Noname manuscript No.
(will be inserted by the editor)

Color Image Encryption in Non-RGB Color Spaces

Xin Jin · Sui Yin · Ningning Liu · Xiaodong Li · Geng Zhao · Shiming Ge*

Received: date / Accepted: date

Abstract To protect the contents of images in the mobile internet era during image storage and transmission, image encryption has achieved a tremendous success during the last decades. Traditional color image encryption method often use the RGB color space. We have the observation that in non-RGB color spaces, the luminance channels often contain more information for content recognition than the chroma channels do. Thus, in this paper we propose to use *high level* encryption schemes in more informative channels and *low level* encryption schemes in less informative channels. The 2D Arnold's cat map followed by the 3D Lu chaotic map are conducted in the luminance channel. The less complicated DNA coding and 1D logistic map based encryption scheme is leveraged in the chroma channels. We use this strategies in 4 typical non-RGB color spaces, i.e., YCbCr, YIQ, HSV, L*a*b*. We evaluate and compare the performances and the time consumptions of the methods in the 4 Non-RGB color spaces. The experimental results reveal that the encryption methods in Non-RGB color spaces can achieve similar results as the method that conducts the same encryption level in each channel of the RBG color space, including the resistance to several attacks such as brute-force attack, statistic attack, correlation attack, while consuming less time. The method in YCbCr color space performances the best in the time consumption.

Xin Jin, Sui Yin, Xiaodong Li, Geng Zhao
Beijing Electronic Science and Technology Institute, Beijing, 100070, P.R.China

Ningning Liu
University of International Business and Economics, School of Information technology and Management, Beijing, 100029, P.R.China

Shiming Ge*
Institute of Information Engineering, Chinese Academy of Sciences, Beijing, 100093, P.R.China *Corresponding Author E-mail: geshiming@iie.ac.cn

Keywords Color Image Encryption · Non-RGB · Color Space · Security Attack

1 Introduction

Cameras and smart phones are now used in everyday life. Tremendous images are transmitted to thousands of people by social network software and cloud storages. On August 31, 2014, a collection of almost 500 private pictures of various celebrities, mostly women, and with many containing nudity, were posted on the image board 4chan, and later disseminated by other users on websites and social networks such as Imgur, Reddit and Tumblr. The images were believed to have been obtained via a breach of Apple's cloud services suite iCloud. This event alerts that the privacy of us in the cloud is being threatened. Besides, once the government or military images are leaked, the state security will be violated. Thus image encryption technologies are required in order to accomplish a high level of security, integrity, confidentiality and to prevent unauthorized access of sensitive information during image storage or transmission over an insecure channel [1] [3] [4] [12] [13].

Current image encryption technologies mainly concentrate on gray image encryption [21] [2]. The use of RGB color space dominate the color image encryption methods. Little attention has been paid to non-RGB color spaces such as YCbCr, YIQ, HSV, L*a*b* color spaces. RGB color space is one of best widely used for handling and storing the data of image due to high connection between the red, green and blue components. Actually, RGB color space mixes the chroma and luminance components so it can't use in color analysis and segmentation methods based on color criteria [1].

As shown in figure 1, most of the non-RGB color spaces share a property that one channel contains more visual recognition information than those in other two channels. This property enables us to use *high level* encryption schemes in more informative channels and *low level* encryption schemes in less informative channels.

Recently, several image encryption methods in non-RGB color spaces have been proposed such as YCbCr [1] [6] and L*a*b* [5]. In this paper we present a comparative study of color image encryption operated in 4 typical non-RGB color spaces,i.e., YCbCr, YIQ, HSV, L*a*b*. We evaluate and compare the performances and the time consumptions of the methods in the 4 Non-RGB color spaces. The experimental results reveal that our encryption methods in Non-RGB color spaces can achieve similar results as the method that conducts the same encryption level in each channel of the RBG color space, including the resistance to several attacks such as brute-force attack, statistic attack, correlation attack, while consuming less time. The method in YCbCr color space performances the best in the time consumption.

The rest of this paper is organized as follow: In section 2, we give a brief review of the related work. In section 3, some preliminaries are described. In section 4, we introduce our image encryption methods in non-RGB color

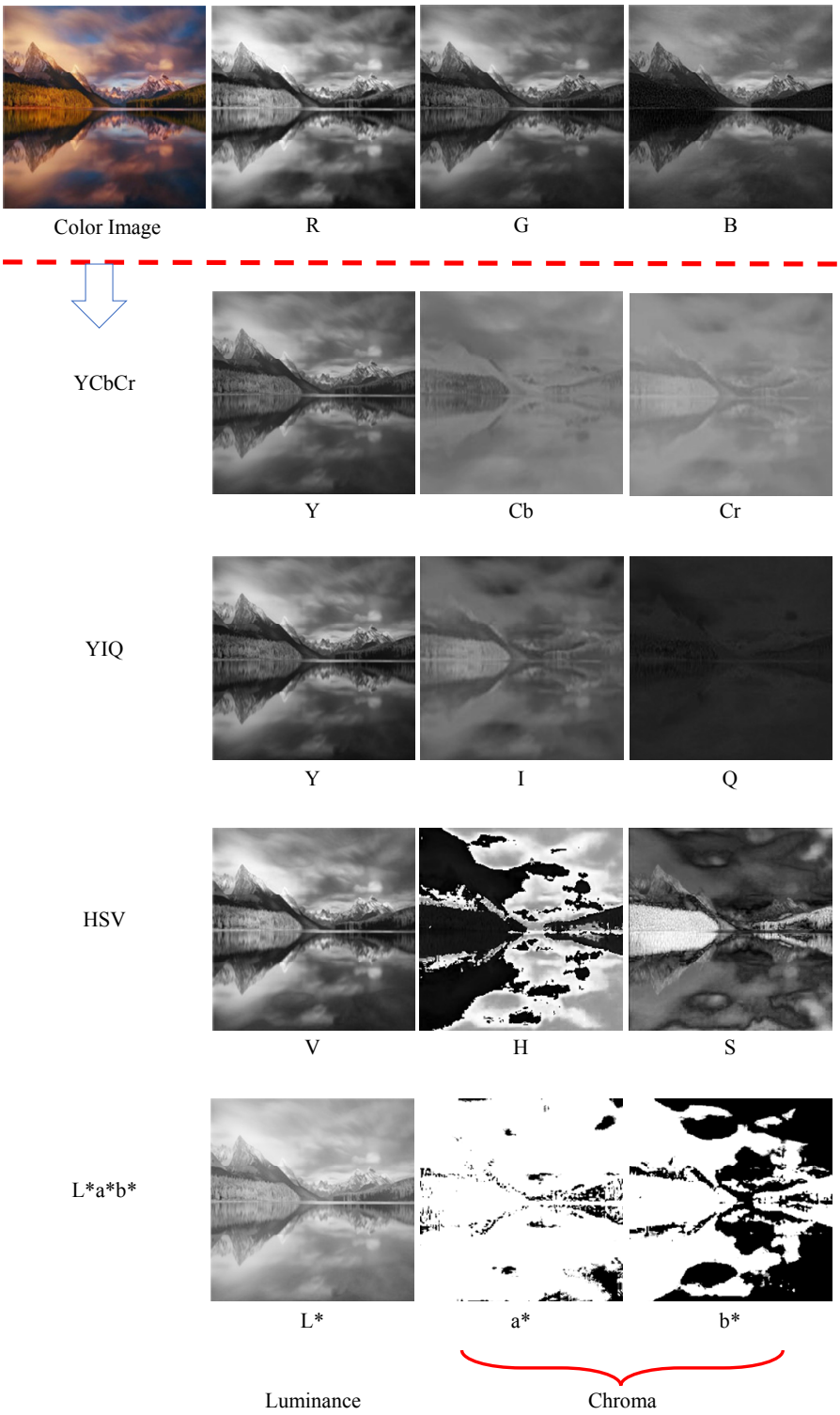

Fig. 1 Converting RGB to non-RGB color spaces, i.e., YCbCr, YIQ, HSV, L*a*b*. One can easily recognize the image contents from the Luminance Channels (LC), including the Y, Y, V, L* channels, but can almost find nothing from the Chroma Channels (CC), including the CbCr, IQ, HS, a*b* in the YCbCr, YIQ, HSV and L*a*b* color spaces.

spaces. We show simulation results in section 4.4. The security and performance analysis are presented in section 5. At last, we give the conclusion and discussion in section 6. Parts of the technical details presented in this paper have previously appeared in our previous work [5] [6] [7]. All the figures and results are novel for the systematically comparative study.

