# A Novel Self-adaptive Color Image Encryption Scheme

Ruisong Ye, Meng Ge, Peiling Huang, Huan Li

*Department of Mathematics, Shantou University, Shantou, Guangdong, 515063, China*

***Abstract***— *A novel self-adaptive color image encryption scheme with exchange strategy is proposed. The 2D skew tent map is used to generate chaotic sequences to exchange the 4 higher bits part and the 4 lower bits part at half-pixel level with respect to the red, green, blue color components of the plain-image. The resulted three base color components are combined horizontally and encrypted simultaneously then to reduce the correlations among the three base color components. Moreover, self-adaptive diffusion process is adopted to encrypt the red, green, blue components in a cross way. The security and performance of the proposed image encryption scheme have been analyzed. All the experimental results show that the proposed scheme is secure and effective for practical application.*

**Keywords** —*2D skew tent map, chaotic system, exchange strategy, image encryption.*

## I. INTRODUCTION

With the rapid development of computer network technique and multimedia processing technology, large amounts of information, such as sound, image, video, are transmitted over the network, and consequently people pay more attention to information security [1]. As a matter of fact, more than one-third of the information transmitting on the network is image information, therefore, the security transmission and the storage of image information are highly focused. It is well known that chaotic systems own some perfect natures, such as high sensitivity to initial conditions and system parameters, ergodicity, pseudo-randomness etc. These good chaotic natures agree with the fundamental requirements such as confusion and diffusion in cryptography, and therefore chaotic systems provide a potential candidate for constructing cryptosystems. Chaos-based image encryption schemes have been extensively studied and developed in the last decades [2-9].

In this paper, we present a novel color image encryption scheme with a half-pixel level exchange strategy and self-adaptive mechanism. The exchange strategy between the 4 higher bits part and the 4 lower bits part of the three base color components will improve the security and performance significantly. The color image encryption scheme proposed consists of two kinds of operations: half-pixel level exchange operation between the 4 higher bits part and the 4 lower bits part, substitution operation cross the three base color components. To achieve desirable key sensitivity and plaintext sensitivity, the operations are designed to be dependent on the content of plain-image. As a result, the proposed image scheme owns good resistance to known-plaintext and chosen-plaintext attacks. The diffusion stage is performed globally with respect to whole image to improve the encryption rate. The exchange and substitution operations achieve good diffusion effect and shows good resistance against differential analysis as well. The security and performance analysis of the proposed image encryption are carried out thoroughly. All the experimental results show that the proposed image encryption scheme is highly secure and demonstrates excellent performance.

## II. THE PROPOSED IMAGE ENCRYPTION SCHEME

Read a color plain-image $P$ expressed by a 3D matrix with size $H \times W \times 3$. We assume that the three base color components are denoted by 2D matrices $R, G, B$ respectively. The three base color components $R, G, B$ are divided into two parts consisting of the 4 higher bits and the 4 lower bits respectively. We denote them to be $RH, RL$, $GH, GL, BH, BL$. Then the exchange operation is performed between $RH$ and $RL$, $GH$ and $GL$, $BH$ and $BL$ respectively. Moreover, the exchange operation is designed to be related to the content of the plain-image. After the exchange operation between the 4 higher bits part and the 4 lower bits part, the resulted $RH, RL, GH, GL, BH, BL$ are then integrated into $R, G, B$ with 256 gray scale levels, which are combined horizontally and encrypted simultaneously by the same exchange operation, and this greatly reduces the relationship among the three base color components. The substitution operation is applied at the whole image level to achieve the diffusion effect. The complete proposed image encryption scheme is composed of two rounds of exchange process and one substitution process. It is outlined as follows.

Step 1. Generation of pseudo-random sequences $x, y$. With cipher keys $x_0, y_0$, $a_1, b_1$ and $N_1$, we iterate the 2D skew tent map (1) for $N_1$ times and reject the transient points $\{(x_k, y_k) : k=0,$

$1,\mathrm{L}\ ,N_1-1\}$ to avoid the harmful effect. The values of $(x_0,y_0)$ are reset to be $(x_{N_1},y_{N_1})$ and the 2D skew tent map (1) with new initial values $(x_0,y_0)$ is applied to yield $\{(x_k,y_k):k=1,\mathrm{L}\ ,HW\}$.

