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

Xin Jin, Yingya Chen, Shiming Ge, Kejun Zhang, Xiaodong Li, et al.

Beijing Electronic Science and Technology Institute
GOCPCCC Key Laboratory of Information Security
Xidian University
Institute of Information Engineering, Chinese Academy of Sciences
Corresponding author: {jinxin,lxd}@besti.edu.cn

Outline

1 Motivation

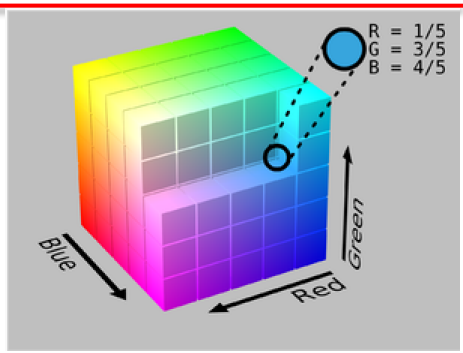
2 Preliminaries

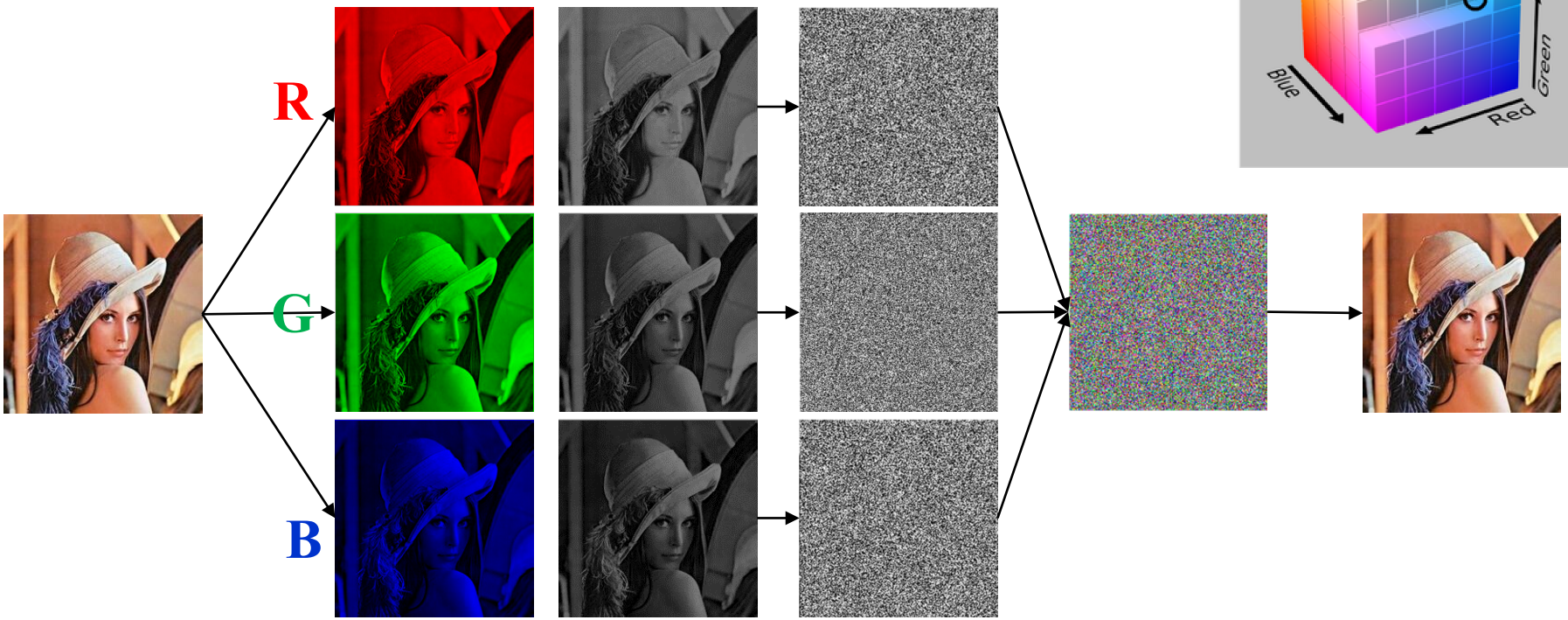
3 Color Image Encryption in L*a*b*

4 Results and Security Analysis

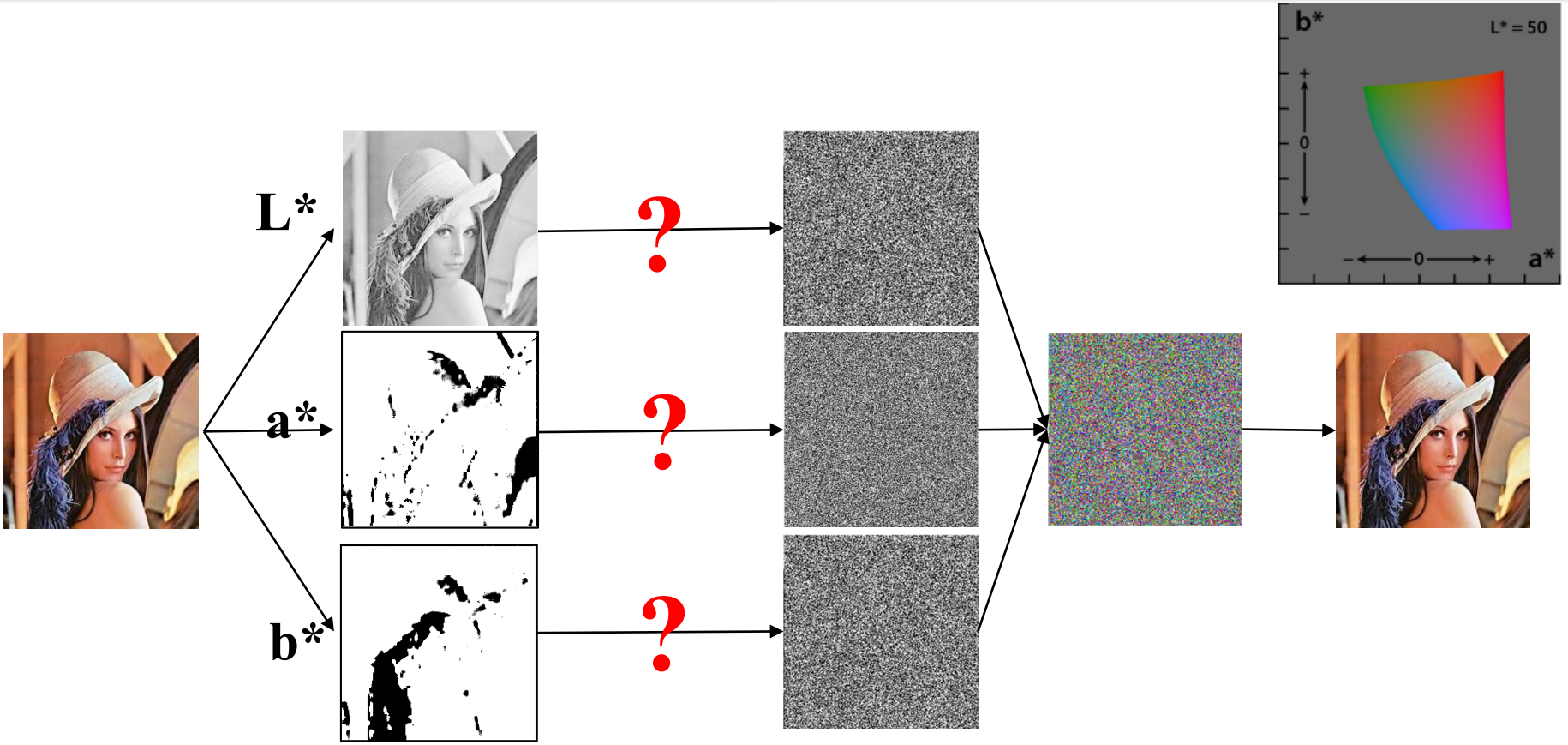
5 Conclusion and Discussion

Motivation





Motivation



Outline