2 Previous Work

The particular properties of chaos, such as sensitivity to initial conditions and system parameters, pseudo-randomness, ergodicity and so on, have granted chaotic dynamics as a promising alternative for the conventional cryptographic algorithms. The inherent properties connect it directly with cryptographic characteristics of confusion and diffusion, which is presented in Shannon‘s works. High-dimensional chaotic system is more reliable to design secure image encryption scheme because of its high complexity [20] [2] [8] [9]. Some cryptosystems, which are based on a low-dimensional chaotic map, have obvious drawbacks, such as short period and small key space.

Meanwhile, The DNA cryptography became a novel cryptographic tool [10]. The DNA computing based image encryption generally contains three stages [2]:

- Encode the pixels of the plain image into DNA sequence.
- Decompose the pixel into 4 DNA elements, which can make the confusion and diffusion more efficient.
- Use DNA operation rules to encrypt each pixel.

Zhang et al. [21] propose a gray image encryption method by using 1D logistic map and DNA encoding . However, Hermassi et al. [22] point out that the method of [21] is not reversible, namely, it can only encrypt the plain image, but has no method on the cipher image in the case of known the secret key. Jin et al. [7] add a random matrix to the DNA addition and make the encryption reversible.

Recently, several image encryption methods in non-RGB color spaces have been proposed such as YCbCr [1] [6] and L*a*b* [5]. In this paper, we extend the method of [6] and [5] to HSV and YIQ color spaces. We make a comparative study of encrypting color images in the RGB, YCbCr, YIQ, HSV, and L*a*b* color spaces. The resistance to several attack and time consumption are compared systemically. Besides, we evaluate these encryption methods in a large scale image dataset.

3 Preliminaries

We choose four typical and common used color spaces for comparison, include YCbCr, YIQ, HSV and L*a*b*. Each of these four color spaces contains a luminance channel and two chroma channels. We adopt a low dimensional

chaotic map: 1D logistic map and two high dimensional chaotic maps: the 2D Arnold's cat map and the 3D Lu map.

3.1 Non-RGB Color Spaces

The YCbCr color space is a family of color spaces used as a part of the color image pipeline in video and digital photography systems. Y is the luminance component and Cb and Cr are the blue-difference and red-difference chroma components [14].

The YIQ color space is the color space used by the NTSC color TV system, employed mainly in North and Central America, and Japan. I stands for in-phase, while Q stands for quadrature, referring to the components used in quadrature amplitude modulation. Some forms of NTSC now use the YUV color space, which is also used by other systems such as PAL. The Y component represents the luma information, and is the only component used by black-and-white television receivers. I and Q represent the chrominance information. In YUV, the U and V components can be thought of as X and Y coordinates within the color space. I and Q can be thought of as a second pair of axes on the same graph, rotated 33; therefore IQ and UV represent different coordinate systems on the same plane [15].

The HSV color space is one of the most common cylindrical-coordinate representations of points in an RGB color model. HSV stands for hue, saturation, and value. This representations rearrange the geometry of RGB in an attempt to be more intuitive and perceptually relevant than the cartesian (cube) representation. Developed in the 1970s for computer graphics applications, HSV is used today in color pickers, in image editing software, and less commonly in image analysis and computer vision [16].

The L*a*b* color space is a color-opponent space with dimension L* for lightness and a* and b* for the color-opponent dimensions, based on non-linearly compressed (e.g. CIE XYZ color space) coordinates. The L* channel is more independent to color component and more close to human perception on lightness than RGB color space [17].

3.2 1D Logistic Map

The simple but efficient 1D logistic map is defined as follows:

$$\begin{aligned} &x_{n+1} = \mu x_n(1 - x_n) \\ &3.569945672... < \mu \leq 4, 0 \leq x_n \leq 1 \\ &n = 0, 1, 2, ... \end{aligned} \tag{1}$$

3.3 2D Arnold's Cat Map

In mathematics, Arnold's cat map is a chaotic map from the torus into itself, named after Vladimir Arnold, who demonstrated its effects in the 1960s using an image of a cat, hence the name [18]. Arnold's cat map transformation use for shuffling the pixels of color image and to perform extra security of cipher system. The 2D Arnolds cat transform does not alter the value of the image pixels. It only shuffles the data of image and it given in Eq. 2 for image encryption and Eq. 3 for image decryption [1].

$$\begin{bmatrix} X' \\ Y' \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & p*q+1 \end{bmatrix} * \begin{bmatrix} X \\ Y \end{bmatrix} \bmod U \tag{2}$$

$$\begin{bmatrix} X \\ Y \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & p*q+1 \end{bmatrix}^{-1} * \begin{bmatrix} X' \\ Y' \end{bmatrix} \bmod U, \tag{3}$$

where p and q represent the positive secret keys. (X, Y) is the original 2D variables. (X', Y') is the new values of (X, Y). U is the upper bounds of values of X and Y.

3.4 3D Lu Map

The Lu map is a 3D chaotic map. It is described by Eq. 4

$$\begin{cases} \dot{x} = a(y - x) \\ \dot{y} = -xz + cy, \\ \dot{z} = xy - bz \end{cases} \tag{4}$$

where (x, y, z) are the system trace. (a, b, c) are the system parameters. When $a = 36, b = 3, c = 20$, the system contain a strange attractor and being in chaotic state.

3.5 DNA Encoding

A DNA sequence contains four kinds of nucleic acids. $A - T$ is a couple, and $G - C$ is a couple. As we all know, in the binary, $1 - 0$ is a couple. Thus $00 - 11$ is a pair. $10 - 01$ is a pair. In this paper, we use A, G, C, T to replace 00, 01, 10 and 11. For each 8-bit image pixel, 4 nucleic acids can be used to represent it. For example, the pixel value 123 in decimal can be represented as a binary vector 01111011 and can be further encoded as a DNA sequence $AGTG$ [2]. Based on the above encoding rule, we use three kinds of operations for DNA encoding, as shown in Fig. 1.

Table 1 The DNA addition, DNA subtraction and DNA complement. The Cmp(X) is the complement of X. $X \in \{A, T, G, C\}$

DNA+	T	A	C	G	DNA-	T	A	C	G	X	Cmp(X)
T	C	G	T	A	T	C	G	T	A	A	T
A	G	C	A	T	A	A	C	G	T	T	A
C	T	A	C	G	C	T	A	C	G	C	G
G	A	T	G	C	G	G	T	A	C	G	C

4 Non-RGB Image Encryption

In this section, we describe the color image encryption method in non-RGB color spaces. As shown in Fig. 2, the upper part is the traditional RGB encryption [20]. Each channel of the RGB color space is fed into a high dimensional chaotic maps based encryption pipeline, for high security. The lower part is the non-RGB encryption. First we convert the plain image from RGB color space to non-RGB color spaces. Then the informative luminance channels are encrypted by 2 high dimensional chaotic maps, which is the same as the pipeline of that of the RGB encryption. The less informative chroma channels are encrypted by a low dimensional chaotic map for efficient computation.