$$(x_{n+1},y_{n+1})=\begin{cases}(x_n/a,y_n/b), & \text{if } (x_n,y_n)\in[0,a]\times[0,b],\\ (x_n/a,(1-y_n)/(1-b)), & \text{if } (x_n,y_n)\in[0,a]\times(b,1],\\ ((1-x_n)/(1-a),y_n/b), & \text{if } (x_n,y_n)\in(a,1]\times[0,b],\\ ((1-x_n)/(1-a),(1-y_n)/(1-b)), & \text{if } (x_n,y_n)\in(a,1]\times(b,1].\end{cases} \quad (1)$$

Step 2. Sort two sequences $x_k,y_k,k=1,\mathrm{L}\ ,HW$ in ascendant order to get the new sequences $x_k^{'},y_k^{'},k=1,\mathrm{L}\ ,HW$, and get the position indices $t_k,s_k,k=1,\mathrm{L}\ ,HW$ such that $x_k^{'}=x_{t_k}$, $y_k^{'}=y_{s_k}$ respectively. We get two P-boxes $T,S$:

$$T=\{t_1,\mathrm{L}\ ,t_{HW}\},S=\{s_1,\mathrm{L}\ ,s_{HW}\}.$$

Step 3. Perform the exchange operation. Calculate the sum of all the pixels' gray values of $RH,RL$ respectively and the value of $k1$:

$$sum_1=GH\ 1,1\ +\ldots+GH\ 1,W\ +\ GH\ 2,1\ +\ldots+GH\ H,W\ ,$$

$$sum_2=GL\ 1,1\ +\ldots+GL\ 1,W\ +\ GL\ 2,1\ +\ldots+GL\ H,W\ ,$$

$$k1=\mathrm{mod}(sum_1+sum_2,2).$$

If $k1=0$, then we exchange the 4-bit gray values of pixel pairs between $GH$ and $GL$ according to the yielded P-box $T$ by

$$GH(i)\leftrightarrow GL(t_i),i=1,\mathrm{L}\ ,HW,$$

otherwise we exchange them by P-box $S$ using

$$GH(i)\leftrightarrow GL(s_i),\ i=1,2,\mathrm{L}\ ,HW.$$

The same operation is also performed with respect to $GH,GL$ and $BH,BL$. Then we integrate the resulted $RH,RL,GH,GL,BH,BL$ into three color components by

$$R=RH\times16+RL,$$
$$G=GH\times16+GL,$$
$$B=BH\times16+BL.$$

The resulted R, G, B are scrambled by the P-boxes $T,S$ once again according to the value of $k1$. If $k1=0$, then

$$R(i)\leftarrow R(T(i)),G(i)\leftarrow G(T(i)),B(i)\leftarrow B(T(i)),$$

else

$$R(i)\leftarrow R(S(i)),G(i)\leftarrow G(S(i)),B(i)\leftarrow B(S(i)).$$

Step 4. Generation of pseudo-random sequences $w,z$. With cipher keys $w_0,z_0$, $a_2,b_2$ and $N_2$, we iterate the 2D skew tent map (1) for $N_2$ times and reject the transient points $\{(z_k,w_k):k=0,1,\mathrm{L}\ ,N_2-1\}$ to avoid the harmful effect. The values of $(w_0,z_0)$ are reset to be $(w_{N_2},z_{N_2})$ and the 2D skew tent map with new initial values $(w_0,z_0)$ is used to yield $\{(w_k,z_k):k=1,\mathrm{L}\ ,3HW\}$. Sort two sequences $w_k,z_k,k=1,\mathrm{L}\ ,3HW$ in ascendant order to get the new sequences $w_k^{'},z_k^{'},k=1,\mathrm{L}\ ,3HW$, and get the position indices $u_k,v_k,k=1,\mathrm{L}\ ,3HW$, such that $w_k^{'}=w_{u_k}$, $z_k^{'}=z_{v_k}$ respectively. We get two P-boxes $U,V:U=\{u_1,\mathrm{L}\ ,u_{3HW}\},S=\{v_1,\mathrm{L}\ ,v_{3HW}\}$.

Step 5. The encrypted three base color components $R,G,B$ are combined horizontally and encrypted simultaneously by the same exchange operations as those in Step 3. We then obtain the encrypted three color components $R,G,B$.