1 Motivation

2 Preliminaries

3 Color Image Encryption in L*a*b*

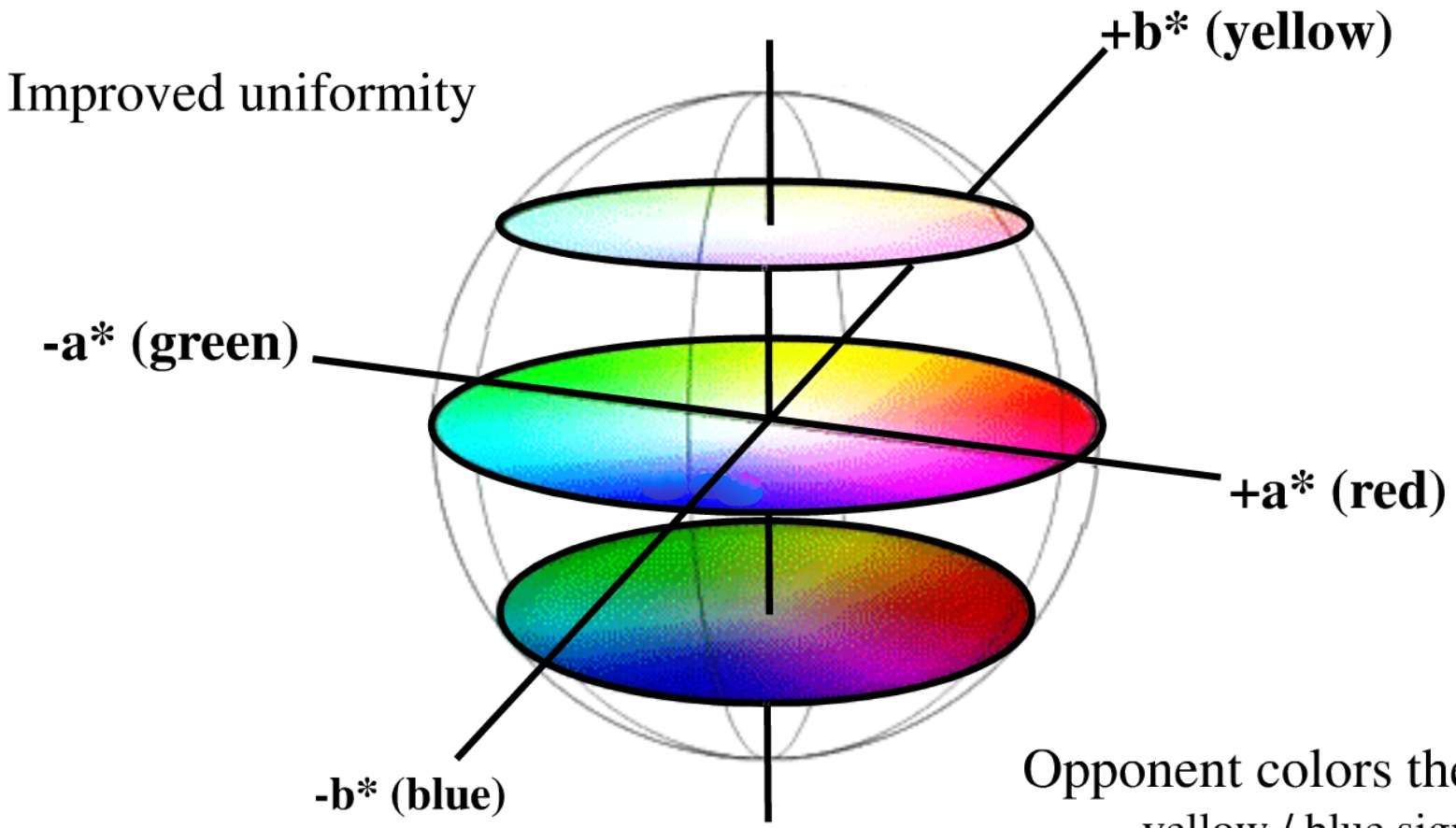
4 Results and Security Analysis

5 Conclusion and Discussion

Preliminaries

- CIE L*a*b* Color Space
- 1D Logistic map
- 2D Arnold cat map
- 3D Lu map
- DNA Computing

Preliminaries



Opponent colors theory !

yellow / blue signal

red / green signal

black / white signal

Preliminaries

RGB ⇒ XYZ ⇒ L*a*b*

$$\begin{cases} R = \text{gamma}(\frac{r}{255.0}) \\ G = gamma(\frac{g}{255.0}) \\ B = gamma(\frac{b}{255.0}) \end{cases}$$

$$\text{gamma(x)}=\begin{cases} (\frac{x+0.055}{1.055})^{2.4} & (x > 0.04045) \\ \frac{x}{12.92} & (\text{其它}) \end{cases}$$

$$\begin{bmatrix} X \\ Y \\ Z \end{bmatrix} = M * \begin{bmatrix} R \\ G \\ B \end{bmatrix} \qquad [M] = \begin{bmatrix} 0.436052025 & 0.385081593 & 0.143087414 \\ 0.222491598 & 0.716886060 & 0.060621486 \\ 0.013929122 & 0.097097002 & 0.714185470 \end{bmatrix}$$

$$\begin{cases} L^* = 116f\left(\frac{Y}{Y_n}\right) - 16 \\ a^* = 500\left[f\left(\frac{X}{X_n}\right) - f(\frac{Y}{Y_n})\right] \\ b^* = 200\left[f\left(\frac{Y}{Y_n}\right) - f(\frac{Z}{Z_n})\right] \end{cases}$$

$$\text{f(t)} = \begin{cases} t^{\frac{1}{3}} & if\ t > (\frac{6}{29})^3 \\ \frac{1}{3}(\frac{29}{6})^2 t + \frac{4}{29} & otherwise \end{cases}$$

