Color Image Encryption in CIE L*a*b* Space

Xin Jin[1,*], Yingya Chen[1], Shiming Ge[2], Kejun Zhang[1], Xiaodong Li[1,*], Yuzhen Li[1,3], Yan Liu[1,3], Kui Guo[1], Yulu Tian[1], Geng Zhao[1], Xiaokun Zhang[1], and Ziyi Wang[1]

[1]Beijing Electronic Science and Technology Institute, Beijing 100070, China, GOCPCCC Key Laboratory of Information Security, Beijing 100070, China
[2]Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China [3]Xidian University, Xi'an, 710071, China
{jinxin,lxd}@besti.edu.cn

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. Currently, little attention has been paid to non-RGB color spaces such as HSV, YUV and L*a*b* color spaces in the color image encryption community. In this paper we use *high level* encryption schemes in more informative channels and *low level* encryption schemes in less informative channels. This paper is the first time to encrypt color image in CIE L*a*b* color space. First we convert RGB to L*a*b* color space. The 2D Arnold's cat map followed by the 3D Lu chaotic map are conducted in the L* channel. The less complicated DNA coding and 1D logistic map based encryption scheme is leveraged in the a* and b* channels, which contain less information than that in the L* channel. The experimental results reveal that our method achieves similar results with the method that conducts the same scheme in each channel of the RGB color space, while consuming less time. In addition, our method can resistant several attacks such as brute-force attack, statistic attack, correlation attack.

Keywords: Color Image Encryption, L*a*b*, Chaotic Map, Selective Encryption

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

* Corresponding Authors: {jinxin,lxd}@besti.edu.cn

government or military images are leaked, the state security are 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 channels [1] [3] [4].

Current image encryption technologies mainly concentrate on gray image encryption [10] [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 HSV, YUV or 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 chrominance 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 or two channel(s) contain(s) more visual recognition information than those in (the) other channel(s). This property enables us to use *high level* encryption schemes in more informative channels and *low level* encryption schemes in less informative channels.

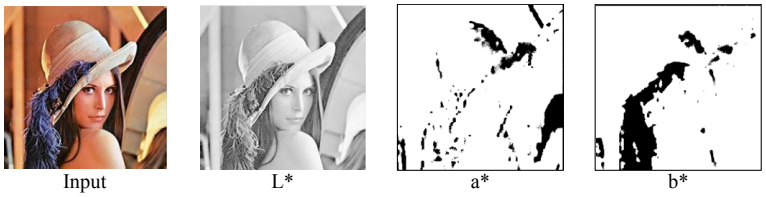

Fig. 1. Converting RGB to L*a*b*. The L*a*b* color space is a color-opponent space with dimension L* for lightness and a* and b* for the color-opponent dimensions, based on non-linearly compressed (e.g. CIE XYZ color space) coordinates. The L* channel is more independent to color component and more close to human perception on lightness than RGB color space [6]. One can easily recognize Lena from the L* channel, but can almost find nothing from the a* and b* channel.

In this paper, it is the first time for the color image encryption to be operated in CIE L*a*b* color space. First, we convert RGB to L*a*b* color space. The 2D Arnold's cat map followed by the 3D Lu chaotic map are conducted in the L* channel. The less complicated DNA coding and 1D logistic map based encryption scheme is leveraged in the a* and b* channels, which contain less information than that in the L* channel. Our method in this study has been tested on some images and showed good results. The experimental results reveal our method achieves similar results with the method that conducts the same scheme in each channel of the RGB color space, while consuming less time. In addition, our method can resistant several attacks such as brute-force attack, statistic attack and correlation attack.

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. Some cryptosystems, which are based on a low-dimensional chaotic map, have obvious drawbacks, such as short period and small key space [9] [2].

Zhang et al. [10] propose a gray image encryption method by using DNA encoding and 1D logistic map. However, in 2014, Hermassi et al. [11] points out that the method of [10] is not reversible, namely, it can only encrypt the plain image, and had no method on the cipher image in the case of known the secret key. We add a random matrix to the DNA addition and make the encryption reversible.

The most similar work to ours is Mahdi et al. [1]. They propose a color image encryption method in the YCbCr color space. In the Y channel, the Arnold cat map is conducted followed with a 3D logistic map. The Cb and Cr channels are directly send to a 3D logistic map system. In this paper we propose a color image encryption method in L*a*b* color space. 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 nonlinear relations for L*, a*, and b* are intended to mimic the nonlinear response of the eye. Furthermore, uniform changes of components in the L*a*b* color space aim to correspond to uniform changes in perceived color, so the relative perceptual differences between any two colors in L*a*b* can be approximated by treating each color as a point in a three-dimensional space (with three components: L*, a*, b*) and taking the Euclidean distance between them [6].