Algorithm 1 Luminance channel confusion using Arnold's cat map

Input:
The plain luminance channel LC of the input image with resolution of $(N \times N)$.
Output:
The confused luminance channel LC^c.
1: Set the iteration number IT. Repeat the following 2 steps (2,3) IT times.
2: For each pixel (X, Y) in the plain luminance channel LC:

$$\begin{bmatrix} X' \\ Y' \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & p*q+1 \end{bmatrix} * \begin{bmatrix} X \\ Y \end{bmatrix} \bmod N, \tag{5}$$

where p and q represent the positive secret keys. (X, Y) is the original position of the image pixel of LC before shuffling. (X', Y') is the new position of the image pixel of LC^c after shuffling. N is the image resolution.
3: Set the new value of (X', Y') of LC^c as the original value of (X, Y) of LC.
4: **return** the confused luminance channel LC^c.

4.1 Color Conversion

We convert the RGB color space to non-RGB color spaces. The ranges of some channels are not from 0 to 255. For example, the L* coordinate ranges from 0 to 100. The possible range of a* and b* coordinates is independent of the color space that one is converting from, since the conversion below uses X and Y, which come from RGB. The a* and b* channels range from -128 to 127.

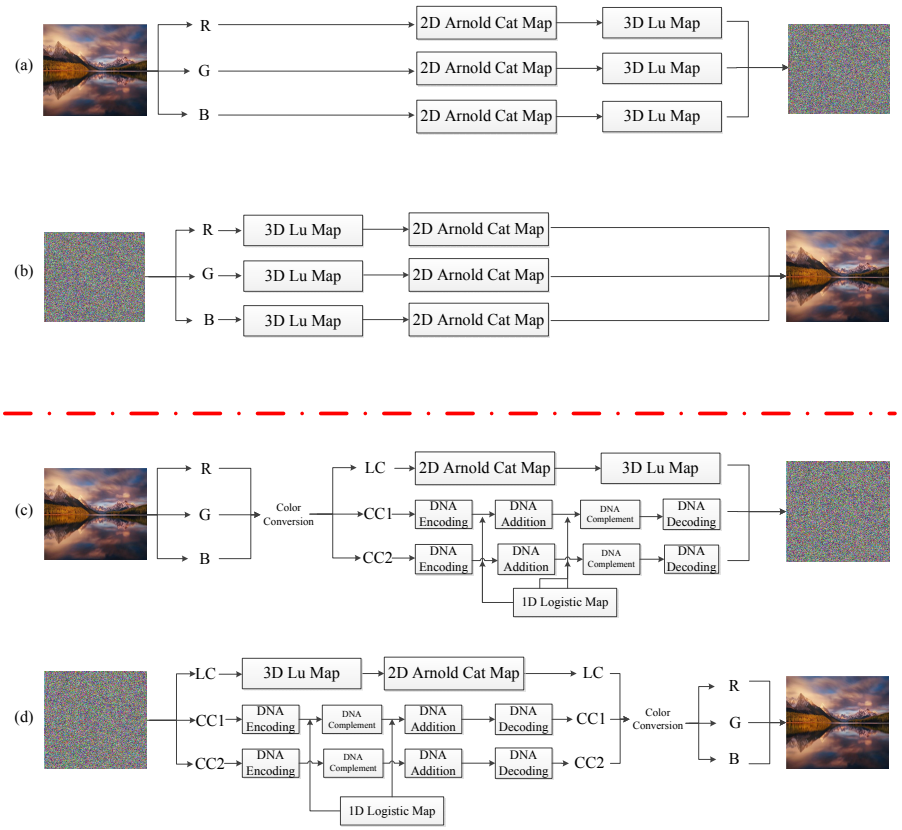

Fig. 2 The RGB encryption is shown in the upper part (a) [20]. Each channel of the RGB color space is fed into 2D Arnold cat map following with 3D Lu map. Our non-RGB encryption is shown in the lower part (b). First we convert the plain image from RGB color space to non-RGB color spaces, i.e. YCbCr, YIQ, HSV and L*a*b*. Then the luminance channels (LC), i.e., Y, Y, V, L*, are shuffled by the 2D Arnold cat map followed by the diffusion via the 3D Lu map. The chroma channels (CC), i.e., CbCr, IQ, HS, and a*b*, are encrypted by DNA encoding and 1D Logistic map. (c) and (d) The decryption method is the inverse version of the corresponding encryption method.

For the encryption using chaotic map and DNA encoding we convert all the non-RGB channels to the range of 0 to 255 (8 bits).

4.2 The Luminance Channel

For the luminance channels, i.e., Y, Y, V, L*, we adopt a 2D and a 3D chaotic maps. The 2D Arnold's cat map is used for confusion of image pixels. The 3D Lu map is used for diffusion of image pixels.

Algorithm 2 Luminance channel diffusion using Lu map

Input:
The confused luminance channel IL^c of the input image with resolution of $(N \times N)$.
Output:
The encrypted luminance channel IL^{cd}.

1: Giving the initial value (x_0, y_0, z_0) of the Lu map, let the system iterate $N \times N$ times, produce three sequence values (x, y, z) each time using Eq. 4. For each pixel P^c of IL^c, do the following 4 steps (2,3,4,5):
2: Take the decimal fraction of three values (x, y, z), and put fourths of three fractions together, constitute a new integer A.
3: The remainder of $A(\mathrm{mod}\, 256)$ is converted binary. The gray value of the image is between 0-255, therefore, the result of $A(\mathrm{mod}\, 256)$ must be in this scope.
4: Convert the value of the pixel P^c of IL^c to binary, and let two binary values exclusive or processing. The OR result is P_b^c.
5: Convert the binary P_b^c to decimal again and produce P^{cd}.
6: **return** the encrypted luminance channel IL^{cd}.

Algorithm 3 Chroma channel encryption using logistic map

Input:
The plain luminance channel CC of the input image with resolution of $(N \times N)$.
Output:
The encrypted chroma channel CC^{enc}.

1: Use the DNA encoding method described in Section 3.5 to convert each pixel of the plain luminance channel CC into DNA codes version CC^{DNA}.
2: Use 1D logistic map to generate a random matrix RM with the same size of the chroma channel. RM is converted to a DNA matrix RM^{DNA} using DNA encoding. Use DNA addition to add it to the encoded result CC^{DNA}. The addition result is CC^{ADD}.
3: Another real value random matrix RM_R with the same size of the chroma channel is generated by 1D logistic map and convert it to a binary matrix RM_R^{bin} with the threshold 0.5. The pixels of RM_R^{bin} is converted into 1 if the values are above 0.5.
4: The DNA addition result CC^{ADD} is then converted to the DNA complement result CC^{COM} when the corresponding value in the second random matrix RM_R^{bin} is 1.
5: Use DNA decoding to convert the CC^{COM} to the 8-bit encrypted result CC^{enc}.
6: **return** the encrypted chroma channel CC^{enc}.

4.2.1 Image Confusion

The different iteration times make the different confusion results. For a gray image with the resolution $256*256$, above 6 iterations can make good shuffling result. However, after 64 iterations the result image is the same as the original plain image because of the periodicity of the Arnold cat map. The different image sizes have different periods. The periodicity of the Arnold's cat map make the confusion become less secure. Thus, in the next step we leverage the 3D Lu map for the diffusion of the confusion result, so as to enhance the safety. As shown in Fig. 3, the confusion results of the luminance channels are nearly random. The confusion algorithm using Arnold cat map is described in Algorithm 1.