Preliminaries

1D Logistic map

$$x_{n+1} = \mu x_n (1 - x_n)$$

$$3.569945672... < \mu \leq 4, 0 \leq x_n \leq 1$$

$$n = 0, 1, 2, ...$$

Preliminaries

2D Arnold cat map

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

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

Preliminaries

2D Arnold's cat map

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

a = 36, b = 3, c = 20

Preliminaries

DNA Encoding

8 bit Pixel 00011011

00 A ⟷ T 11

01 G ⟷ C 10

Preliminaries

DNA Computing

+	T	A	C	G
T	C	G	T	A
A	G	C	A	T
C	T	A	C	G
G	A	T	G	C

—	T	A	C	G
T	C	G	T	A
A	A	C	G	T
C	T	A	C	G
G	G	T	A	C

X	Complement(X)
A	T
T	A
C	G
G	C

Outline

1 Motivation

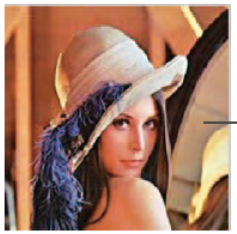
2 Preliminaries

3 Color Image Encryption in L*a*b*

4 Results and Security Analysis

5 Conclusion and Discussion

Color Image Encryption in L*a*b*



R

G

B

Color Conversion

L*

a*

b*

2D Arnold Cat Map

3D Lu Map

DNA Encoding

DNA Addition

DNA Complement

DNA Decoding

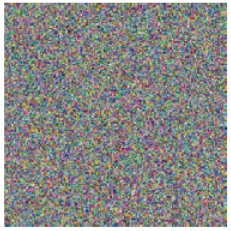
DNA Encoding

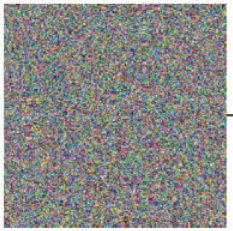
DNA Addition

DNA Complement

DNA Decoding

1D Logistic Map





L*

a*

b*

3D Lu Map

2D Arnold Cat Map

DNA Encoding

DNA Complement

DNA Addition

DNA Decoding

DNA Encoding

DNA Complement

DNA Addition

DNA Decoding

1D Logistic Map

L*

a*

b*

Color Conversion

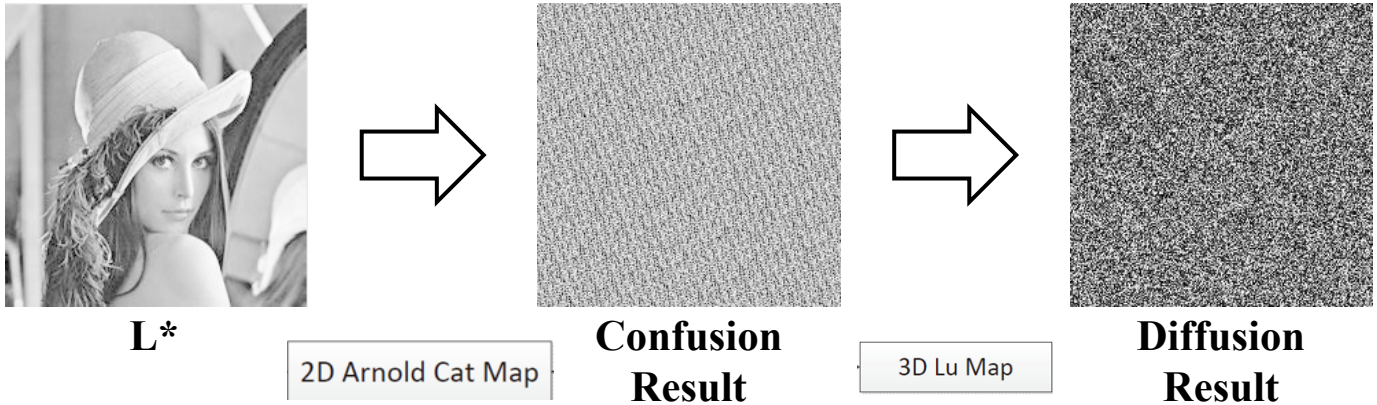
R

G

B

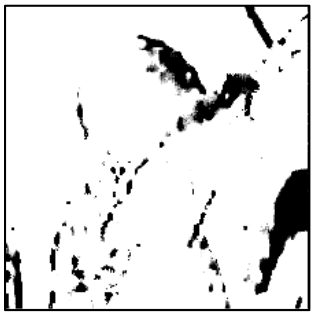
Color Image Encryption in L*a*b*

The L* Channel



Color Image Encryption in L*a*b*

The a*b* Channel



a* Channel

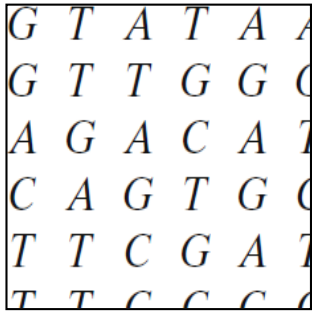
DNA Encoding

A_b

1D Logistic Map

(X',Y')

DNA Addition

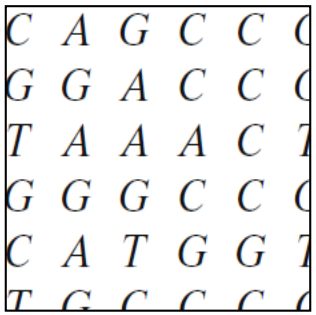


B

Complement

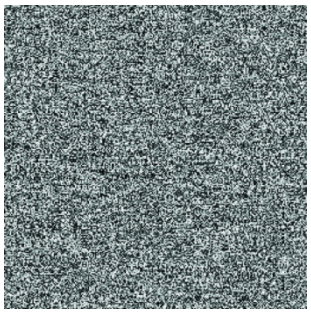
Z

1D Chaotic Map



B_{comp}

DNA Decoding



Cipher Image D

Outline

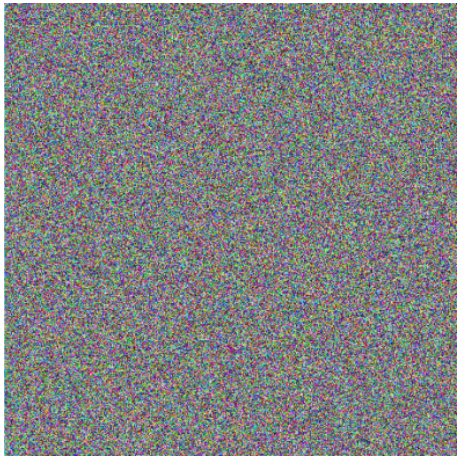
1. Motivation
2. Preliminaries
3. Color Image Encryption in L*a*b*
4. **Results and Security Analysis**
5. Conclusion and Discussion

