..., n$, simulated time interval, and initial values for the APFM nonlinear adaptive filter to generate chaotic trajectories. The APFM nonlinear adaptive filter could produce chaos in accordance with the numerical simulation results by Matlab tools using the ordinary differential equation (ODE) solver and solving on a simulated time interval $t_{\text{span}} = [t_0, t_f]$, when $\mu_1 = 1$, $\mu_2 = 0.08$, $\mu_3 = 1$, $t_{\text{span}} = [0, 4]$, with an arbitrarily small initial values $(A_0, \omega_0, \phi_0) = (1.11, 0.01, 0.1)$, computed precision is 10^{-14}, and $u(t)$ chooses the following three cases:

(i) Case 1: $u(t) = \sum_{i=1}^{n} (a_i \sin(\omega_i t + \delta_i))$, for

$n = 1,\ \ 0 \le a_1 \le 50,\ \omega_1 = 10,\ \delta_1 = 0.01$, i.e.,
$u(t) = a_1 \sin(10t + 0.01)$.

(ii) Case 2: $u(t) = \sum_{i=1}^{n} (a_i \sin(\omega_i t + \delta_i))$, for

$n = 2,\ 0 \le a_1 \le 50,\ \omega_1 = 7,\ \delta_1 = 0,\ a_2 = 1, \omega_2 = 2\pi,\ \delta_2 = 0.$
i.e., $u(t) = a_1 \sin(7t) + \sin(2\pi t)$.

(iii) Case 3: $u(t) = \sum_{i=1}^{n} (a_i \sin(\omega_i t + \delta_i))$, for

$n = 6,\ 0 \le a_1 \le 50,\ \omega_1 = 12,\ \delta_1 = 0.006,\ a_2 = 1,\ \omega_2 = 10,$
$\delta_2 = 0.005,\ a_3 = 1.2,\ \omega_3 = 8, \delta_3 = 0.004,\ a_4 = 1.3,\ \omega_4 = 6,$
$\delta_4 = 0.003,\ a_5 = 1.4,\ \omega_5 = 4,\ \delta_5 = 0.002, a_6 = 1.5,$
$\omega_6 = 2,\ \delta_6 = 0.001$, i.e.,

$$u(t) = a_1 \sin(12t + 0.006) + \sin(10t + 0.005) + 1.2\sin(8t + 0.004) + 1.3\sin(6t + 0.003) + 1.4\sin(4t + 0.002) + 1.5\sin(2t + 0.001).$$

As depicted in Figs. 1-3, which respectively refer to above Cases 1-3, a_1 is a controlled parameter, also known as bifurcation parameter, for the APFM nonlinear adaptive filter. The chaotic diagrams of this APFM nonlinear adaptive filter are shown in Figs. 1-3, whose sub-Figs. (a)-(c) denote the $a_1 - A$ plane, $a_1 - \omega$ plane, and $a_1 - \phi$ plane, respectively.

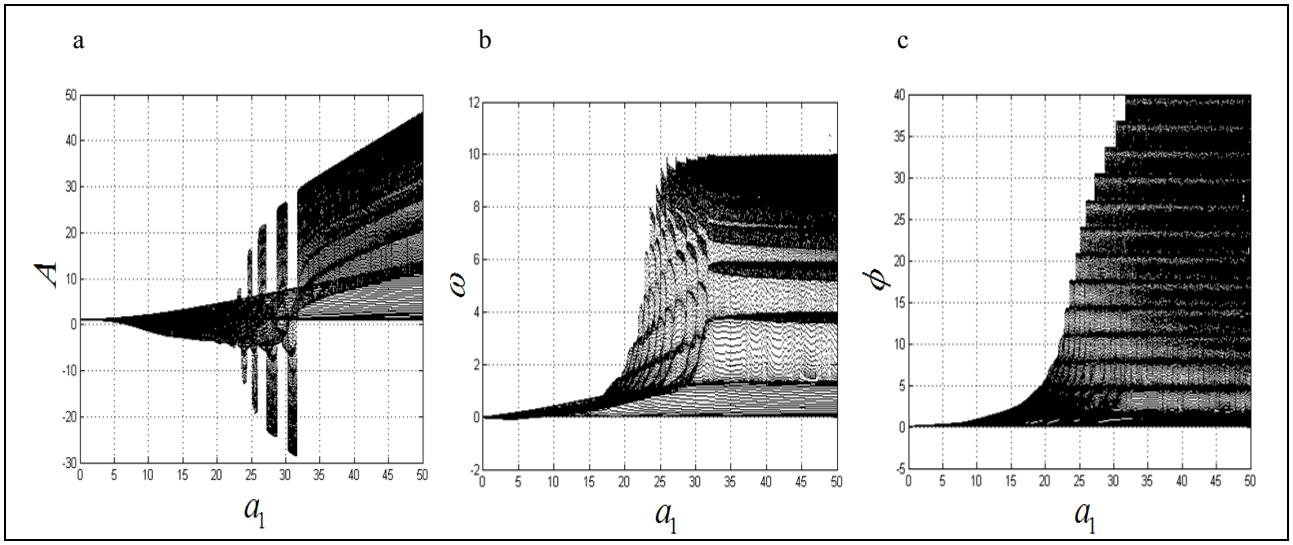

Figure 1. APFM nonlinear adaptive filter chaotic trajectories for Case 1, the parameters are $u(t) = a_1 \sin(10t + 0.01)$, $0 \le a_1 \le 50$, $\mu_1 = 1$, $\mu_2 = 0.08$, $\mu_3 = 1$, $t_{\text{span}} = [0, 4]$, $(A_0, \omega_0, \phi_0) = (1.11, 0.01, 0.1)$. (a) $a_1 - A$ plane, (b) $a_1 - \omega$ plane, (c) $a_1 - \phi$ plane