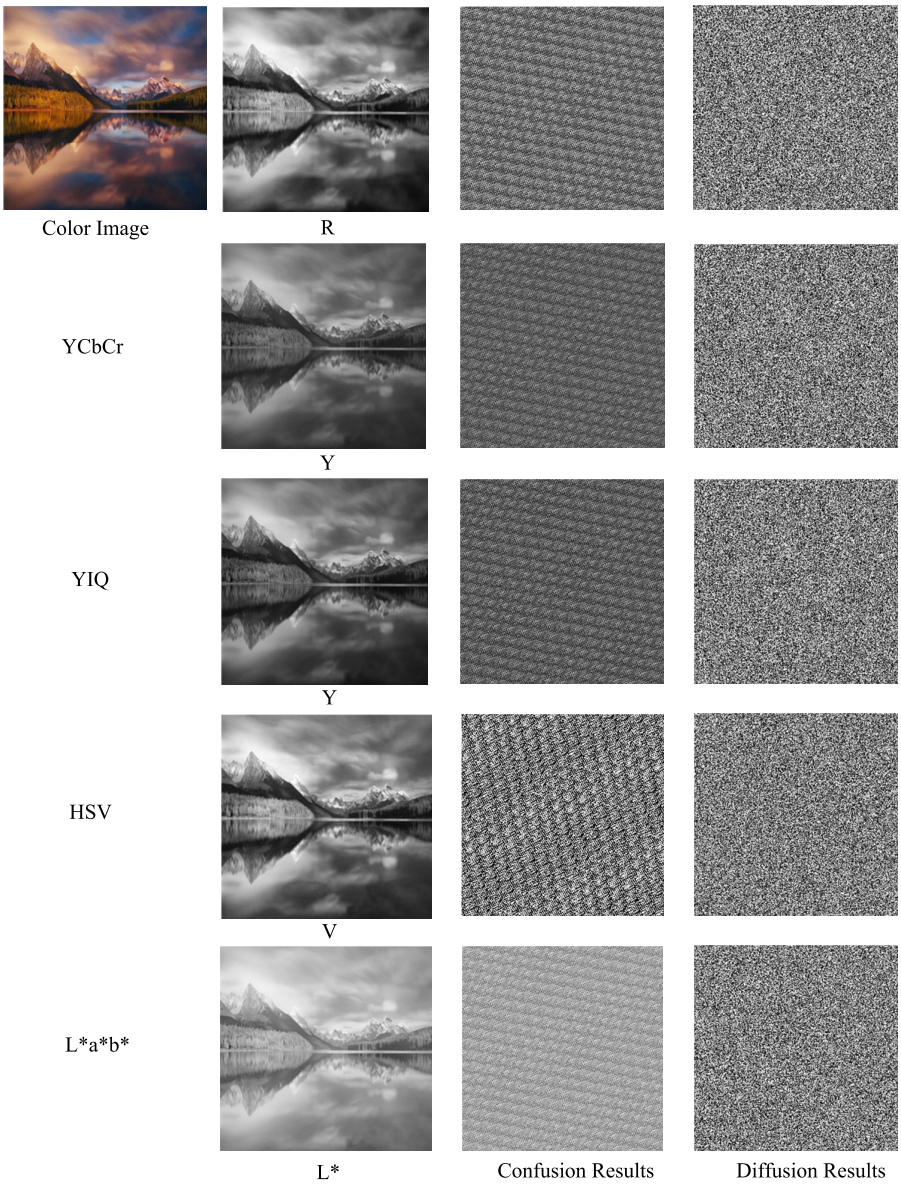

Fig. 3 The confusion results after 20 iterations of the luminance channels. And the diffusion results after the 3D Lu Map. Although the confusion results are slightly different, the final diffusion results are nearly the same using RGB and non-RBG color spaces.

Table 2 The secret keys. We use two logistic maps in the chroma channel encryption. Thus we have 2 pairs of keys of logistic maps: (μ^{a*}, x_0^{a*}) and (μ^{b*}, x_0^{b*}) in Eq. 1. The p and q are the parameters of the Arnold's cat map. (Eq. 2). The a, b, c, x_0, y_0, z_0 are the parameters of the Lu map (Eq. 4).

Chaotic Maps	Keys
1D logistic map	$\mu^{a*} = 3.9, x_0^{a*} = 0.62, \mu^{b*} = 3.99999, x_0^{b*} = 0.26$
2D Arnold' cat map	$p = 1, q = 1$
3D Lu	$a = 36, b = 3, c = 20, x_0 = -6.045, y_0 = 2.668, z_0 = 16.363$

4.2.2 Image Diffusion

We use the 3D Lu map for the diffusion of the confusion result. Giving the initial value x_0, y_0, z_0 of the Lu map, let the system iterate $N \times N$ times, produce three sequence values each time. Then these sequences have the same characteristics of chaos signals namely the characteristics of randomness, ergodic, and the sensibility to initial value, so they can be used on image encryption [19]. The steps that through the Lu map to change each pixel value are described in Algorithm 2 [20]. As shown in Fig. 3, after the diffusion of the result of the confusion, the results are randomized.

4.3 The Chroma Channel

For the chroma channels, i.e., CbCr, IQ, HS, and a*b*, we adopt the method of Jin et al. [7]. The encryption process can be summarised in Algorithm 3.

4.4 Simulation Results

We use plenty of plain images to test our method, as shown in Fig. 4, with the secret key shown in Table 2.

The images with various contents are tested. All the encryption results can be correctly decrypted to the original plain images with the correct secret keys. We can see that the all the simulation results in RGB and non-RGB color spaces are quite satisfactory.

5 Security and Performance Analysis

A well designed image encryption scheme should be robust against different kinds of attacks, such as brute-force attack and statistical attack [2]. In this section, we analyse the security of the non-RGB encryption method in an example image named *couple* with size 256×256, as shown in Fig. 5.

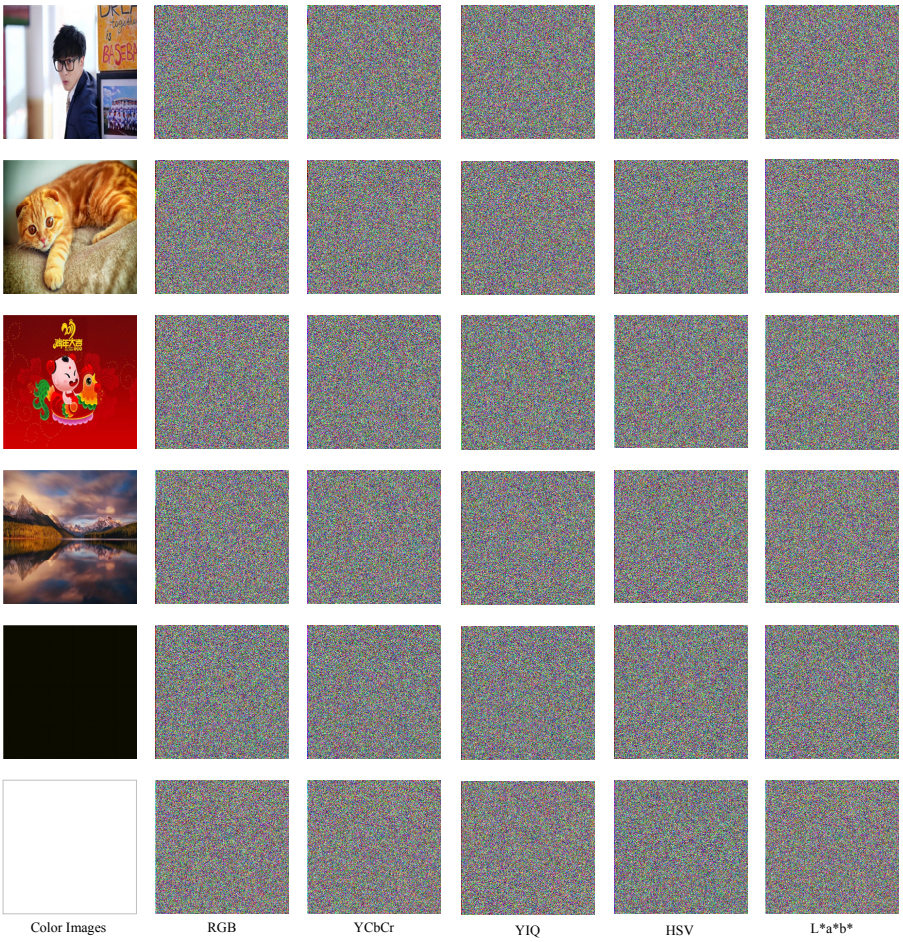

Fig. 4 The simulation results. we test our method on images with various contents including portraits, paintings, animal, landscape, and a pure black image and a pure white image. More results are shown in Section 5.