Step 6. The resulted $\{(x_k,y_k):k=1,\mathrm{L}\ ,HW\}$ at Step 1 is used to generate the pseudo-random gray value sequences by

$$x(n)=mod(\,floor(x_n\times10^{14}),256),$$
$$y(n)=mod(\,floor(y_n\times10^{14}),256),n=1,\mathrm{L}\ ,HW,$$

where function *floor(x)* returns the largest integer less than or equal to *x*, and function *mod(x,y)* returns the remainder after *y* divided by *x*. The vectors $x(n),y(n),n=1,2,\mathrm{L}\ ,HW$ are then converted into two matrices $X,Y$ with size $H\times W$. We Calculate the sum of all the pixels' gray values of $R,G$ and determine the value of $k2,k3$ by

$$k2=\mathrm{mod}(\sum_{i=1}^{H}\sum_{j=1}^{W}R(i,j),2),$$
$$k3=\mathrm{mod}(\sum_{i=1}^{H}\sum_{j=1}^{W}G(i,j),2).$$

Then we substitute the pixels values of $R,G$ components by

$$G1=\begin{cases}\mathrm{mod}(G+R+X,256), & \text{if } k2=0,\\ \mathrm{mod}(G+R+Y,256), & \text{if } k2=1,\end{cases}$$

$$B1=\begin{cases}\mathrm{mod}(B+G1+X,256), & \text{if } k3=0,\\ \mathrm{mod}(B+G1+Y,256), & \text{if } k3=1.\end{cases}$$

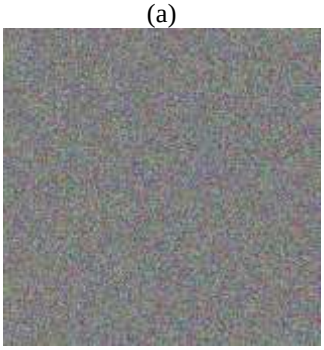
The sum of all the pixels' gray values of $B1$ is then used to determine the value of $k4$ and change the values of $R$ by

$$k4=\mathrm{mod}(\sum_{i=1}^{H}\sum_{j=1}^{W}B1(i,j),2)\ ,$$

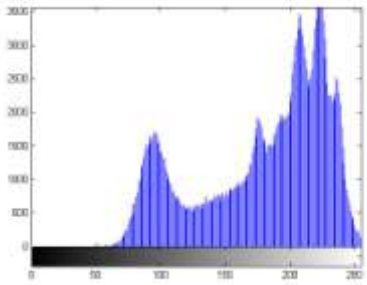
$$R1=\begin{cases}\mathrm{mod}(R+B1+X,256), & \text{if } k4=0,\\ \mathrm{mod}(R+B1+Y,256), & \text{if } k4=1.\end{cases}$$

The resulted color cipher-image of plain-image Lena (Fig. 1(a)) consists of the three base color components $R1,G1,B1$, as shown in Fig. 1(b).

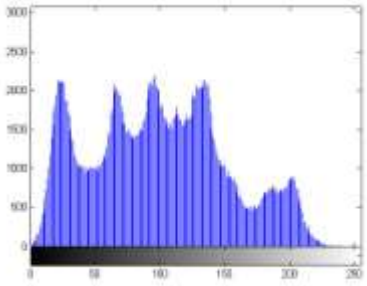
(a)



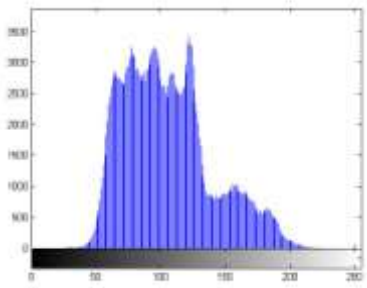
(b)



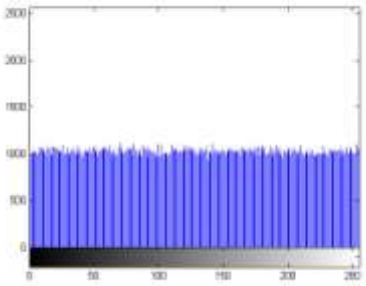
(c)



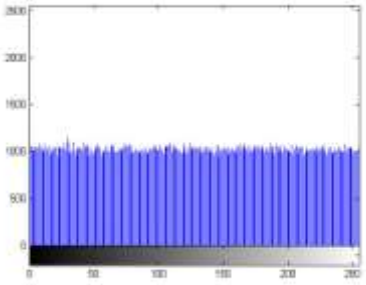
(d)



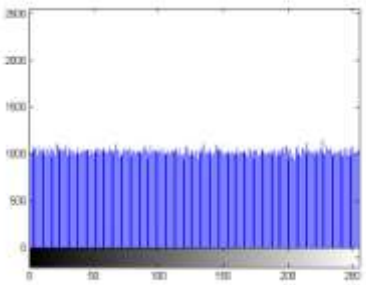
(e)



(f)



(g)



(h)

Fig. 1. The encrypted results: (a) plain-image Lena; (b) cipher-image; (c)-(e) histograms for $R,G,B$ components of Lena; (f)-(h) histograms for $R,G,B$ components of cipher-image.