The secret key

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

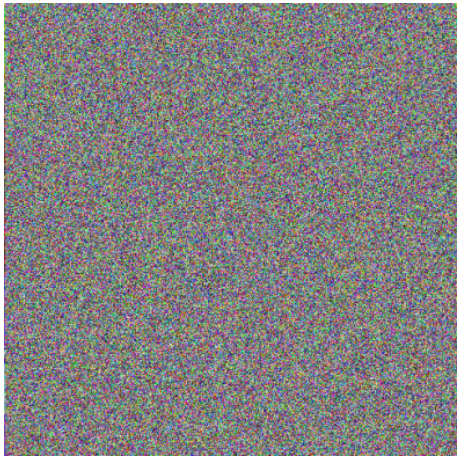
The Encryption Results

Tower



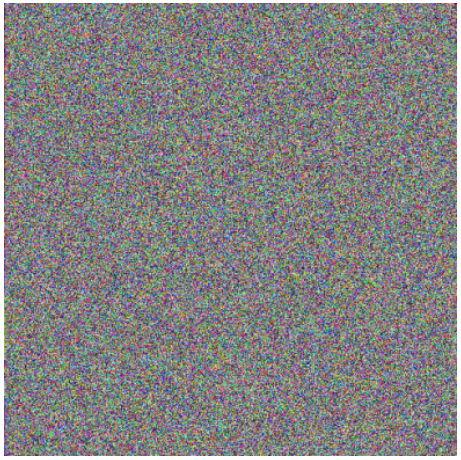
Cipher Tower

Jumpers



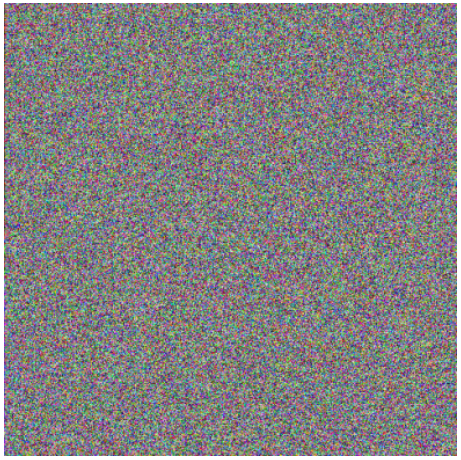
Cipher Jumpers

Soccer player



Cipher Soccer player

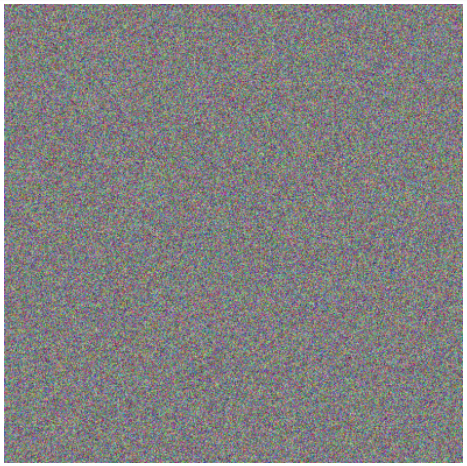
Building



Cipher Building

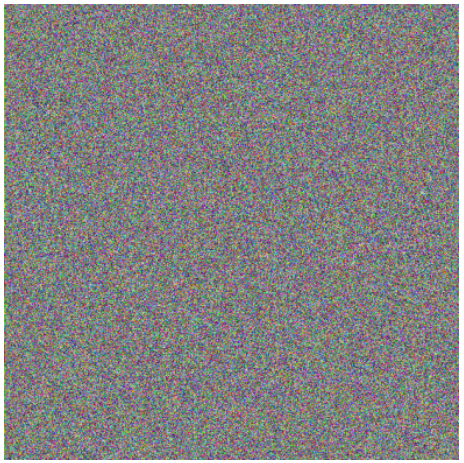
The Encryption Results

Group



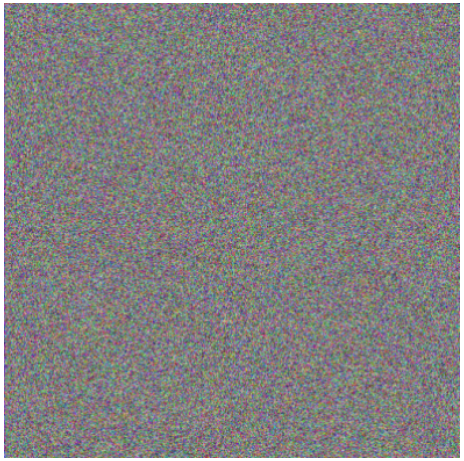
Cipher Group

Night view



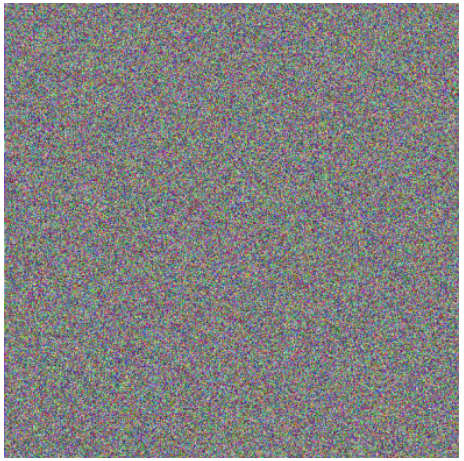
Cipher Night view

Baby



Cipher Baby

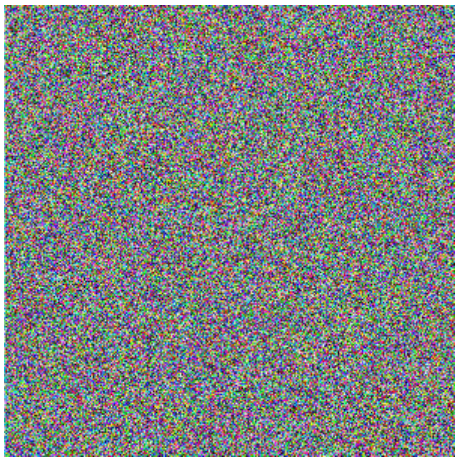
Girl



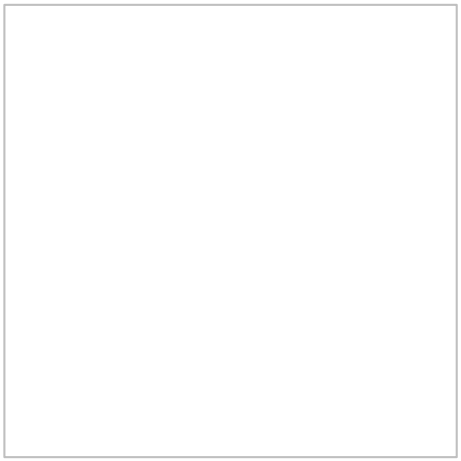
Cipher Girl

The Encryption Results

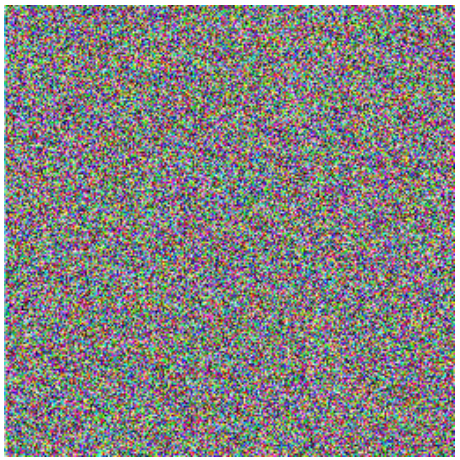
Black



Cipher Black



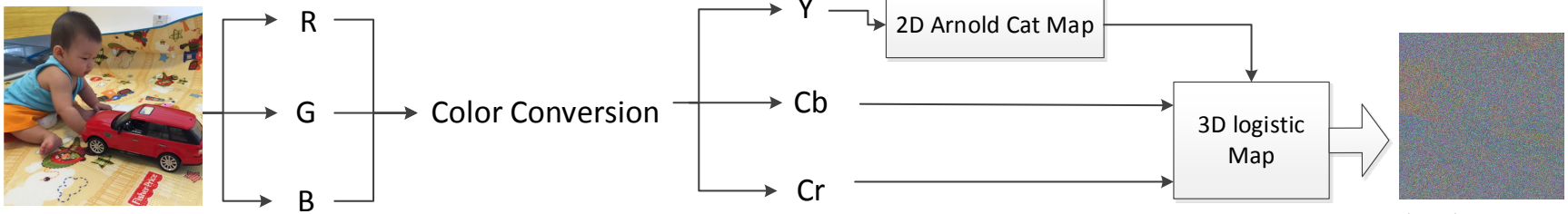