5.1 Resistance to the brute-force Attack

5.1.1 Key Space

The key space of the image encryption scheme should be large enough to resist the brute-force attack, otherwise it will be broken by exhaustive search to get the secret key in a limited amount of time. In our encryption method, we have the key spaces shown in Table 3.

The precision of 64-bit double data is 10^{-15}, thus the key space is about $(10^{15})^9 = 10^{135} \approx 2^{449}$, which is much lager than the max key space (2^{256}) of practical symmetric encryption of the AES. Our key sapce is large enough to resist brute-force attack.

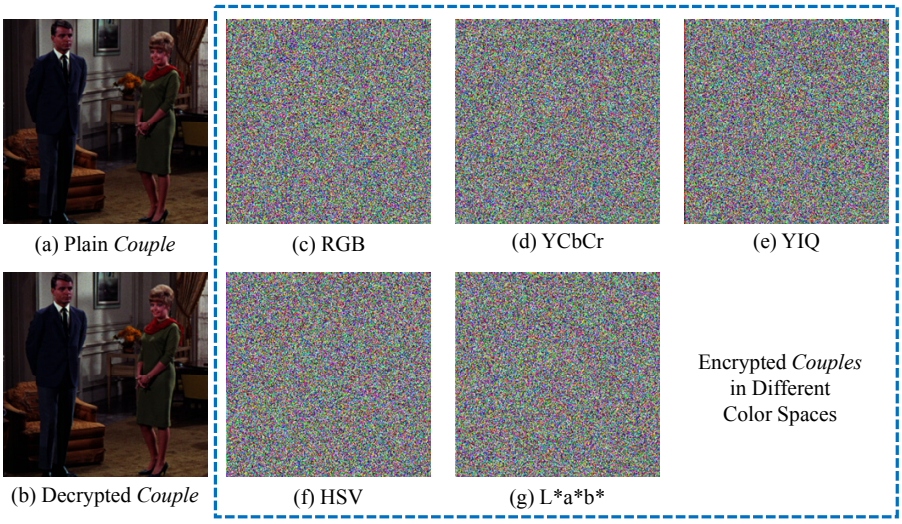

Fig. 5 The example image *couple*. (a) is the original plain image. (c)-(e) are the encryption results in RGB and non-RGB color spaces. (b) is the decryption result. All the method in RGB and non-RGB color spaces can be decrypted correctly. One can recognize nothing in the encryption results.

Table 3 The key spaces.

Chaotic Maps	Key Spaces
1D logistic map	$3.569945672... < \mu^{a*}, \mu^{b*} \leq 4, x_0^{a*}, x_0^{b*} \in [0, 1]$
2D Arnold' cat map	p, q *are positive integers*
3D Lu	$-40 < x_0 < 50, -100 < y_0 < 80, 0 < z_0 < 140$

Table 4 Slightly change the key values.

Secret Keys	Original Values	Novel Values
x_0^{a*}	0.62	0.62000000000001
x_0^{b*}	0.26	0.26000000000001
x_0	-6.045	-6.04500000000001

Using our method in non-RGB color spaces, even the chroma channels are cracked, the luminance channel is not easy attacked. Since the chroma channels contains less recognition information than that of the luminance channel, our encryption method in non-RGB color spaces are secure enough to resist brute-force attack.

5.1.2 Sensitivity of Secret Key

The chaotic systems are extremely sensitive to the system parameter and initial value. A light difference can lead to the decryption failure. To test the secret key sensitivity of the image encryption scheme, we change the secret keys as shown in Table 4.

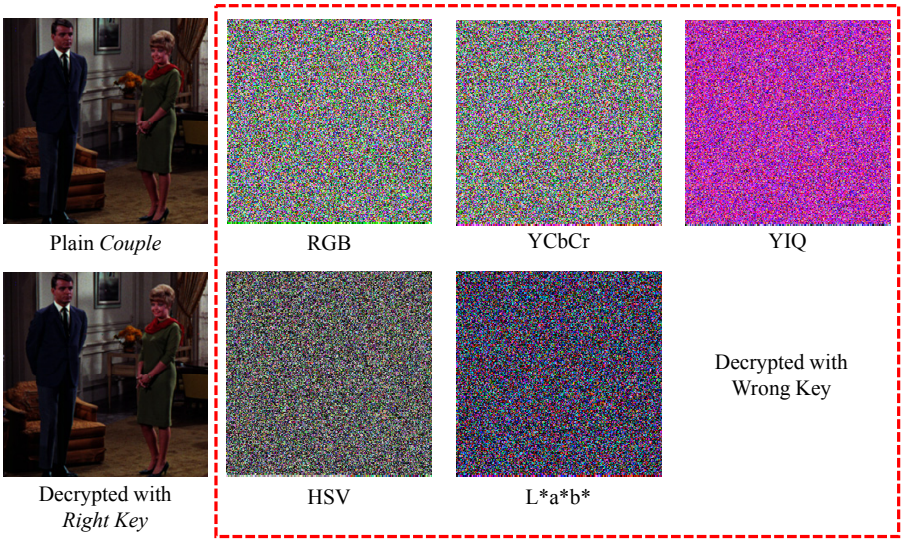

Fig. 6 Decrypted with wrong key. We slightly change the key and get the completely wrong decrypted results using RGB and non-RGB image encryption methods.

We use the changed key to decrypt the *couple* cipher images in Fig. 5, while the other secret keys remain the same. The decryption results are shown in Fig. 6. We can see that the decrypted images are completely different from the original *couple* image. The test results of the other secret key are similar. The experiments show that both the RGB and non-RGB image encryption scheme is quite sensitive to the secret key, which also indicates the strong ability to resist exhaustive attack.

5.2 Resistance to the Statistic Attack

5.2.1 The Histogram Analysis

The histogram is used to show the distribution of pixel values of a gray image. The histogram of cipher image should be flat enough, otherwise some information can be leaked to cause the statistical attack. This makes cipher-only attack possible through analysing the statistic property of the cipher image. Figure 7. shows the histograms of the *couple* image and the corresponding cipher images, respectively. Comparing the histogram pairs we can see that the pixel values of the original *couple* image are concentrated on some values, but the histograms of their cipher images using RGB and non RGB image encryption are very uniform, which makes statistical attacks impossible.

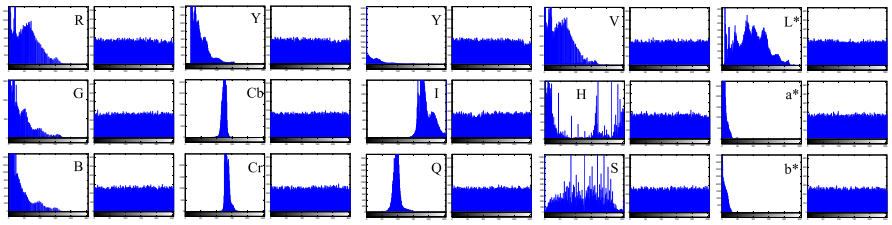

Fig. 7 The histogram of each channel of the RGB and non-RGB color spaces before and after encryption. The histograms of the non-RGB color spaces are nearly as flat as those of the RGB color space.

Table 5 The entropy of each channel after encryption using RGB and non-RGB methods.

R	G	B
7.9963	7.9972	7.9973
Y	Cb	Cr
7.9961	7.9974	7.9971
Y	I	Q
7.9951	7.9970	7.9976
V	H	S
7.9959	7.9977	7.9971
L*	a*	b*
7.9974	7.9972	7.9973

5.2.2 The Information Entropy

The information entropy [2] is used to express randomness and can measure the distribution of gray values in the image. The more uniform the distribution of pixel gray values, the greater the information entropy is. It is defined as follows:

$$\mathrm{H}(m) = -\sum_{n=0}^{N} \mathrm{P}(m_i) \log_2(m_i) \tag{6}$$

where m_i is the i-th gray value for an N level gray image, $N = 255$. $P(m_i)$ is the probability of m_i in the image and $\sum_{i=0}^{L} P(m_i) = 1$. The information entropy of an ideal random image is 8, which shows that the information is completely random. The information entropy of the cipher image should be close to 8 after encryption. The closer it is to 8, the smaller possibility for the scheme leaks information.