## III. Performance Analysis

### A. Histogram Analysis

Histogram analysis visually shows the pixel distribution over the available intensity levels. For a 24-bit color image, three histograms can be drawn for each 8-bit red, green and blue channel. Encrypt the color image Lena one round with cipher keys $(x_0, y_0, a, b, N_1, w_0, z_0, a_1, b_1, N_2)$ to be (0.371, 0.589, 0.733, 0.89, 100, 0.51, 0.39, 0.13, 0.49, 120), and then plot the histograms of red, green, blue components of plain-image and cipher-image as shown in Fig. 1(c)-(h). One can conclude from the histograms of the cipher-image that they are fairly uniform and significantly different from the corresponding histograms of the plain-image.

### B. Correlation Coefficient Analysis

For one nature image with definite visual contents, each pixel is highly related to its adjacent pixels either in horizontal, vertical or diagonal direction.

An ideal encryption cryptosystem should generate cipher-images with less correlation between adjacent pixels. We calculate the correlation coefficient of the whole pairs by

$$Cr = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}},$$

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

$$E(x) = \frac{1}{T}\sum_{i=1}^{T} x_i,\ \ D(x) = \frac{1}{T}\sum_{i=1}^{T}(x_i - E(x))^2,$$

where $x_i, y_i$ form the $i$-th pair of horizontally, vertically or diagonally adjacent pixels and $T = H \times (W-1), (H-1) \times W, (H-1) \times (W-1)$ for the three cases respectively. The correlation coefficients of horizontally, vertically, diagonally adjacent pixels for plain-image Lena and its cipher-image are given in Table 1. We can see from Table 1 that the proposed image encryption scheme significantly reduces the correlation between the adjacent pixels of the plain-image.

We also demonstrate the correlations between the red, green, blue components of the plain-image and the cipher-image. The experimental results are shown in Table 2, Table3. It is clear from Table 2 that the coefficients Crg, Crb, Cgb between the R, G, B components of the plain-image is large, while those of the cipher-image is close to zero. The correlation coefficients between the red, green, blue components of the plain-image and cipher-image are all close to zero. All these results indicate that the proposed image encryption scheme significantly reduces the correlations of the three base color components.

Table 1. Correlation coefficients between adjacent pixels of plain-image and cipher-image.

| | | Correlation between adjacent pixels | | |
|---|---|---|---|---|
| | | Red | Green | Blue |
| Horizontal | Plain-image | 0.9753 | 0.9871 | 0.9634 |
| | Cipher-image | 0.0004 | 0.0015 | -0.0025 |
| Vertical | Plain-image | 0.9748 | 0.9872 | 0.9630 |
| | Cipher-image | -0.0017 | 0.0005 | -0.0029 |
| Diagonal | Plain-image | 0.9532 | 0.9741 | 0.9334 |
| | Cipher-image | 0.0004 | 0.0024 | -0.0002 |

Table 2. Correlation coefficients between the R,G,B components within the plain-image and cipher-image.

| | Crg | Crb | Cgb |
|---|---|---|---|
| Plain-image Lena | 0.8856 | 0.6995 | 0.9191 |
| Cipher-image | -0.0028 | 0.0010 | -0.0029 |

Table 3. Correlation coefficients between the R,G,B components of plain-image and cipher-image.

| | | Plain-image | | |
|---|---|---|---|---|
| | | Red | Green | Blue |
| Cipher-image | Red | 0.0012 | 0.0015 | 0.0021 |
| | Green | 0.0008 | -0.0013 | -0.0023 |
| | Blue | 0.0012 | 0.0006 | -0.0007 |

### C. Information Entropy Analysis

Information entropy measures the randomness of information sequence [8]. It can be used to measure the uniformity of image histograms as well. The entropy $H(m)$ of a message source $m$ can be calculated by

$$H(m) = -\sum_{i=0}^{L-1} p(m_i)\log(p(m_i))\ \text{(bits)},$$

where $L$ is the total number of symbols $m$, $p(m_i)$ represents the probability of occurrence of symbol $m_i$ and log denotes the base 2 logarithm so that the entropy is expressed in bits. For a 24-bit color image, the information entropy for red, green, blue components can be calculated similarly. We have calculated the information entropy for plain- image Lena and its cipher-image. The results are shown in Table 4. The value of information entropy for the cipher-image is very-very close to the expected value of truly random image, i.e., 8bits. Hence the proposed encryption scheme is extremely robust against entropy attacks.