3 Preliminaries

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 1D Logistic map

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

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

3.2 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 [7]. Arnolds 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].

$$\begin{bmatrix} X' \\ Y' \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & p*q+1 \end{bmatrix} * \begin{bmatrix} X \\ Y \end{bmatrix} \bmod 256 \tag{2}$$

$$\begin{bmatrix} X \\ Y \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & p*q+1 \end{bmatrix}^{-1} * \begin{bmatrix} X' \\ Y' \end{bmatrix} \bmod 256 \tag{3}$$

, where p and q represent the positive secret keys. X, Y is the original position of the image pixel before shuffling. X', Y' is the new position of the image pixel after shuffling.

3.3 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. 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 [8].

4 Color Image Encryption in L*a*b*

In this section, we describe the proposed color image encryption method in CIE L*a*b* color space. As shown in Fig. 2, first we convert we convert the plan image from RGB color space to L*a*b* space. Then the informative L* channel encrypted by 2 high dimensional chaotic map. The less informative a* and b* channels are encrypted by a low dimensional chaotic map for efficient computation.

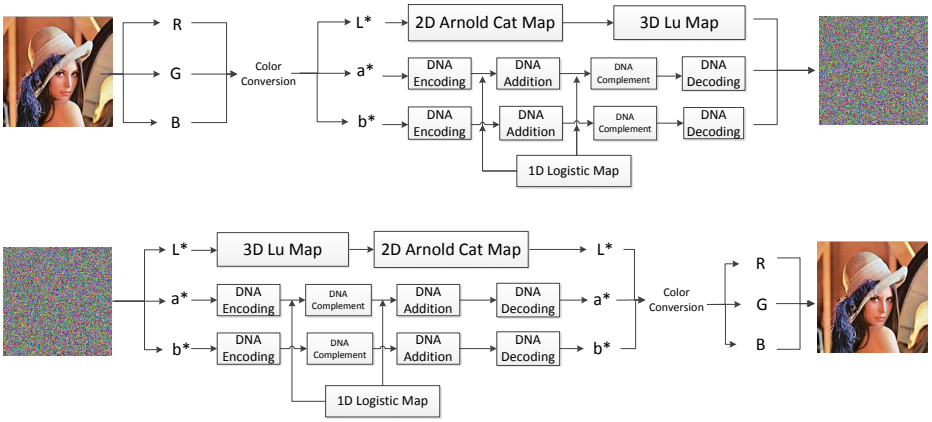

Fig. 2. Our proposed method for color image encryption in L*a*b* space. First we convert the plan image from RGB color space to L*a*b* space. Then the L* channel is shuffled by the 2D Arnold cat map followed by the diffusion via the 3D Lu map. The a* and b* channel are encrypted by DNA encoding and 1D Logistic map. The decryption method is the inverse version of the encryption method.

4.1 Color Conversion

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. For the encryption using chaotic map and DNA encoding we convert all the 3 channels of L*, a* and b* to the range of 0 to 255 (8 bits).

4.2 The L* Channel

In the L* channel we adopt a 2D and a 3D chaotic maps. The 2D Arnold cat map is used for confusion of image pixels. The 3D Lu map is used for diffusion of image pixels.

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 plan image because of the periodicity of the Arnold cat map. The different image sizes have different periods. The periodicity of the Arnold cat map make the confusion become less safety. Thus, in the next step we leverage the 3D Lu map for the diffusion of the confusion result, so as to enhance the safety.

Image Diffusion We use the 3D Lu map for the diffusion of the confusion result. The step that through the Lu map to change each pixel value are as follows [9]:

- 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.
- Take the decimal fraction of three values, and put fourths of three fractions together, constitute a new integer A.
- 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.
- Convert the value which is encrypted by the cat map to binary, and let two binary values exclusive or processing, total $N \times N$ times.
- The result of the above step is converted decimal again. It returns the 2D image, and completes the second encryption.

4.3 The a* and b* Channel

The a* or b* channel is firstly encoded by DNA encoding [10]. Then, we use 1D logistic map to generate a random matrix with the same size of a* or b* and use DNA addition to add it to the encoded result. After that, another random matrix with the same size of a* or b* is generated by 1D logistic map and convert it to a binary matrix with the threshold 0.5. The DNA addition result is then converted to the DNA complement result when the corresponding value in the second random matrix is 1. The last step is DNA decoding to obtain the 8-bit encryption result.