The information entropy of *couple* cipher image using our methods in RGB and non-RGB color spaces are summarized in Table 5. The results show that the non-RGB methods perform as well as the RGB method [20] (the entropy is very close to 8).

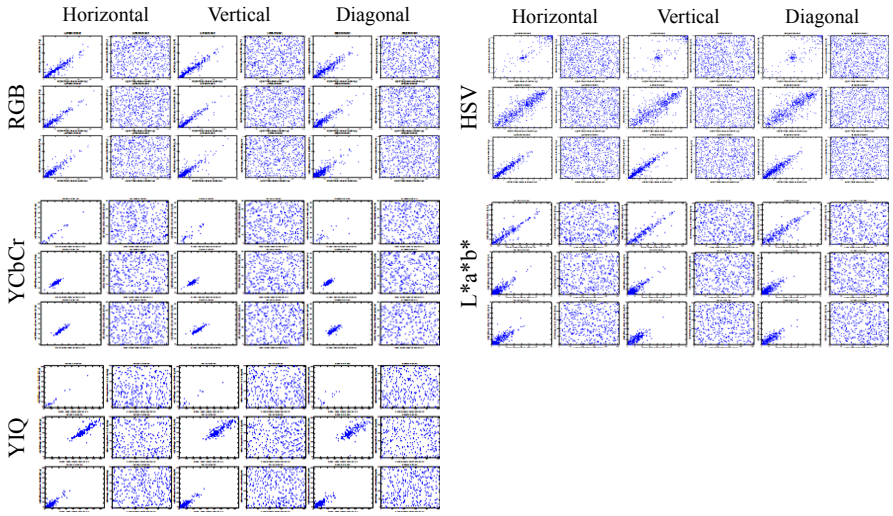

Fig. 8 The correlation of each channel of RGB and non-RGB color spaces before and after encryption in 3 directions (horizontal, vertical and diagonal).

5.3 Resistance to the Correlation Attack

Correlation indicates the linear relationship between two random variables. In image processing, it is usually employed to investigate the relationship between two adjacent pixels. Usually, the correlation of between adjacent pixels in the plain image is very high. A good encryption scheme should reduce the correlation between adjacent pixels, i.e., the less correlation of two adjacent pixels have, the safer the cipher image is. In order to test the correlation of two adjacent pixels, we test 3 directions (horizontal, vertical and diagonal) of adjacent pixels from the original *couple* image and its corresponding cipher images, as shown in Fig. 8.

The correlation coefficients are shown in the Table. 6. It shows that there is strong correlation between adjacent pixels of each direction in original *couple* image since the correlation coefficients are all close to 1 while the correlation coefficients of the adjacent pixels in the cipher image are very small, which are close to 0. So the image encryption scheme can greatly reduce the correlation of the cipher image in each channel of the non-RGB color space. The results show that the non-RGB methods perform as well as the RGB method [20].

5.4 Evaluation on a Large Scale Dataset

Only one example image can not reveal all the truth. Thus, we use a large scale image dataset to evaluate our methods. The Caltech101 dataset [23] contains images of objects belonging to 101 categories, with about 40 to 800 images per category. Most categories have about 50 images.

Table 6 The correlation coefficients before and after encryption of the example image *couple*.

	Plain *Couple*			Cipher *Couple*		
	R	G	B	R	G	B
Horizontal	0.9556	0.9499	0.9397	-0.0234	-0.0080	-0.0138
Vertical	0.9530	0.9399	0.9139	-0.0057	-0.0278	-0.0220
Diagonal	0.9243	0.8966	0.8876	-0.0276	-0.0251	-0.0068
	Y	Cb	Cr	Y	Cb	Cr
Horizontal	0.9537	0.8787	0.9272	-0.0252	-0.0045	-0.0205
Vertical	0.9352	0.8701	0.9093	0.0082	0.0070	0.0234
Diagonal	0.9015	0.8501	0.8789	0.0305	0.0133	-0.0156
	Y	I	Q	Y	I	Q
Horizontal	0.9533	0.9364	0.7826	-0.0214	-0.0246	-0.0073
Vertical	0.9265	0.9109	0.7477	0.0034	0.0035	0.0044
Diagonal	0.9018	0.8859	0.7104	-0.0094	0.0322	-0.0380
	H	S	V	H	S	V
Horizontal	0.5276	0.8691	0.9593	-0.0100	0.0049	-0.0153
Vertical	0.5050	0.8124	0.9461	-0.0071	-0.0154	0.0060
Diagonal	0.4748	0.7804	0.9170	0.0419	-0.0300	-0.0255
	L*	a*	b*	L*	a*	b*
Horizontal	0.9611	0.8781	0.9074	-0.0093	0.0243	0.0042
Vertical	0.9352	0.8287	0.8911	-0.0286	0.0124	-0.0078
Diagonal	0.9071	0.7869	0.8713	0.0031	0.0358	-0.0055

Table 7 The average entropy of 101 cipher images from Caltech101 dataset.

R	G	B
7.9965	7.9971	7.9971
Y	Cb	Cr
7.9965	7.9971	7.9971
Y	I	Q
7.9965	7.9970	7.9972
V	H	S
7.9965	7.9971	7.9971
L*	a*	b*
7.9963	7.9971	7.9971

5.4.1 Encryption Results

We randomly pickup one image per category for our evaluation, which forms a subset of 101 images. We encrypt all the 101 images using the RGB and non-RGB methods. As shown in Fig. 9, the encryption results of non-RGB methods perform as well as the RGB method in such a large scale image dataset.

5.4.2 The Entropy

In addition, we calculate the average entropy of each channel of the cipher images in Fig. 9 of RGB and non-RGB channels over 101 images. The results are shown in Table 7. All the average entropy is near 8, which shows that our non-RGB encryption methods perform robustly over various types of images.

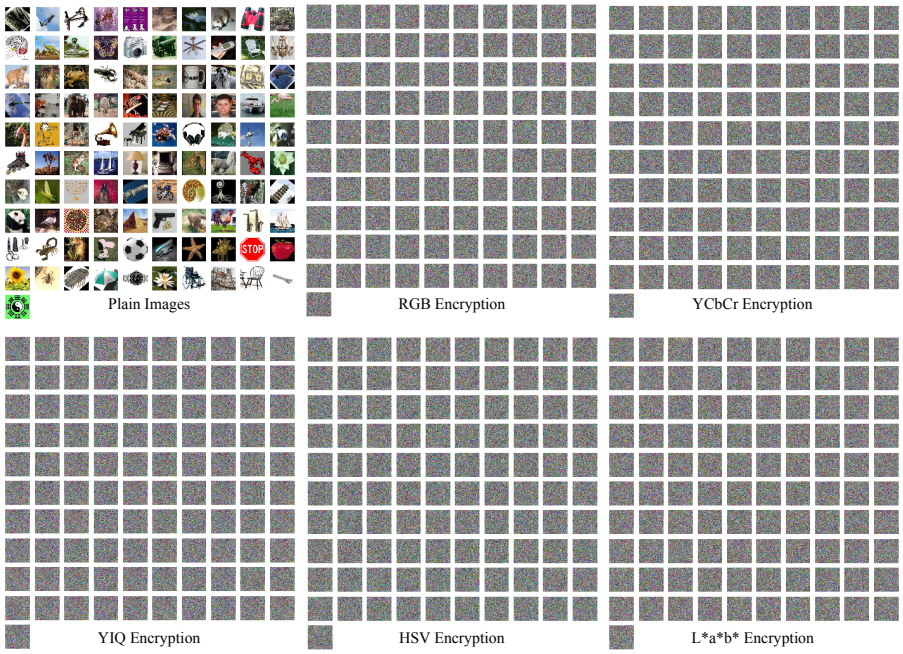

Fig. 9 The encryption results of 101 images from Caltech101 dataset.