Table 4. Information entropy analysis.

| | Red | Green | Blue |
|---|---|---|---|
| Plain-image Lena | 7.2634 | 7.5899 | 6.9854 |
| Cipher-image | 7.9993 | 7.9993 | 7.9993 |

### D. Differential Attack Analysis

Differential cryptanalysis studies the issue that how differences in a plaintext can affect the resultant differences in the ciphertext with the same cipher key. If one slight difference in the plain-image will cause significant, random and unpredictable changes in the cipher-image, then the encryption scheme will resist differential analysis attack efficiently. Two most common measures NPCR (number of pixel change rate) and UACI (unified average changing intensity) are used to test the robustness of image cryptosystems against the differential cryptanalysis. If $C^{R/G/B}$ and $\bar{C}^{R/G/B}$ represent the $R,G,B$ channels for two cipher-images, then NPCR and UACI for each color channel are defined by

$$\text{NPCR}^{R/G/B} = \frac{\sum_{i=1}^{H}\sum_{j=1}^{W} D_{i,j}^{R/G/B}}{W \times H} \times 100\%,$$

$$D_{i,j}^{R/G/B} = \begin{cases} 1, & \text{if } C_{i,j}^{R/G/B} \neq \bar{C}_{i,j}^{R/G/B}, \\ 0, & \text{if } C_{i,j}^{R/G/B} = \bar{C}_{i,j}^{R/G/B}, \end{cases}$$

$$\mathrm{UACI}^{R/G/B} = \frac{1}{W \times H} \sum_{i=1}^{H} \sum_{j=1}^{W} \frac{| C_{i,j}^{R/G/B} - \bar{C}_{i,j}^{R/G/B} |}{2^{L^{R/G/B}} - 1} \times 100\%.$$

We have performed the differential analysis by calculating NPCR and UACI on plain-image Lena. The analysis has been done by randomly choosing 100 pixels in plain-image, and changing one of the three color intensity values by one unit randomly at the selective pixel as well. The averages of 100 NPCR values and 100 UACI values thus obtained for all three color components are given in Table 5. It is clear that the NPCR and UACI values are very close to the expected values, thus the proposed image encryption technique shows good sensitivity to plaintext and hence invulnerable to differential attacks.

Table 5. Difference analysis of plain-image Lena.

| Average NPCR (%) | | | Average UACI (%) | | |
|---|---|---|---|---|---|
| Red | Green | Blue | Red | Green | Blue |
| 99.5974 | 99.6053 | 99.6059 | 33.4174 | 33.4095 | 33.4516 |

### *E. Key Sensitivity Analysis*

Good key sensitivity is an essential feature of an effective cryptosystem. Key sensitivity of a cryptosystem can be observed and simulated from two aspects: (i) significantly different cipher-images should be generated even if keys with minor difference are used to encrypt the same plain-image; (ii) the cipher-image cannot be correctly decrypted even if there is tiny difference between encryption and decryption keys. As for key sensitivity analysis, we will use the following cipher keys to perform the simulations (one is master cipher key MKEY, the other keys are yielded by introducing a slight change to one of the parameters of master cipher key with all other parameters unchanged). Master cipher key is set to be $(x_0, y_0, a, b, N_1, w_0, z_0, a_1, b_1, N_2)$ = (0.371, 0.589, 0.733, 0.89, 100, 0.51, 0.39, 0.13, 0.49, 120). Ten slightly different keys are

SKEY1 $(x_0 - 10^{-14}, y_0, a, b, N_1, w_0, z_0, a_1, b_1, N_2)$ ;

SKEY2 $(x_0, y_0 - 10^{-14}, a, b, N_1, w_0, z_0, a_1, b_1, N_2)$ ;

SKEY3 $(x_0, y_0, a - 10^{-14}, b, N_1, w_0, z_0, a_1, b_1, N_2)$ ;