5 Simulation Results

We use plenty of plan images to test our method, as shown in Fig. 3, with the secret key

$$\begin{cases} \text{1D logistic: } \mu^{a*} = 3.9, x_0^{a*} = 0.62, \mu^{b*} = 3.99999, x_0^{b*} = 0.26 \\ \text{2D Arnold: } N_{iteration} = 20, p = 1, q = 1 \\ \text{3D Lu:} a = 36, b = 3, c = 20, x_0 = -6.045, y_0 = 2.668, z_0 = 16.363 \end{cases} \tag{5}$$

The images with various contents are tested. All the encryption results can be correctly decrypted to the original plan images with the correct secret keys. We can see that the simulation results are quite satisfactory.

6 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 proposed encryption method in an example image named *Baby & Car* with size 851×851. We also compare our method (referred as L*a*b* method in the following) with the method of [1] (referred as YUV

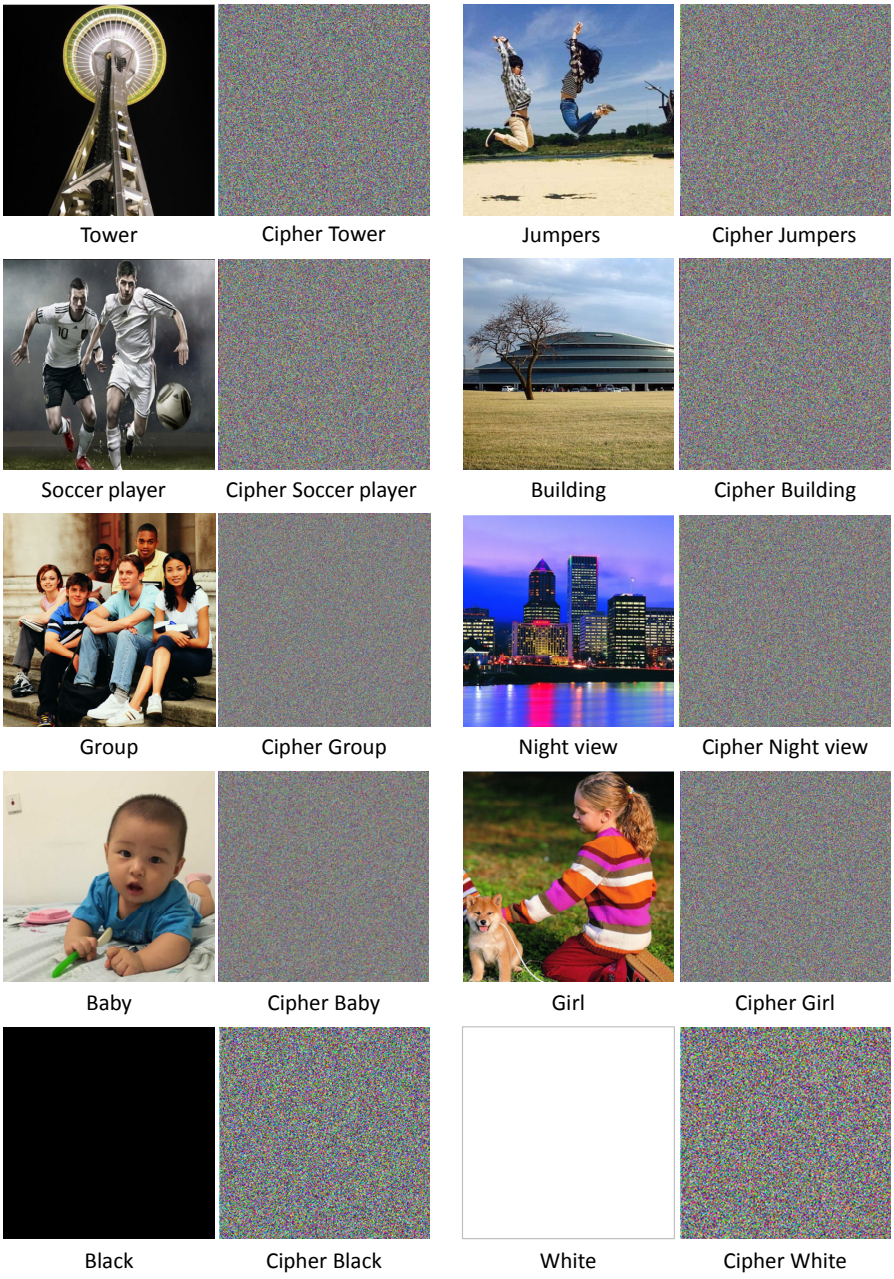

Fig. 3. The simulation results. we test our method on images with various contents including portraits, landscape, architecture, and a pure black image and a pure white image.

method in the following) and an encryption method in the RGB color space (referred as RGB method in the following): in each channel of R, G and B, the same encryption scheme to the one used in the L* channel of our proposed method is adopted [9], , as shown in Fig. 4.