Table 8 The entropy and the image size.

	128*128	256*256	384*384	512*512	640*640	768*768	896*896
R	7.9887	7.9976	7.9986	7.9993	7.9995	7.9996	7.9997
G	7.9888	7.9969	7.9987	7.9993	7.9996	7.9997	7.9998
B	7.9897	7.9967	7.9986	7.9993	7.9995	7.9997	7.9998
Y	7.9861	7.9971	7.9985	7.9992	7.9994	7.9995	7.9995
Cb	7.9871	7.9973	7.9987	7.9993	7.9996	7.9997	7.9998
Cr	7.9886	7.9969	7.9987	7.9992	7.9996	7.9997	7.9998
Y	7.9894	7.9976	7.9988	7.9992	7.9996	7.9997	7.9997
I	7.9886	7.9968	7.9987	7.9992	7.9996	7.9997	7.9998
Q	7.9901	7.9969	7.9987	7.9996	7.9996	7.9997	7.9998
V	7.9902	7.9975	7.9986	7.9993	7.9995	7.9997	7.9997
H	7.9877	7.9973	7.9986	7.9992	7.9996	7.9997	7.9998
S	7.9877	7.9973	7.9986	7.9992	7.9996	7.9997	7.9998
L*	7.9884	7.9965	7.9983	7.9989	7.9992	7.9993	7.9995
a*	7.9888	7.9969	7.9987	7.9993	7.9996	7.9997	7.9998
b*	7.9897	7.9967	7.9986	7.9993	7.9995	7.9997	7.9998

We evaluate the relation between the image size and the entropy of the cipher images. We randomly pickup 7 images with sizes of 128*128 256*256 384*384 512*512 640*640 768*768 896*896 and calculate the entropy of the cipher images using the RGB and non-RGB encryption methods. As shown in Table 8, the image sizes influence the entropy. The larger the image size is, the

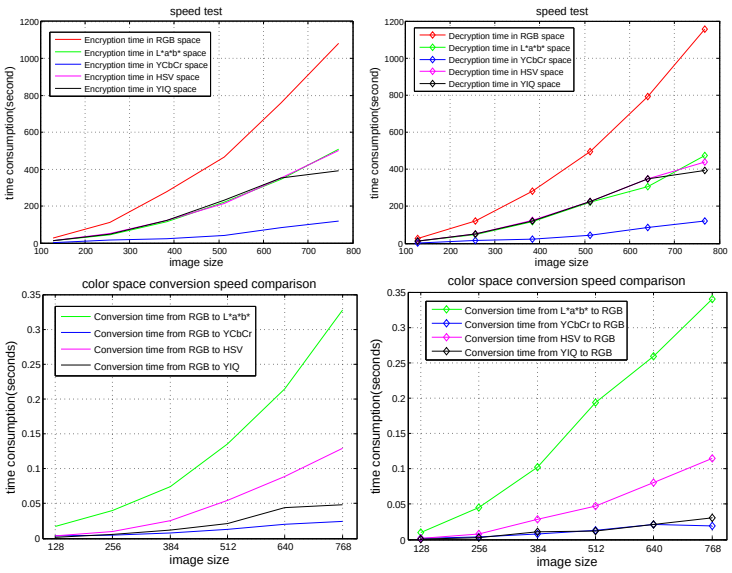

Fig. 10 The comparison of the speed of the encryption and decryption progress using the non-RGB method and the RGB method [20] in several image resolutions: 128*128, 256*256, 384*384, 512*512, 640*640, 768*768.

larger the entropy of cipher image is. In all the image sizes in our experiments, the non-RGB methods perform as well as the RGB method.

5.4.3 The Speed of the Encryption and Decryption

The image encryption scheme is implemented by Matlab on personal computer with Intel(R) Core(TM0 i5-2522S CPU @2.70G Core Processor 2.19GHz and 8.00G RAM.. The encryption and decryption consumption time is recorded for the images of different sizes. The larger size of the image, the more time it needs for encryption and decryption. When our implementation in Matlab 2014a transplanted to other implement environment, like C/C++, the speed can be much faster, which can satisfy practical demand.

As show in Fig. 10, we test the speed of the encryption and decryption using the non-RGB methods and the RGB method [20] with various image sizes. The comparison show that although the non-RGB methods contain the color conversion at the begining and the end, they are all faster than the RGB method. The conversion time cost between RGB and YCbCr is less than others. Thus, the encryption and decryption time cost is the lowest using the YCbCr method.

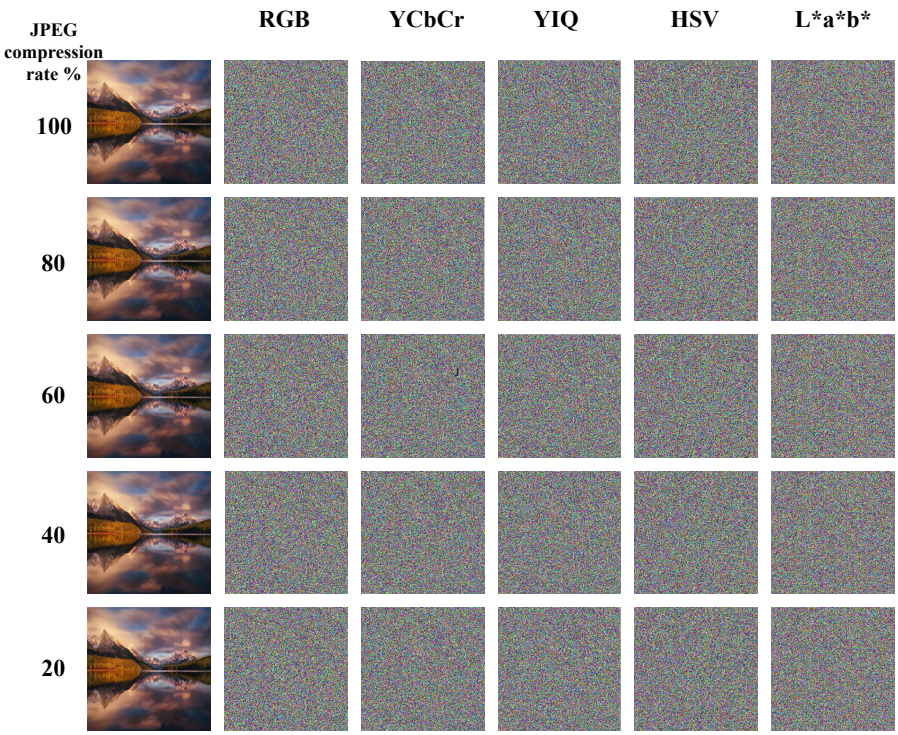

Fig. 11 We test our methods on the same image resolution with various JPEG compression rates from 20% to 100%.

5.5 Evaluation with Various JPEG Compression Rates

In general, the higher the JPEG compression rate is, the lesser information the chroma channels have. However, our encryption methods are conducted after the depression of the JPEG images. We have not taken the compression of the chroma channels into consideration. Thus our methods can be applied to various JPEG compression rates.

5.5.1 The Simulation Results and the Entropy

We evaluate our methods with various JPEG compression rates. The simulation results are shown in Fig. 11. Our methods can be applied to various JPEG compression rates. We also evaluate the information entropy with various JPEG compression rates. The results are shown in Table 9. The entropy with various rates are nearly the same.

5.5.2 The Speed

Our encryption methods are conducted after the depression of the JPEG images. Thus, the speed of the encryption and decryption are correlated with the

Table 9 The entropy of each channel after encryption using RGB and non-RGB methods with various JPEG compression rates.