SKEY4 $(x_0, y_0, a, b - 10^{-14}, N_1, w_0, z_0, a_1, b_1, N_2)$ ;

SKEY5 $(x_0, y_0, a, b, N_1 + 1, w_0, z_0, a_1, b_1, N_2)$ ;

SKEY6 $(x_0, y_0, a, b, N_1, w_0 - 10^{-14}, z_0, a_1, b_1, N_2)$ ;

SKEY7 $(x_0, y_0, a, b, N_1, w_0, z_0 - 10^{-14}, a_1, b_1, N_2)$ ;

SKEY8 $(x_0, y_0, a, b, N_1, w_0, z_0, a_1 - 10^{-14}, b_1, N_2)$

SKEY9 $(x_0, y_0, a, b, N_1, w_0, z_0, a_1, b_1 - 10^{-14}, N_2)$ ,

SKEY10 $(x_0, y_0, a, b, N_1, w_0, z_0, a_1, b_1, N_2 + 1)$ .

(i) To estimate the key sensitivity for the first case, we encrypt plain-image Lena with MKEY and get the first cipher-image, then we encrypt Lena with SKEY1-SKEY10 and get ten cipher-images respectively. The correlation coefficients between the first cipher-image and the other ten cipher-images are calculated. The experimental results are shown in Table 6. From the results, we can see that all the correlation coefficients are very small which indicate that even there is only slightly difference between the cipher keys, the cipher-images are greatly different. Hence the proposed encryption scheme is extremely sensitive to the cipher keys.

(ii) Decryption using keys with minor difference are also performed in order to evaluate the key sensitivity of the second case. Firstly, we decrypt the cipher image using MKEY and we get the plain-image Lena. Secondly, ten decrypted images are produced as we decrypt the cipher-image using SKEY1-SKEY10 respectively. We have computed the correlation coefficients between Lena and this ten decrypted images, the results have been given in Table 7. One can see from Table 7 that even there is only a tiny difference between the decipher keys, the deciphered images have low correlation coefficients with the plain-image Lena. So for the second case, the proposed encryption scheme is of highly sensitive to the cipher keys too.

Table 6. Key sensitivity analysis I.

| | Correlation coefficients between the encrypted images obtained using MKEY and | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | SKEY1 | SKEY2 | SKEY3 | SKEY4 | SKEY5 | SKEY6 | SKEY7 | SKEY8 | SKEY9 | SKEY10 |
| Crr | 0.0022 | 0.0022 | -0.0004 | 0.0020 | 0.0001 | -0.0019 | 0.0012 | 0.0008 | -0.0010 | -0.0002 |
| Crg | 0.0014 | 0.0026 | 0.0047 | 0.0007 | -0.0010 | 0.0008 | -0.0032 | 0.0002 | 0.0023 | -0.0010 |
| Crb | -0.0003 | -0.0019 | 0.0001 | -0.0014 | -0.0007 | -0.0002 | 0.0025 | 0.0010 | 0.0008 | -0.0024 |
| Cgr | -0.0033 | -0.0028 | -0.0006 | -0.0004 | 0.0015 | 0.0047 | 0.0001 | -0.0009 | -0.0010 | 0.0001 |
| Cgg | 0.0015 | 0.0007 | 0.0014 | -0.0024 | 0.0028 | 0.0007 | 0.0041 | 0.0024 | 0.0042 | -0.0021 |
| Cgb | 0.0025 | -0.0009 | -0.0006 | -0.0015 | -0.0007 | -0.0005 | -0.0012 | 0.0002 | 0.0001 | 0.0043 |
| Cbr | 0.0010 | 0.0023 | -0.0006 | -0.0018 | 0.0016 | -0.0005 | 0.0007 | 0.0025 | 0.0023 | 0.0016 |
| Cbg | -0.0021 | 0.0011 | -0.0011 | -0.0008 | 0.0003 | 0.0056 | 0.0017 | -0.0030 | -0.0032 | 0.0028 |
| Cbb | -0.0002 | -0.0066 | 0.0044 | -0.0002 | -0.0017 | 0.0034 | -0.0037 | -0.0026 | 0.0005 | 0.0018 |

Table 7. Key sensitivity analysis II.