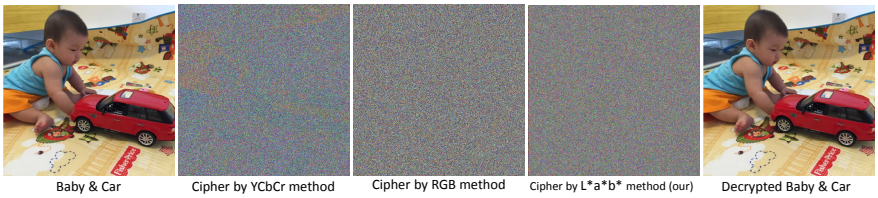

Fig. 4. The example image *Baby & Car*. From the left to the right: the Original plan image, the cipher image using the YCbCr, the RGB and the L*a*b*(our) method, and the decrypted image.

6.1 Resistance to the brute-force Attack

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 space as follow:

$$\begin{cases} \text{1D logistic: } 3.569945672... < \mu \leq 4, x_0 \in [0,1] \\ \text{2D Arnold: } N_{iteration} > 15, p, q \textit{ are positive integers} \\ \text{3D Lu:} a = 36, b = 3, c = 20, -40 < x_0 < 50, -100 < y_0 < 80, 0 < z_0 < 140 \end{cases} \tag{6}$$

The precision of 64-bit double data is 10^{-15}, thus the key space is about $(10^{15})^8 = 10^{120} \approx 2^{399}$, 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.

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 key as follow:

$$\begin{cases} x_0 \text{ from } -6.045 \text{ to } & -6.04500000000001 \\ x_0^{a*} \text{ from } 0.62 \text{ to } & 0.62000000000001 \\ x_0^{b*} \text{ from } 0.26 \text{ to } & 0.26000000000001 \end{cases} \tag{7}$$

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

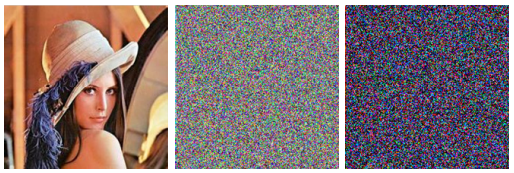

Fig. 5. Decrypted with wrong key. We slightly change the key and get the wrong decrypted result.

6.2 Resistance to the Statistic Attack

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 6. shows the histograms of the *Baby & Car* image and its corresponding cipher image, respectively. Comparing the two histograms we can see that the pixel values of the original *Baby & Car* image are concentrated on some values, but the histograms of its cipher image are very uniform, which makes statistical attacks impossible.

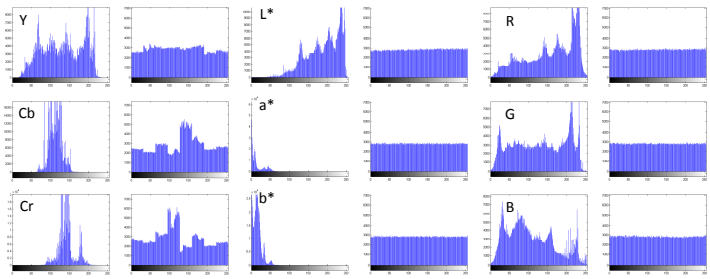

Fig. 6. The histogram of each channel of YCbCr, L*a*b* and RGB before and after encryption.

We also test the YCbCr method [1] and the RGB method [9] and show the histogram in each channel of their method in Fig 6. The histograms of our method are nearly as flat as those of the RGB method, which are both better than those of the YCbCr method.