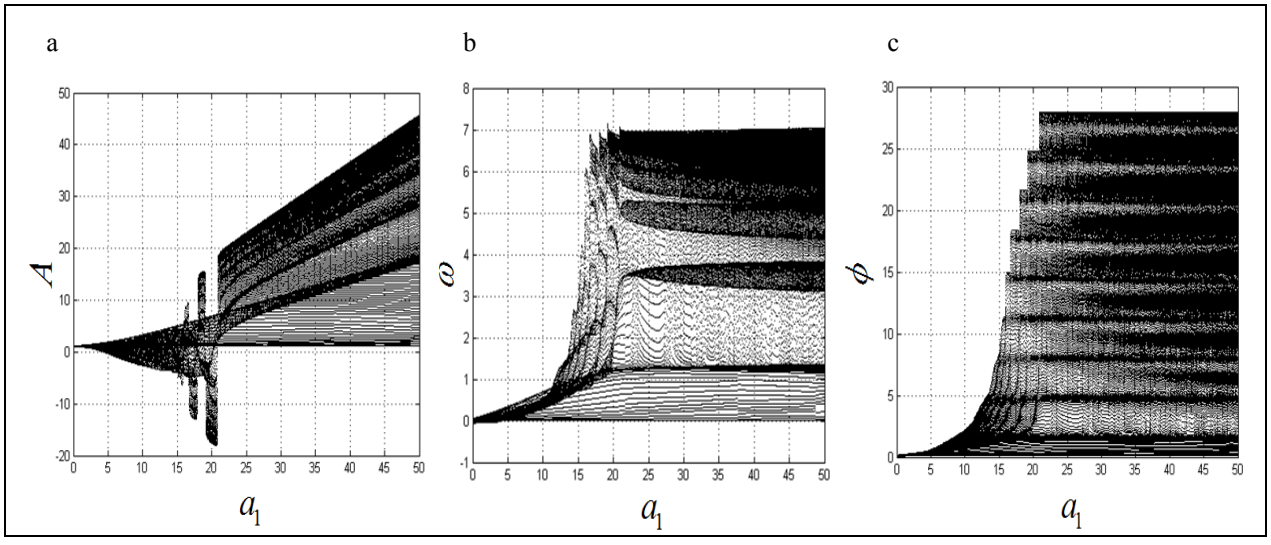

Figure 2. APFM nonlinear adaptive filter chaotic trajectories for Case 2, the parameters are $u(t) = a_1 \sin(7t) + \sin(2\pi t)$, $0 \le a_1 \le 50$, $\mu_1 = 1$, $\mu_2 = 0.08$, $\mu_3 = 1$, $t_{\text{span}} = [0, 4]$, $(A_0, \omega_0, \phi_0) = (1.11, 0.01, 0.1)$. (a) $a_1 - A$ plane, (b) $a_1 - \omega$ plane, (c) $a_1 - \phi$ plane