| | Correlation coefficients between the decrypted images obtained using MKEY and | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | SKEY1 | SKEY2 | SKEY3 | SKEY4 | SKEY5 | SKEY6 | SKEY7 | SKEY8 | SKEY9 | SKEY10 |
| Crr | -0.0015 | 0.0001 | 0.0042 | -0.0029 | -0.0008 | -0.0003 | -0.0014 | -0.0020 | -0.0034 | 0.0003 |
| Crg | -0.0039 | 0.0009 | 0.0017 | -0.0017 | 0.0045 | 0.0021 | 0.0000 | 0.0023 | 0.0012 | 0.0025 |
| Crb | 0.0012 | -0.0018 | 0.0004 | -0.0009 | -0.0013 | -0.0024 | -0.0004 | -0.0034 | 0.0026 | 0.0000 |
| Cgr | -0.0010 | -0.0000 | 0.0043 | -0.0029 | -0.0004 | -0.0002 | -0.0023 | -0.0024 | -0.0027 | -0.0003 |
| Cgg | -0.0039 | 0.0014 | 0.0007 | -0.0005 | 0.0047 | 0.0017 | -0.0004 | 0.0019 | 0.0023 | 0.0027 |
| Cgb | 0.0013 | 0.0000 | 0.0015 | -0.0005 | -0.0000 | -0.0034 | -0.0004 | -0.0041 | 0.0010 | 0.0008 |
| Cbr | -0.0003 | 0.0006 | 0.0047 | -0.0022 | -0.0008 | -0.0007 | -0.0022 | -0.0022 | -0.0006 | -0.0005 |
| Cbg | -0.0029 | 0.0007 | 0.0001 | -0.0010 | 0.0036 | 0.0008 | -0.0002 | 0.0016 | 0.0026 | 0.0025 |
| Cbb | 0.0013 | 0.0005 | 0.0019 | -0.0009 | 0.0007 | 0.0031 | -0.0001 | -0.0034 | 0.0009 | 0.0008 |

## IV. CONCLUSIONS

In this paper, we present a novel color image encryption scheme with exchange strategy and self-adaptive mechanism based on the chaotic nature of 2D skew tent map. The 2D skew tent maps are applied to generate chaotic sequences applying to both the exchange stage and substitution stage. The exchange strategy is adopted to exchange the 4 higher bits part and the 4 lower bits part of the three base color components. It greatly improves the security and performance as well as the encryption rate. Substitution operation cross the three base color components is also applied to enhance desirable key sensitivity and plaintext sensitivity. All the operations are designed to be dependent on the content of plain-image. As a result, the proposed image scheme owns good resistance to known-plaintext and chosen-plaintext attacks. The diffusion stage is performed globally with respect to whole image to improve the encryption rate. All the experimental results show that the proposed image encryption scheme is highly secure and demonstrates excellent performance.

## ACKNOWLEDGMENT

This research is supported by Entrepreneurship Training Program of Guangdong Colleges.

## REFERENCES

[1] D. R. Stinson, Cryptography: Theory and Practice. Boca Raton: CRC Press, 1995.

[2] J. Fridrich, Symmetric ciphers based on two-dimensional chaotic maps, International Journal of Bifurcation and Chaos, 8(1998), 1259–1284.

[3] R. Ye, A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism, Opt. Commun., 284(2011), 5290-5298.

[4] R. Ye, A novel image encryption scheme based on generalized multi-sawtooth maps, Fundamenta Informaticae, 133(2014), 87-104.

[5] V. Patidar, N. K. Pareek, G. Purohit, K. K. Sud, A robust and secure chaotic standard map based pseudorandom permutation-substitution scheme for image encryption, Optics Commun., 284(2011), 4331-4339.

[6] J. Chen, Z. Zhu, C. Fu, H. Yu, L. Zhang, An efficient image encryption scheme using gray code based permutation approach, Optics and Lasers in Engineering, 67 (2015), 191-204.

[7] Y. Zhang, X. Wang, A new image encryption algorithm based on non-adjacent coupled map lattices, Applied Soft Computing, 26 (2015),10-20.

[8] H. Liu, X. Wang, Color image encryption using spatial bit-level permutation and high-dimension chaotic system, Optics Communications, 284(2011), 3895–3903.

[9] J. Zhao, W. Guo, R. Ye A Chaos-based image encryption scheme using permutation-substitution architecture, International Journal of Computer Trends and Technology, 15: 4(2014), 174-185.

[10] C. E. Shannon, Communication theory of secrecy system. Bell Syst. Tech. J, 28(1949), 656–715.