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:

$$\mathrm{H}(m) = -\sum_{l=0}^{L} \mathrm{P}(m_i) \log_2(m_i) \tag{8}$$

where m_i is the i-th gray value for an L level gray image, $L = 255$. $P(m_i)$ 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 *Baby & Car* cipher image using our method, the RGB [9], and the YCbCr method [1] can be summarized as follow:

$$\begin{cases} \mathrm{H}(L*) = 7.9994, \mathrm{H}(a*) = 7.9998, \mathrm{H}(b*) = 7.9997 \\ \mathrm{H}(R) = 7.9997, \mathrm{H}(G) = 7.9998, \mathrm{H}(B) = 7.9996 \\ \mathrm{H}(Y) = 7.9940, \mathrm{H}(Cb) = 7.9350, \mathrm{H}(Cr) = 7.9196 \end{cases} \tag{9}$$

The results show that our method performs as well as the RGB method [9] (the entropy is very close to 8), and both outperform the YCbCr method [1].

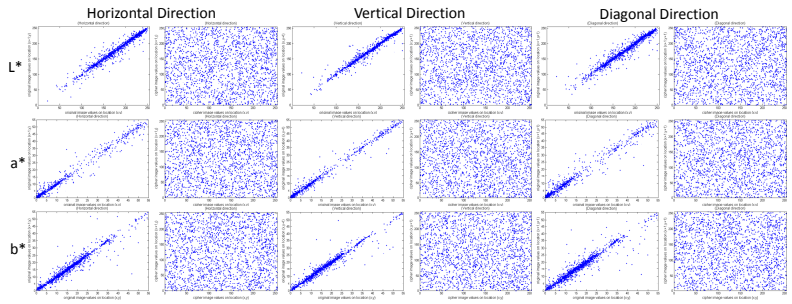

Fig. 7. The correlation of each channel of L*a*b* before and after encryption in 3 directions (horizontal, vertical and diagonal).

The Correlation Analysis 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 *Baby & Car* image and its corresponding cipher image.

6.3 The Speed of the Encryption and Decryption

The image encryption scheme is implemented by Matlab on personal computer with AMD Athlon(tm) X4 750 Quad Core Processor 3.4GHz and 4.00G RAM. The encryption and decryption consumption time is recorded for the images of different size. The larger size of the image, the more time it needs for encryption and decryption.

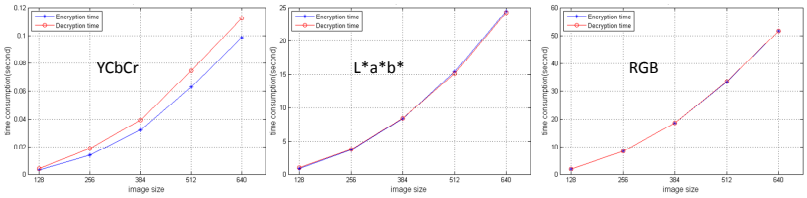

Fig. 8. The comparison of the speed of the encryption and decryption progress using the YCbCr method [1], our method and the RGB method [9] in several image resolutions: 128*128, 256*256, 384*384, 512*512, 640*640.

As show in Fig. 8, we test the speed of the encryption and decryption using the YCbCr method [1], our method and the RGB method [9] with various image sizes. The comparison show that although our method contains the color conversation at the beginning and the end of the method, it is faster than the RGB method [9]. The YCbCr method [1] is faster than both our method and the RGB method. However, as shown in the other experiments, our method performs as well as the RGB method [9], and both outperform the YCbCr method [1].

7 Conclusion and Discussion

In this paper, we are the first to encrypt color images in the CIE L*a*b* color space. In the informative L* channel, 2 high dimensional chaotic maps are adopted. While in the less informative a* and b* channel, we use the 1D logistic map with DNA encoding. Thus, we obtain good encryption results and high efficiency of color image encryption and decryption.

Although our method contains the color conversation at the beginning and the end of the method, it is faster than the RGB method [9]. The YCbCr method [1] is faster than our method and the RGB method. However, as shown in the other experiments, our method performs as well as the RGB method [9], and both outperform the YCbCr method [1].

In future work, we will utilize the fast speed of the YCbCr method and the good encryption performance of proposed L*a*b* method.

8 Acknowledgements

This work is partially supported by the National Natural Science Foundation of China (No.61402021, No.61402023, No.61170037), the Fundamental Research Funds for the Central Universities (No.2014XSYJ01, No.2015XSYJ25), and the Science and Technology Project of the State Archives Administrator. (No.2015-B-10).

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. Zhang Q., Guo L., Wei X. Image encryption using DNA addition combining with chaotic maps. Math Comput Model 52(11):202835 (2010)
6. Lab color space, `https://en.wikipedia.org/wiki/Lab_color_space`
7. Arnold's cat map, `https://en.wikipedia.org/wiki/Arnold\%27s_cat_map#cite_note-Arnold-1`
8. 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)
9. 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)
10. 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)
11. 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)