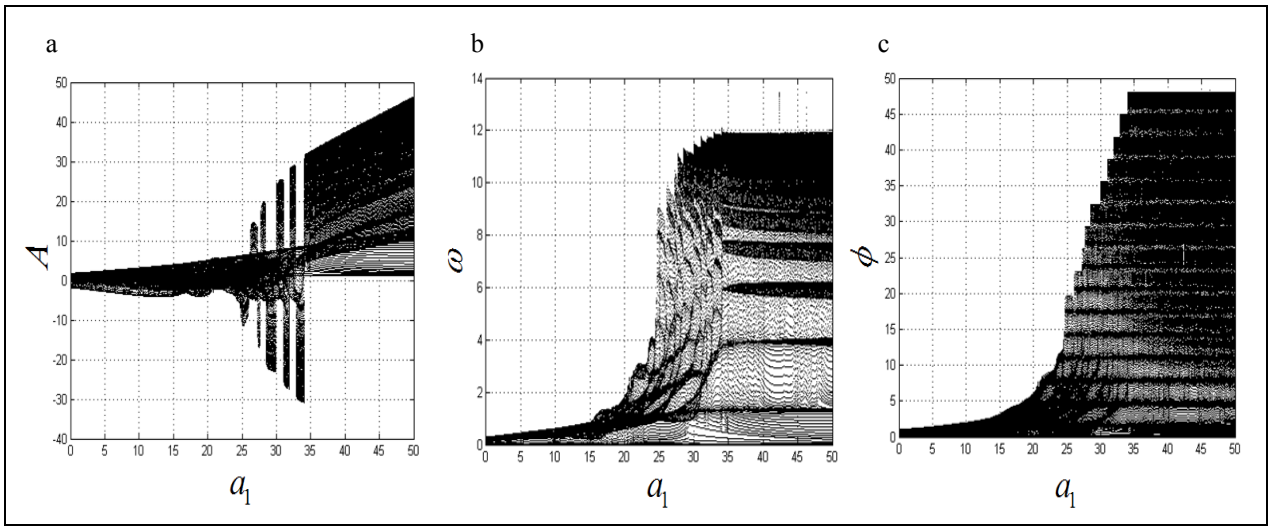

Figure 3. APFM nonlinear adaptive filter chaotic trajectories for Case 3, the parameters are $u(t)=a_1\sin(12t+0.006)+\sin(10t+0.005)+1.2\sin(8t+0.004)+1.3\sin(6t+0.003)+1.4\sin(4t+0.002)+1.5\sin(2t+0.001)$, $0\le a_1\le 50$, $\mu_1=1$, $\mu_2=0.08$, $\mu_3=1$, $t_{\text{span}}=[0,\ 4]$, $(A_0,\ \omega_0,\ \phi_0)=(1.11,\ 0.01,\ 0.1)$. (a) a_1-A plane, (b) $a_1-\omega$ plane, (c) $a_1-\phi$ plane

3. The Proposed Color Image Encryption/Decryption Algorithm

The design of color image encryption algorithm is shown as follows:

Step 1: Supposing the size of original color image is $h\times i\times 3$, h and i denote the width and height, respectively. We randomly choose three pixels named P_1, P_2, and P_3 in the original image. Compute the value ϕ by

$$\phi=\sin(P_1+P_2+P_3), \tag{3}$$

and compute the initial values A_0, ω_0, and ϕ_0 by

$$A_0=A_0'+\phi,\quad \omega_0=\omega_0'+\phi,\quad \phi_0=\phi_0'+\phi, \tag{4}$$

where $(A_0', \omega_0', \phi_0')$ are the given initial values.

Step 2: Giving the encrypted parameters for APFM nonlinear adaptive filter: μ_1, μ_2, μ_3, t_{span}, initial values $(A_0,\ \omega_0,\ \phi_0)$ and $(a_1, \omega_i, \delta_i)$.

Step 3: acquiring the APFM nonlinear adaptive filter 3 solutions $A(k)$, $\omega(k)$, and $\phi(k)$, then preprocess by Eqs. (5)~(7), for $k=1, 2,\ldots, h\times i$.

$$\tilde{A}(k)=\text{mod}\left(\text{abs}(A(k))\times 10^{10},\ 256\right), \tag{5}$$

$$\tilde{\omega}(k)=\text{mod}\left(\text{abs}(\omega(k))\times 10^{10},\ 256\right), \tag{6}$$

$$\tilde{\phi}(k)=\text{mod}\left(\text{abs}(\phi(k))\times 10^{10},\ 256\right), \tag{7}$$

Step 4: Decomposing the original color image to its red, green, and blue components, then get three gray image matrices P_{R}, P_{G}, and P_{B}.

Step 5: Generating three $h\times i$ cipher keys $\lambda_1(p,\ q)$, $\lambda_2(p,\ q)$, and $\lambda_3(p,\ q)$ obtained by

$$\lambda_1(p,\ q)=\tilde{A}\left((p-1)\times n+q\right), \tag{8}$$

$$\lambda_2(p,\ q)=\tilde{\omega}\left((p-1)\times n+q\right) \tag{9}$$

$$\lambda_3(p,\ q)=\tilde{\phi}\left((p-1)\times n+q\right) \tag{10}$$

for $p=1,\ 2,\cdots,\ h$, $q=1,\ 2,\cdots,\ i$.

Step 6: Executing the exclusive-or operation between gray images and cipher keys, and then get three $h\times i$ gray cipher images $IM_R(p,\ q)$, $IM_G(p,\ q)$, and $IM_B(p,\ q)$, for $p=1,\ 2,\cdots,\ h$, $q=1,\ 2,\cdots,\ i$, which are computed by as follows:

$$IM_R(p,\ q)=P_R(p,\ q)\oplus\lambda_1(p,\ q), \tag{11}$$

$$IM_G(p,\ q)=P_G(p,\ q)\oplus\lambda_1(p,\ q), \tag{12}$$

$$IM_B(p,\ q)=P_B(p,\ q)\oplus\lambda_1(p,\ q). \tag{13}$$

Step 7: Eventually, combine the three $h\times i$ gray cipher images IM_R, IM_G, and IM_B into $h\times i\times 3$ color cipher image.

The decryption algorithm is opposite to the encryption scheme due to the decrypted operation is reversed to the process for encryption, and the decrypted parameters are all the same encrypted parameters [14].

4. Experimental Results

4.1. Encryption

We use the color Lena image (Fig. 4(a)) with size $512\times512\times3$ is served as the color original image whose red, green, and blue components are separately shown in Figs. 4(b)-4(d), and the corresponding histograms are shown in Figs. 4(e)-4(g), respectively. The encrypted parameters of APFM nonlinear adaptive filter are $\mu_1=1$, $\mu_2=0.08$, $\mu_3=1$, $t_{\text{span}}=[0,\ 4]$, $\phi=0.1537$, given initial values $(A_0',\ \omega_0',\ \phi_0')=(0.01,\ 0.02,\ 0.03)$, computed precision is 10^{-14}, choosing three different $u(t)$, which are the same as the three cases of $u(t)$ shown in Section 2 except the parameter a_1 that ranges in $[0,\ 50]$, and the three cases are as follows:

(i) Case 1: $u(t)=10\sin(10t+0.01)$.