Comp. Rate	20%	40%	60%	80%	100%
R	7.9973	7.9969	7.9970	7.9974	7.9968
G	7.9969	7.9972	7.9973	7.9974	7.9972
B	7.9969	7.9971	7.9969	7.9970	7.9972
Y	7.9974	7.9973	7.9972	7.9972	7.9970
Cb	7.9972	7.9969	7.9970	7.9969	7.9967
Cr	7.9969	7.9970	7.9968	7.9971	7.9971
Y	7.9965	7.9967	7.9966	7.9965	7.9963
I	7.9971	7.9974	7.9975	7.9975	7.9976
Q	7.9974	7.9974	7.9972	7.9972	7.9973
V	7.9964	7.9966	7.9967	7.9971	7.9963
H	7.9968	7.9971	7.9972	7.9972	7.9975
S	7.9974	7.9974	7.9972	7.9970	7.9971
L*	7.9972	7.9971	7.9972	7.9971	7.9973
a*	7.9970	7.9972	7.9970	7.9971	7.9971
b*	7.9974	7.9975	7.9976	7.9969	7.9972

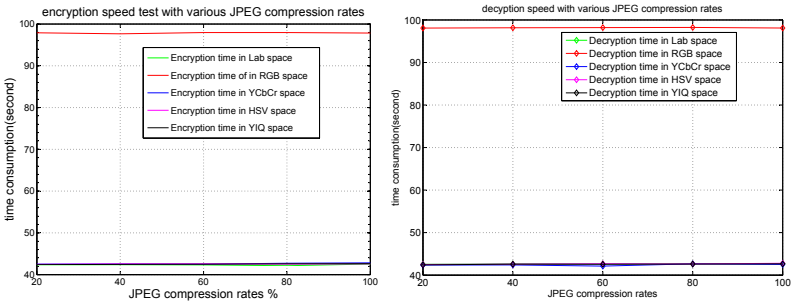

Fig. 12 The encryption and decryption speeds with various JPEG compression rates.

image resolution, as shown in Fig. 10. We test our methods using 10 images with the same resolution and various JPEG compression speed. The average speeds are shown in Fig. 12. Our Non-RGB methods are still faster than the RGB method.

6 Conclusion and Discussion

In this paper, we make a systematic comparative study of non-RGB image encryption. We evaluate four typical non-RGB color spaces, i.e., YCbCr, YIQ, HSV and L*a*b*, which all contain one informative luminance channel and two less informative chroma channels. The high level chaotic maps are used in the luminance channel for secure encryption result. The low level chaotic map is used in the chroma channels for efficient operation. We save the encryption time in less informative chroma channels, while retain high level encryption in the more informative luminance channel for security.

The non-RGB encryption methods are compared to the RGB method, which use high level chaotic maps in all the 3 RGB channels. We analyse the encryption results of RGB and non-RGB methods. An example image are used for the security analysis on several attacks, including the brute-force attack and the statistic attack. In addition, we use a large scale image dataset to evaluate the encryption methods. The experimental results reveal that the non-RGB methods perform nearly as well as the RGB method in the security aspect, while need less time for encryption and decryption. The YCbCr method is the fastest method in most cases.

In the future work, we will take the compression into consideration so as to improve the encryption efficiency.

References

1. Mahdi, A., Alzubaiti, N. Selective Image Encryption with 3D Chaotic Map. European Academic Research. Vol.2, No.4, pp.4757-4773 (2014).
2. Zhen, P., Zhao, G., Min, LQ., Jin, X. Chaos-Based Image Encryption Scheme Combining DNA Coding and Entropy. Multimedia Tools and Applications (MTA), Published Online: 10 April (2015)
3. Jin, X., Liu, Y., Li, X.D., Zhao, G. Chen, Y.Y., Guo, K. Privacy Preserving Face Identification through Sparse Representation. To Appear in the Proceedings of the 10th Chinese Conference on Biometric Recognition (CCBR), (2015)
4. Guellier, A., Bidan, C., Prigent., Nicolas. Homomorphic Cryptography-Based Privacy-Preserving Network Communications. Proceedings of 5th International Conference on Applications and Techniques in Information Security (ATIS), pp.159-170, Melbourne, VIC, Australia, November 26-28, (2014).
5. Jin, X., Chen, Y., Ge S., et al. Color Image Encryption in CIE L*a*b* Space. in the proceeding of the 6th International Conference on Applications and Techniques for Information Security (ATIS), Beijing, China, 4-6 November, pp.74-84, 2015
6. Jin, X., Yin, S., Li, X., Zhao, G., et al. Color Image Encryption in YCbCr Space. in the proceeding of the 8th International Conference on Wireless Communications & Signal Processing (WCSP), Yangzhou, China, October 13-15, pp. 1-5, 2016
7. Jin, X., Tian, Y., Song, C., et al. An Invertible and Anti-Chosen Plaintext Attack Image Encryption Method based on DNA Encoding and Chaotic Mapping. Chinese Automation Congress (CAC), 27-29, November, Wuhan, pp.1159-1164, 2015
8. Jin, X., Wu Z., Song C., et al. 3D Point Cloud Encryption through Chaotic Mapping. The Pacific-Rim Conference on Multimedia (PCM), Xi'an China, 15-16 September, pp.119-129, 2016
9. Jin, X., Guo, K., Song C., et al. Private Video Foreground Extraction through Chaotic Mapping based Encryption in the Cloud. The 22nd International Conference On Multimedia Modelling (MMM), Miami, USA, 4-6 January, pp.562-573, 2016
10. Zhang Y., He L., Fu B. Research on DNA cryptography. Applied cryptography and network security:357 (2012)
11. Zhang Q., Guo L., Wei X. Image encryption using DNA addition combining with chaotic maps. Math Comput Model 52(11):202835 (2010)
12. Xie, X., Zaitsev, Y., Velsquez-Garca, L. F., Teller, S. J., and Livermore, C. (2014). Scalable, MEMS-enabled, vibrational tactile actuators for high resolution tactile displays. Journal of Micromechanics and Microengineering, 24(12), 125014.
13. Xie, X., and Carol L., A pivot-hinged, multilayer SU-8 micro motion amplifier assembled by a self-aligned approach. Micro Electro Mechanical Systems (MEMS), 2016 IEEE 29th International Conference on, 2016.
14. YCbCr color space, `https://en.wikipedia.org/wiki/YCbCr`
15. YIQ color space, `https://en.wikipedia.org/wiki/YIQ`
16. HSL and HSV color space, `https://en.wikipedia.org/wiki/HSL_and_HSV`

17. Lab color space, https://en.wikipedia.org/wiki/Lab_color_space
18. Arnold's cat map, https://en.wikipedia.org/wiki/Arnold\%27s_cat_map#cite_note-Arnold-1
19. Ling B., Liu LC. Image encryption algorithm based on chaotic map and S-DES. International Conference on Advanced Computer Control (ICACC), Vol.5, pp.41-44 (2010)
20. Wang YZ., Ren GY., Jiang JL., Zhang J., Sun LJ. Image Encryption Method Based on Chaotic Map. 2nd IEEE Conference on Industrial Electronics and Applications (ICIEA), pp.2558-2560 (2007)
21. Zhang Q., Guo L., Wei XP. Image encryption using DNA addition combing with chaotic maps. Mathematical and Computer Modelling Vol.52, No.11-12, pp.2028-2035 (2010)
22. Hermassi H., Belazi A., Rhouma R., Belghith SM. Security analysis of an image encryption algorithm based on a DNA addition combining with chaotic maps. Multimedia Tools and Applications (MTA), Vol.72, No.3, pp. 2211-2224 (2014)
23. L. Fei-Fei, R. Fergus and P. Perona. Learning generative visual models from few training examples: an incremental Bayesian approach tested on 101 object categories. IEEE. CVPR 2004, Workshop on Generative-Model Based Vision. 2004