White



Cipher White

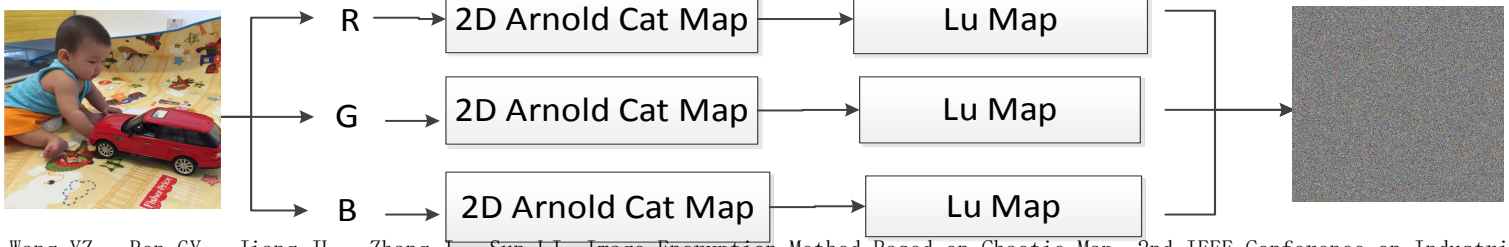
Comparisons and Security Analysis

YCbCr



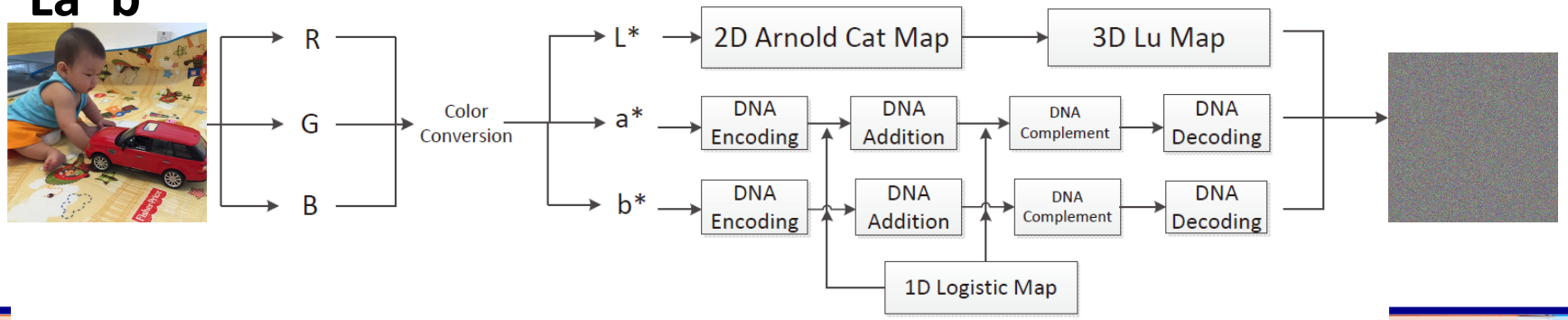
Mahdi, A., Alzubaiti, N. Selective Image Encryption with 3D Chaotic Map. European Academic Research. Vol.2, No.4, pp.4757-4773 (2014).

RGB



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)

La*b*



Key Space

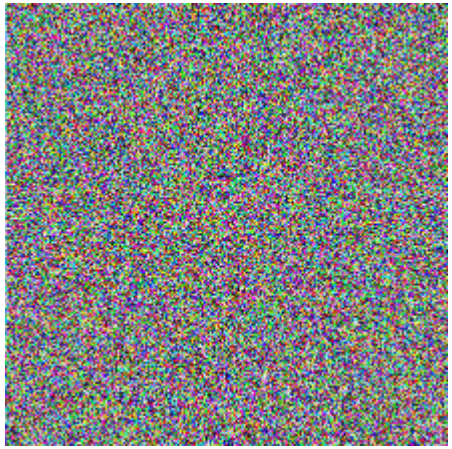
$$\begin{cases} \text{1D logistic: } 3.569945672... < \mu \leq 4, x_0 \in [0,1] \\ \text{2D Arnold: } N_{iteration} > 15, p, q \ are \ positive \ integers \\ \text{3D Lu:} a = 36, b = 3, c = 20, -40 < x_0 < 50, -100 < y_0 < 80, 0 < z_0 < 140 \end{cases}$$

The precision of 64-bit double data is 10^{-15}
The key space is about $(10^{15})^8 = 10^{120} \approx 2^{399}$
The max key space of AES = (2^{256})