(ii) Case 2: $u(t)=45\sin(7t)+\sin(2\pi t)$.

(iii)Case 3:

$$u(t)=50\sin(12t+0.006)+\sin(10t+0.005)+1.2\sin(8t+0.004)+1.3\sin(6t+0.003)+1.4\sin(4t+0.002)+1.5\sin(2t+0.001).$$

The encrypted images and corresponding histograms are depicted in Figs. 5-7, which separately refer to Cases 1-3, in which the sub-fig. (a) denotes the color cipher image, sub-figs. (b)-(d) show the red, green, and blue components of color cipher image, respectively, and sub-figs. (e)-(g) depict the histograms of red , green, and blue components of color cipher image, separately.

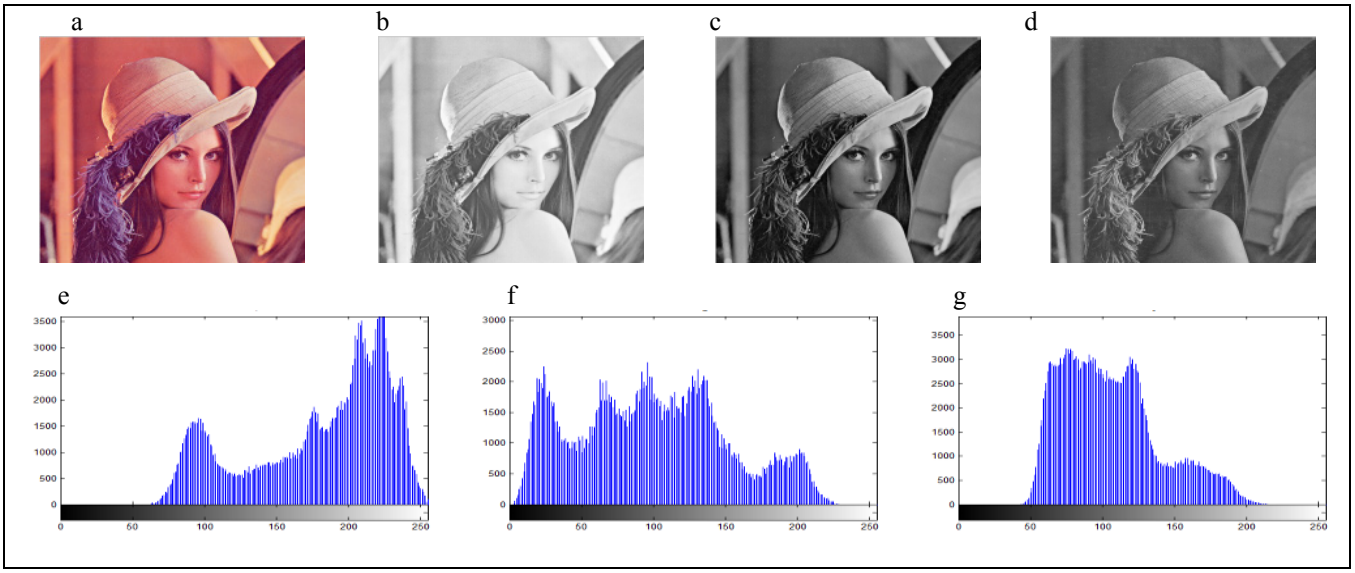

Figure 4. Color original image of Lena includes (a) color plain image, (b) red component, (c) green component, and (d) blue component. Histogram of the color plain image of Lena includes (e) red component, (f) green component, and (g) blue component

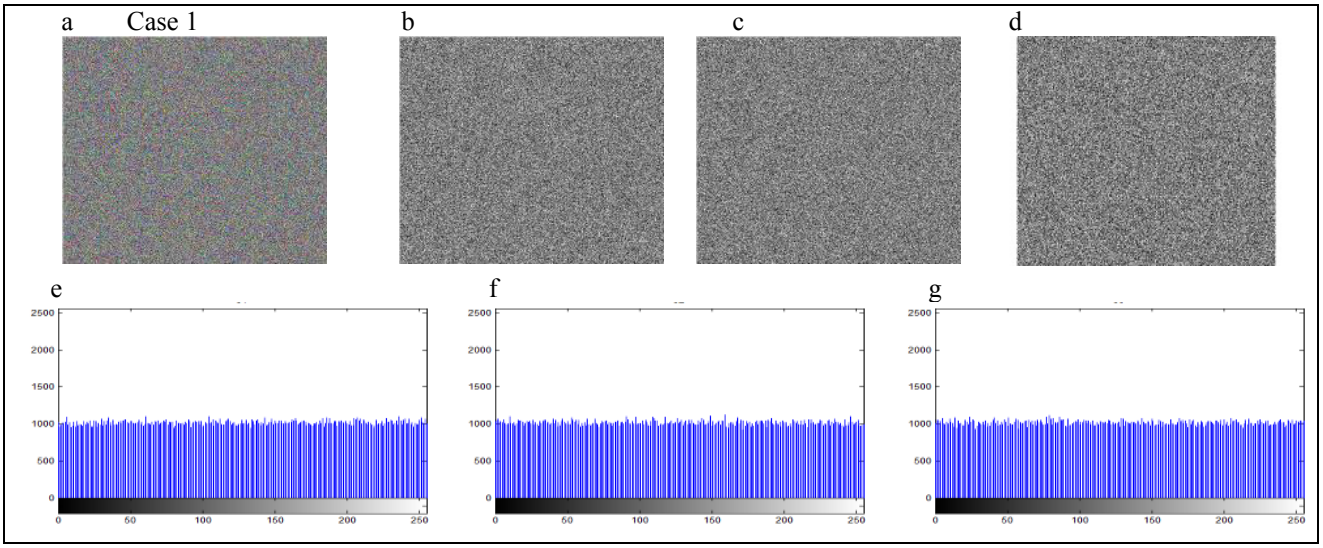

Figure 5. Encrypted image of Case 1 for Lena includes (a) color cipher image, (b) red component, (c) green component, and (d) blue component. Histogram of the color cipher image of Lena includes (e) red component, (f) green component, and (g) blue component

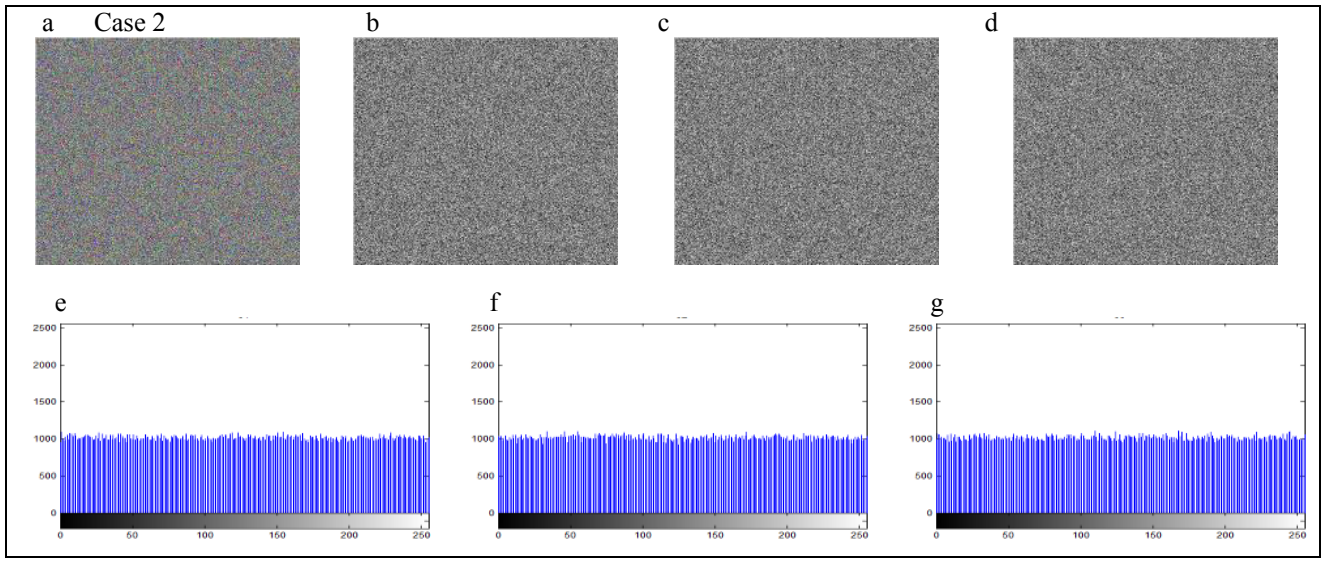

Figure 6. Encrypted image of Case 2 for Lena includes (a) color cipher image, (b) red component, (c) green component, and (d) blue component. Histogram of the color cipher image of Lena includes (e) red component, (f) green component, and (g) blue component