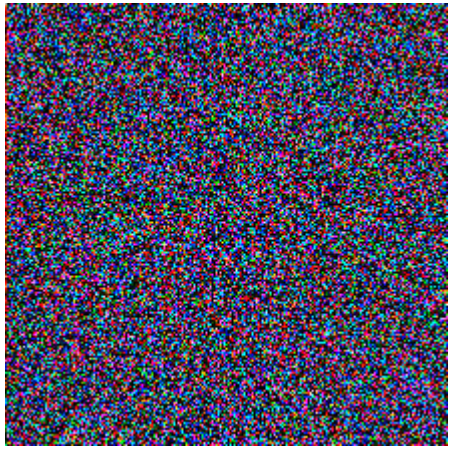
Sensitivity of Secret Key

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

Lena

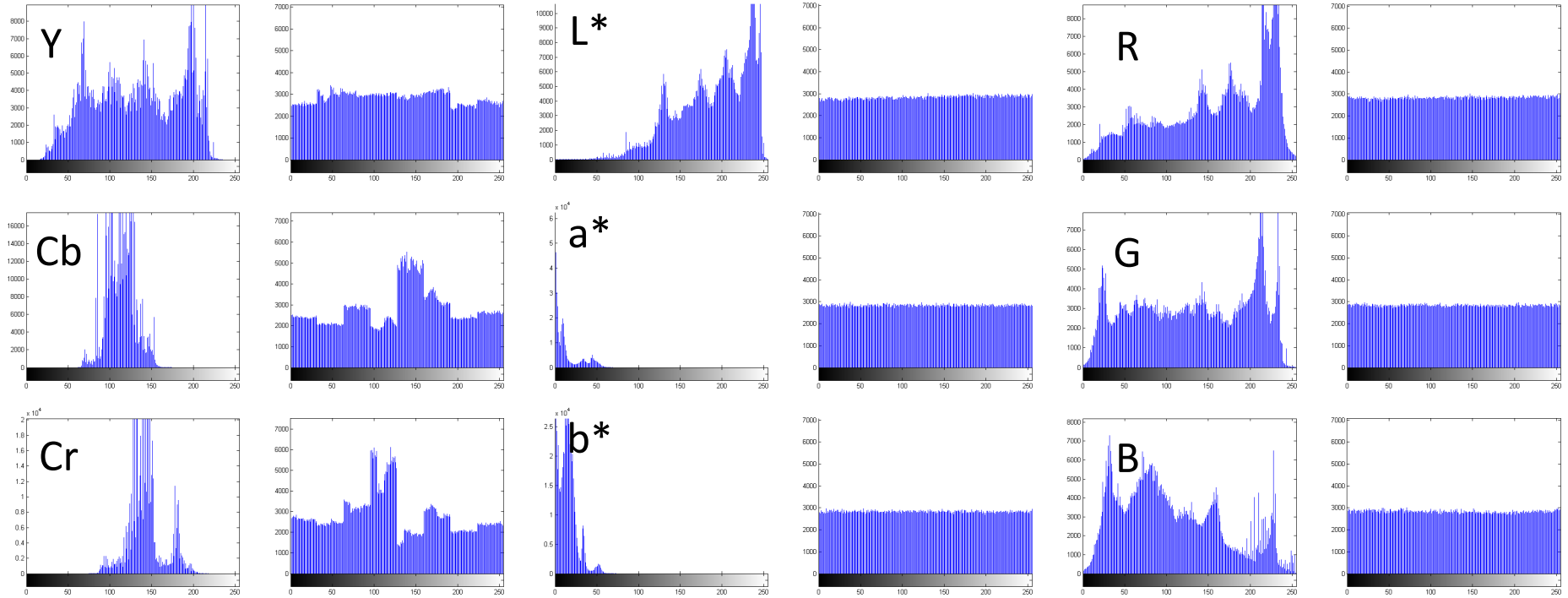


Cipher *Lena*



Decrypted with wrong key

The Histogram Analysis

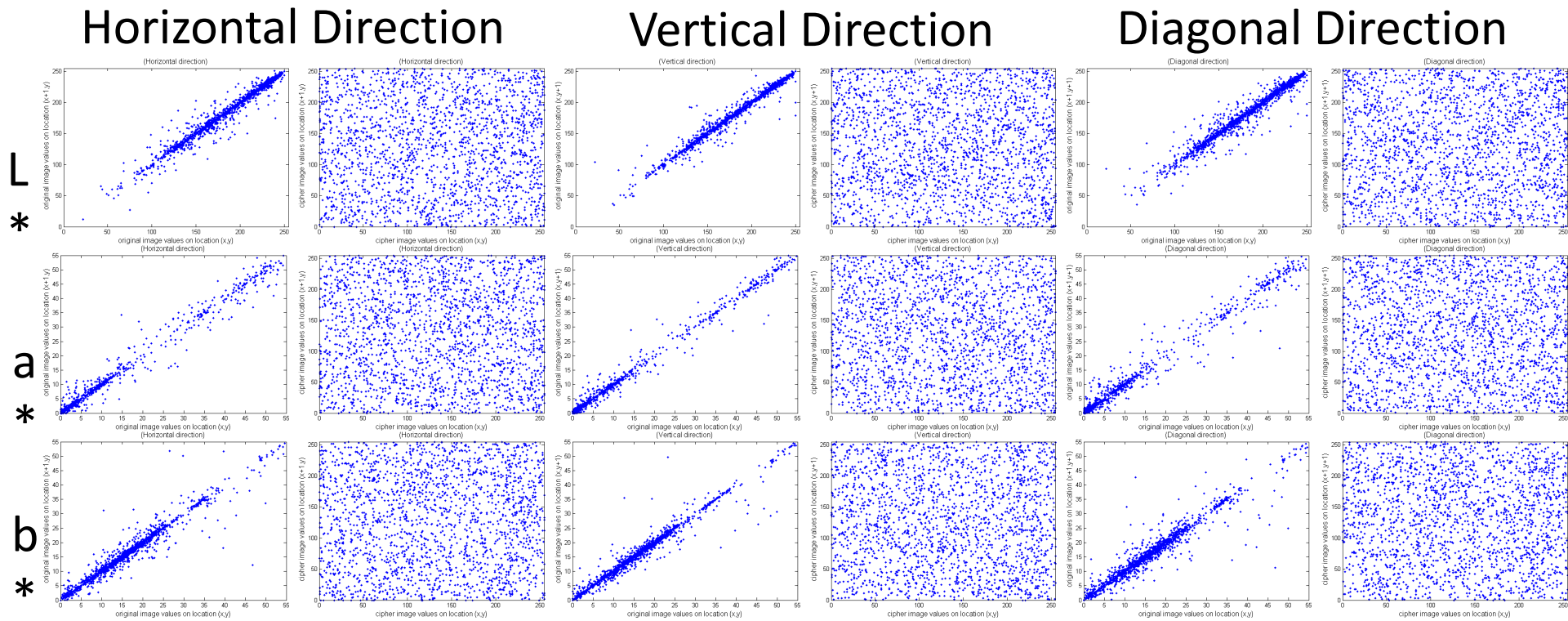


The Information Entropy

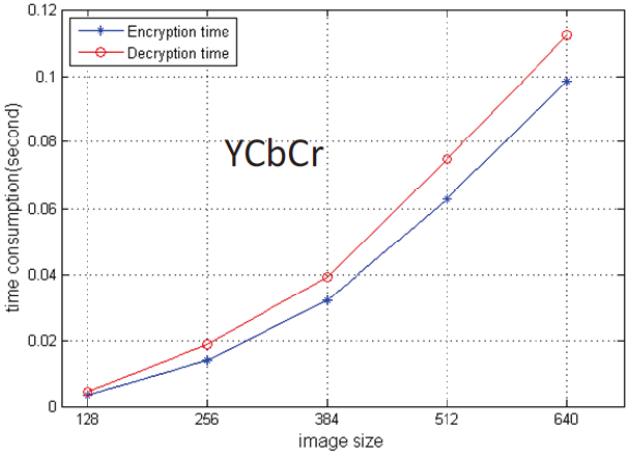
$$\mathrm{H}(m) = -\sum_{l=0}^{L} \mathrm{P}(m_i)\log_2(m_i)$$

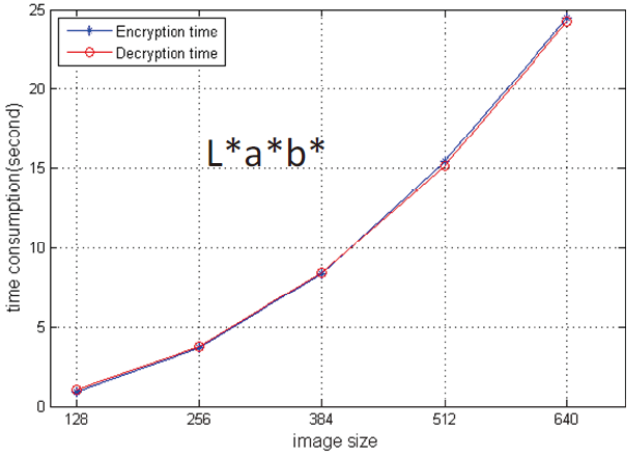
$$\begin{cases} \mathrm{H}(L*) = 7.9994, \mathrm{H}(a*) = 7.9998, \mathrm{H}(b*) = 7.9997 \\ \mathrm{H}(R) = 7.9997, \mathrm{H}(G) = 7.9998, \mathrm{H}(B) = 7.9996 \\ \mathrm{H}(Y) = 7.9940, \mathrm{H}(Cb) = 7.9350, \mathrm{H}(Cr) = 7.9196 \end{cases}$$