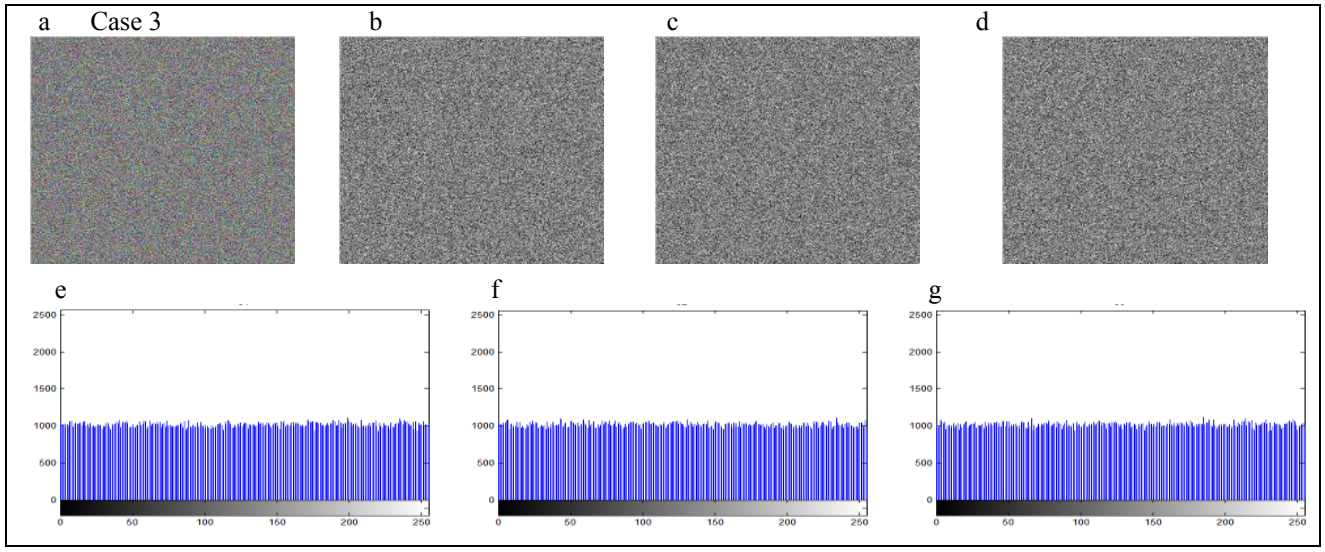

Figure 7. Encrypted image of Case 3 for Lena includes (a) color cipher image, (b) red component, (c) green component, and (d) blue component. Histogram of the color cipher image of Lena includes (e) red component, (f) green component, and (g) blue component

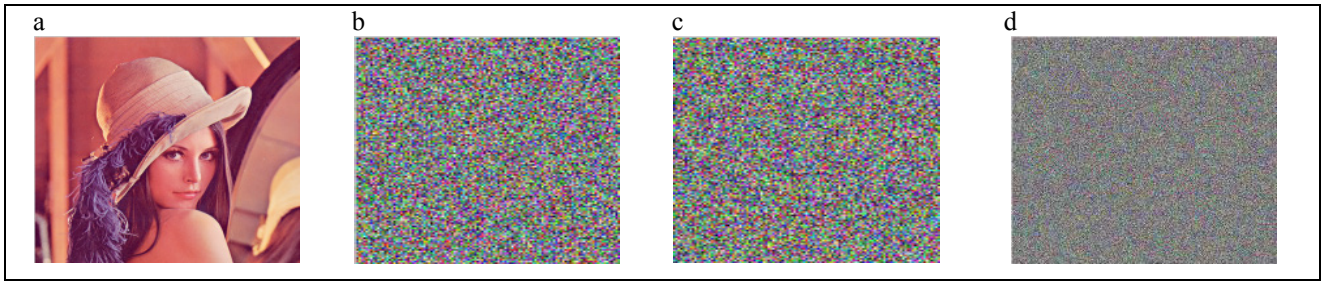

Figure 8. Decrypted images for color cipher image (Fig. 5(a)). (a) successful decryption, (b) failed decryption due to incorrect $u(t) = 10\sin(10t + 0.0100000001)$, (c) failed decryption due to incorrect $u(t) = 10\sin(10.0000000001t + 0.01)$, (d) failed decryption due to incorrect $u(t) = 9.9999999999\sin(10t + 0.01)$.

4.2. Decryption

For explaining the decryption, we use the color cipher image shown in Fig. 5(a) (i.e., generated by Case 1, the encrypted parameters are $u(t) = 10\sin(10t + 0.01)$, etc.) for explaining the decryption.

(1) Successful decryption

The decrypted parameters are all the same as the encrypted parameters of Case 1, which are given in Section 4.1. As depicted in Fig. 8(a), the decrypted image is successful to recover the color Lena image from color cipher image (Fig. 5(a)) due to the correct decrypted parameters.

(2) Failed decryption

The decrypted parameters are also same as the encrypted parameters of Case 1, which are shown in Section 4.1, except the input signal $u(t)$ that are chosen as

(i) $u(t) = 10\sin(10t + 0.0100000001)$

(ii) $u(t) = 10\sin(10.0000000001t + 0.01)$

(iii) $u(t) = 9.9999999999\sin(10t + 0.01)$

As shown in Figs. 8(b)-8(d), which refer to above 3 different $u(t)$, the decrypted images for color cipher image (Fig. 5(a)) are not successful due to the incorrect input signal $u(t)$ of APFM nonlinear adaptive filter.

5. Security Analyses

5.1. Adjustable Secret Key Space Controlled by Input Signal of APFM Nonlinear Adaptive Filter

The chaotic behavior of APFM nonlinear adaptive filter can design our proposed cryptographic system, we use this nonlinear filter to design encryption/decryption algorithm. The parameters, input signal, simulated time interval , and initial values of the APFM nonlinear adaptive filter can be used as the secret keys for proposed cryptographic system, so there are these secret keys (μ_1, μ_2, μ_3, a_i, ω_i, δ_i, t_0, t_f, A_0, ω_0, ϕ_0), for $i = 1, 2,..., n$. The total secret key space κ_{space} is

$$\kappa_{\text{space}} = \beta^{3n+8}, \tag{14}$$

where $\beta = 1/$ (computed precision). The value n depends on the input signal $u(t)$ of APFM nonlinear adaptive filter. We can choose three different $u(t)$ to control the size of secret key space, i.e., the proposed scheme possesses the characteristic of adjustable secret key space. This means that the proposed scheme can use outer signal to adjust the desired secret key space without changing original cryptographic architecture. The size of secret key space κ_{space} depends on input signal $u(t)$ of the APFM nonlinear adaptive filter. If the computed precision is 10^{-14}, calculate the secret key space for three different cases of $u(t)$ by Eq. (14), which are

(i) Case1: $u(t) = 10\sin(10t + 0.01)$, i.e., n=1,

$\kappa_{\text{space}} = \beta^{3n+8} = (10^{14})^{3\times1+8} = 10^{154} \approx 2^{512}$.

(ii) Case 2: $u(t) = 45\sin(7t) + \sin(2\pi t)$, i.e., n=2,

$\kappa_{\text{space}} = (10^{14})^{3\times2+8} = 10^{196} \approx 2^{651}$.

(iii)

$$\begin{aligned}\text{Case 3: } u(t) &= 50\sin(12t + 0.006) + \sin(10t + 0.005)\\ &\quad + 1.2\sin(8t + 0.004) + 1.3\sin(6t + 0.003)\\ &\quad + 1.4\sin(4t + 0.002) + 1.5\sin(2t + 0.001),\end{aligned}$$

$$\text{i.e., } n = 6, \quad \kappa_{\text{space}} = (10^{14})^{3\times6+8} = 10^{364} \approx 2^{1209}.$$

The above three secret key spaces 2^{512}, 2^{651}, and 2^{1209} (i.e., the corresponding secret key lengths are 512, 651, 1209 bits, respectively.) are enough to prevent all kinds of brute-force attacks [15]. Furthermore, the three different input signal $u(t)$ of APFM nonlinear adaptive filter can control the size of secret key space in order to acquire required security strength. Table 2 shows the comparison of secret key space with the proposed method and other scheme, in which the secret key space of proposed method is superior to the other schemes.

Table 2. Comparison of secret key space

Encrypted scheme	Proposed method	Ref. [16] (A. Kanso *et al*., 2012)	Ref. [17] (A. H. Abdullah *et al*., 2012)
Secret key space	2^{1209}	2^{480}	2^{40}

5.2. Histogram

The histograms of red, green and blue components for three cases of color cipher images, which are respectively shown in sub-Figs. (e)-(g) of Figs. 5-7, are almost uniformly distributed. The nearly uniform distribution of histograms can resist the statistical analysis attacks [16].

5.3. Correlation Analysis

The criterion for correlation analysis is computed by the correlation coefficient which is calculated by the following formulas [17]

$$r_{xy} = \frac{|\text{cov}(x, y)|}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{15}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}\big(x_i - E(x)\big)^2,\ D(y) = \frac{1}{N}\sum_{i=1}^{N}\big(y_i - E(y)\big)^2, \tag{16}$$

$$\text{cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N}\big(x_i - E(x)\big)\big(y_i - E(y)\big), \tag{17}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N}x_i,\ E(y) = \frac{1}{N}\sum_{i=1}^{N}y_i, \tag{18}$$

where x_i and y_i respectively denote gray level values of two different pixels in the image itself or between two different images, cov(x, y) indicates the covariance, $D(x)$, $D(y)$ represents the variance, and $E(x)$, $E(y)$ denotes the mean.

Table 3 gives the correlation coefficients of two adjacent pixels, in which we use the sample data that are randomly selected for 3000 pairs of two adjacent pixels from red, green, and blue components of color plain image and three color cipher images in the direction mixing horizontal, vertical, and diagonal direction simultaneously. Table 3 depicts the 3 correlation coefficient average values for three cipher images (i.e., item 5) are very small (they are close to ideal value 0.0) compared with those of color plain image (i.e., item 1 whose 3 correlation coefficient values are close to 1.0).

Similar to Table 3, Tables 4 and 5 respectively show the correlation coefficients of the same position and adjacent position among red, green, and blue components of color plain image and color cipher images, in which the 3 correlation coefficient average values (i.e., item 5 for Tables 4 and 5) for three cipher images are much smaller (they also approach to ideal value 0.0) than those of color plain image (i.e., item 1 for Tables 4 and 5).

Tables 3-5 display the nice encryption property on proposed method, in which it gives the near zero correlation between color plain image and color cipher image. Tables 4-5 depict the proposed method can effectively reduce the correlations among red, green, blue components of color cipher image.

Table 6 shows the correlation coefficients of all pixels of three components between color plain image and decrypted images, in which the three correlation coefficient values of three components between plain image and successful decrypted image are 1.0 (i.e., item 1) denoting the successful decrypted image (Fig. 8(a)) is all the same as the original color image (Fig. 4(a)). The result represents that the successful decrypted image possesses the property of no distortion. Conversely, in the item 5 of Table 6, the three correlation coefficient average values of three components between plain image and failed decrypted images are much smaller (they are near to ideal value 0.0), which denotes the failed decrypted image and original color image are almost uncorrelated, and it also shows the nice cryptographic characteristic in ciphers.