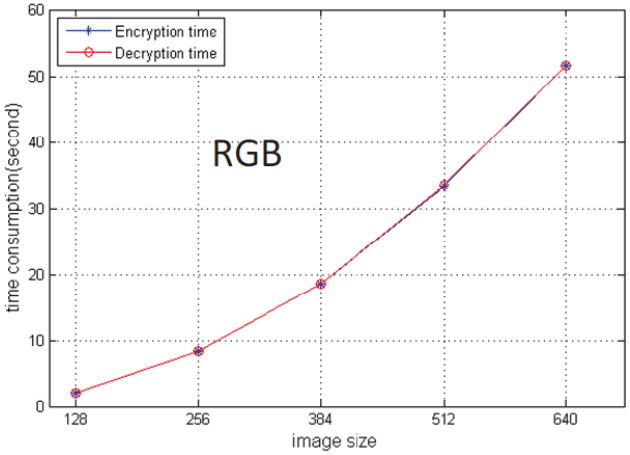
The Correlation Analysis



The Speed of the Encryption and Decryption







Outline

1. Motivation
2. Preliminaries
3. Color Image Encryption in L*a*b*
4. Results and Security Analysis
5. Conclusion and Discussion

Conclusion and Discussion

- **This is the first color image encryption algorithm in CIE L*a*b* space.**

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

Thanks !

Xin Jin, Yingya Chen, Shiming Ge, Kejun Zhang, Xiaodong Li, et al.

Beijing Electronic Science and Technology Institute
GOCPCCC Key Laboratory of Information Security
Xidian University
Institute of Information Engineering, Chinese Academy of Sciences
Corresponding author: {jinxin,lxd}@besti.edu.cn