Table 3. Correlation coefficients of red, green, and blue components of color plain image and color cipher images

Item	Correlation	Red component	Green component	Blue component
1	Color plain image (Fig. 4(a))	0.990025	0.984573	0.953979
2	Color cipher image (Fig. 5(a))	0.030142	0.012145	0.025011
3	Color cipher image (Fig. 6(a))	0.024069	0.005835	0.002961
4	Color cipher image (Fig. 7(a))	0.021741	0.008127	0.029471
5	The average for items 2-4	0.025317	0.008702	0.019148

Table 4. Correlation coefficients of same position among red, green, and blue components

Item	Correlation	Between red and green components	Between red and blue components	Between green and blue components
1	Color plain image (Fig. 4(a))	0.878634	0.676363	0.910647
2	Color cipher image (Fig. 5(a))	0.002715	0.001369	0.001302
3	Color cipher image (Fig. 6(a))	0.000724	0.001069	0.000612
4	Color cipher image (Fig. 7(a))	0.002581	0.002548	0.000875
5	The average for items 2-4	0.002007	0.001662	0.000930

Table 5. Correlation coefficients of adjacent position among red, green, and blue components

Item	Correlation	Between red and green components	Between red and Blue components	Between green and Blue components
1	Color plain image (Fig. 4(a))	0.871627	0.675574	0.900630
2	Color cipher Image (Fig. 5(a))	0.000237	0.002053	0.001043
3	Color cipher Image (Fig. 6(a))	0.003067	0.001341	0.001375
4	Color cipher Image (Fig. 7(a))	0.000261	0.001575	0.002058
5	The average for items 2-4	0.001188	0.001656	0.001492

Table 6. Correlation coefficients between plain image and decrypted images

Item	Correlation	Red component	Green component	Blue component
1	Between plain image (Fig. 4(a)) and successful decrypted image (Fig. 8(a))	1.0	1.0	1.0
2	Between plain image (Fig. 4(a)) and failed decrypted image (Fig. 8(b))	0.000845	0.000201	0.000731
3	Between plain image (Fig. 4(a)) and failed decrypted image (Fig. 8(c))	0.001278	0.000649	0.002151
4	Between plain image (Fig. 4(a)) and failed decrypted image (Fig. 8(d))	0.002761	0.000419	0.001301
5	The average for items 2-4	0.001628	0.000423	0.001394

6. Conclusions

In this paper, a novel cryptographic system with adjustable secret key space for color image security using the chaotic APFM nonlinear adaptive filter is proposed, in which the adjustable secret key space overcomes the issue for acquiring enough security strength of secret key length. The color cipher images possess nice randomness properties for color image security. The security analyses demonstrate that the proposed scheme is a secure cryptographic system.

REFERENCES

[1] G. Chen, Y.B. Mao, C.K. Chui, 2004, A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos, Solitons & Fractals 21, 749–761.

[2] Y. Wang, K.W. Wong, X.F. Liao, G.R. Chen, 2011, A new chaos-based fast image encryption algorithm, Applied Soft Computing 11, 514–522.

[3] M. Karimi-Ghartemani, A.K. Ziarani, 2003, Periodic orbit analysis of two dynamical systems for electrical engineering applications, J. Eng. Math. 45 (2), 135-154.

[4] Data Encryption Standard (DES), 1999, FIPS PUB 46-3, http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf.

[5] Advanced Encryption Standard (AES), 2001, FIPS PUB 197, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

[6] X. Ge, F.L. Liu, B. Lu, W. Wang, J. Chen, 2010, An image encryption algorithm based on spatiotemporal chaos in DCT domain, The 2nd IEEE International Conference on Information Management and Engineering, 267–270.

[7] AS. Alghamdi, H. Ullah, A secure iris image encryption technique using bio-chaotic algorithm, 2010, Int J Comput Netw Secur 2(4), 78–84.

[8] N.R. Zhou, Y.X. Wang, L.H. Gong, H. He, J.H. Wu, 2011, Novel single-channel color image encryption algorithm based on chaos and fractional Fourier transform. Optics Communications 284, 2789–2796.

[9] Y. Wang, K.W. Wong, X.F. Liao, T. Xiang, G.R. Chen, 2009, A chaos based image encryption algorithm with variable control parameters, Chaos, Solitons & Fractals 41 (4), 1773–1783.

[10] R.C.-W. Phan, 2007, Reducing the exhaustive key search of the Data Encryption Standard (DES), Comput. Stand. Inter. 29 (5), 528-530.

[11] S. Heron, Advanced Encryption Standard (AES), 2009, Netw. Security 2009 (12), 8-12.

[12] Recommendation for Key Management: Part 1: General (Revision3), NIST SP 800-57, http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_part1_rev3_general.pdf (2012).

[13] M.S. Tavazoei, M. Haeri, 2009, Chaos in the APFM nonlinear adaptive filter, Signal Processing 89 (5), 697-702.

[14] N. Bigdeli, Y. Farid, K. Afshar, 2012, A novel image encryption/decryption scheme based on chaotic neural networks, Engineering Applications of Artificial Intelligence 25, 753–765.

[15] M. Francois a, T. Grosges, D. Barchiesi, R. Erra, 2012, A new image encryption scheme based on a chaotic function, Signal Processing: Image Communication 27, 249–259.

[16] A. Kanso, M. Ghebleh, A novel image encryption algorithm based on a 3D chaotic map, 2012, Commun Nonlinear Sci Numer Simulat 17, 2943–2959.

[17] A. H. Abdullah, R. Enayatifar, M. Lee, 2012, A hybrid genetic algorithm and chaotic function model for image encryption, Int. J. Electron. Commun. (AEÜ) 66, 806– 816.