Color Image Encryption in YCbCr Space

Xin Jin[1], Sui Yin[1], Xiaodong Li[1], Geng Zhao[1], Zhaohui Tian[2], Nan Sun[1], Shuyun Zhu[2]

[1]Beijing Electronic Science and Technology Institute
GOCPCCC Key Laboratory of Information Security
[2]Xidian University
Corresponding authors: {jinxin,lxd}@besti.edu.cn

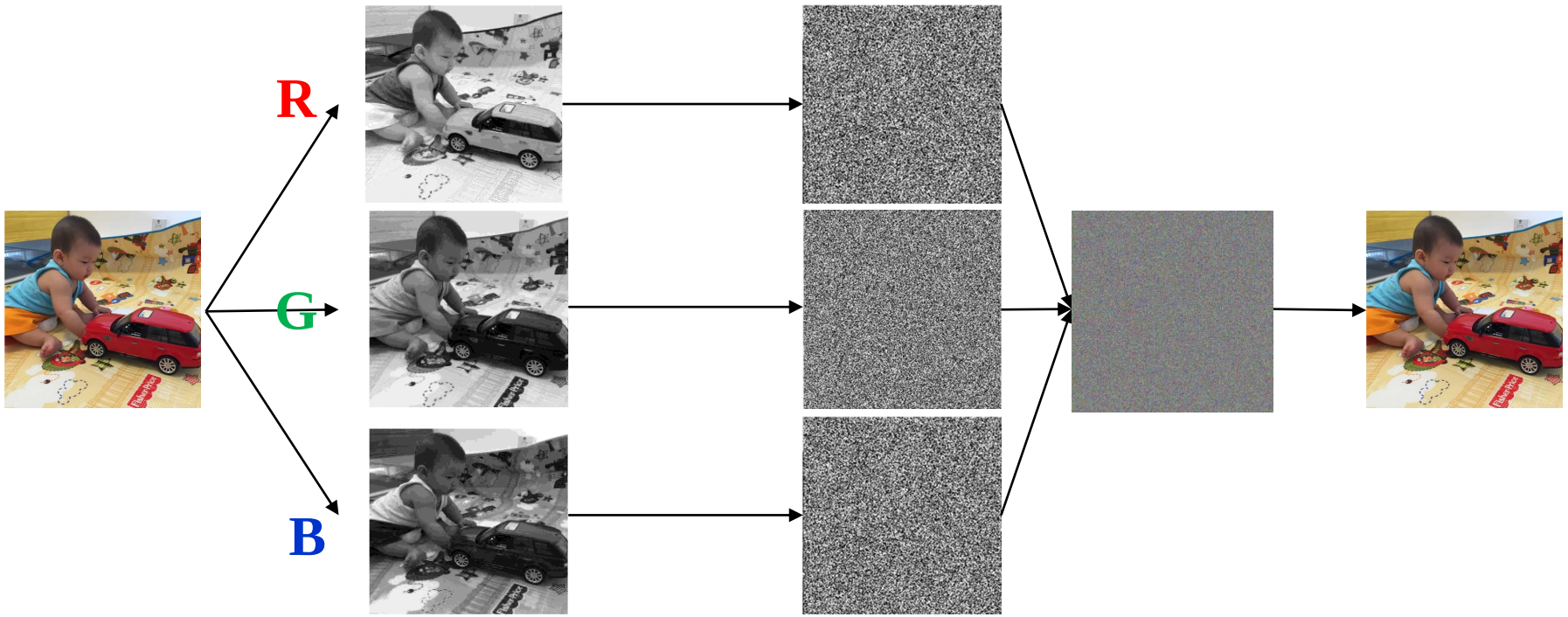
北京電子科技学院
Beijing Electronic Science and Technology Institute

VICTORY besti

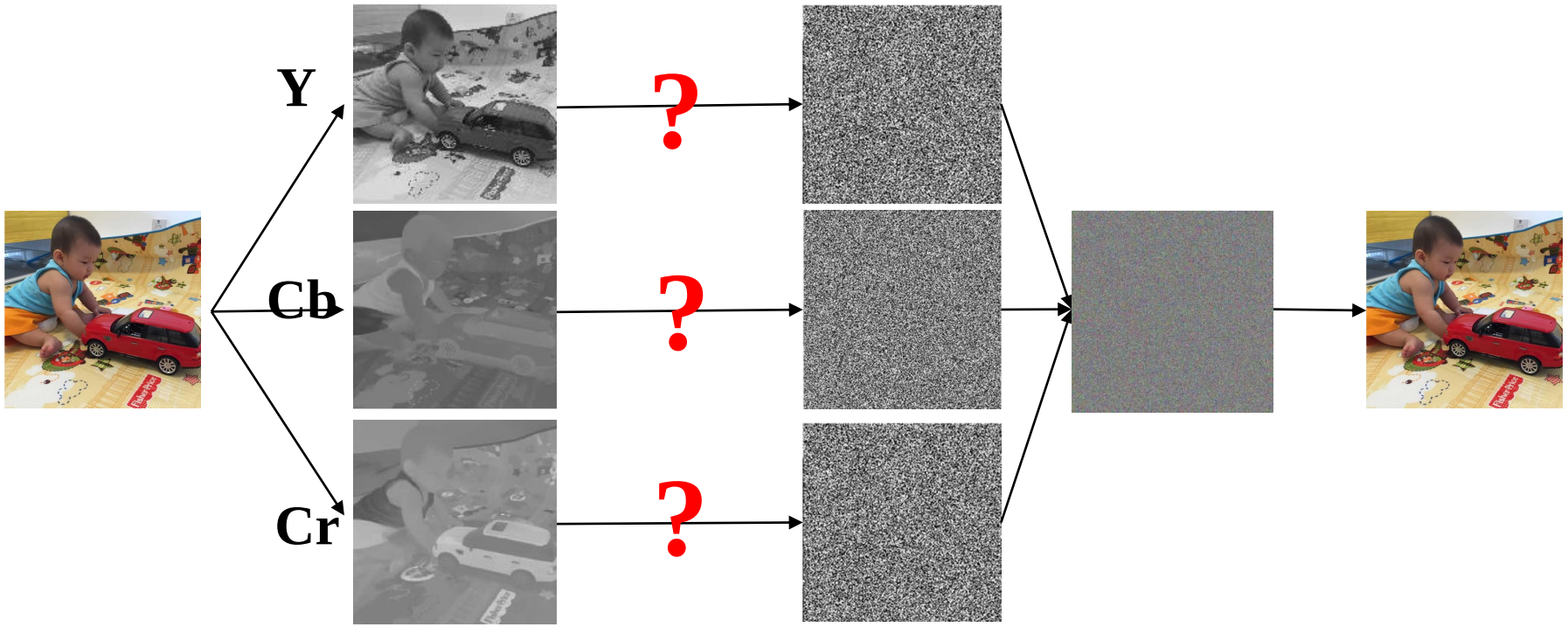
西安電子科技大學
XIDIAN UNIVERSITY

Outline

Motivation



Motivation



Outline

Preliminaries

- RGB→YCbCrr
- 1D Logistic map
- 2D Arnold cat map
- 3D Lu map
- DNA Computing

Preliminaries

RGB ⇒ YCbCr

$$\begin{bmatrix} Y \\ Cb \\ Cr \end{bmatrix} = \begin{bmatrix} 16 \\ 128 \\ 128 \end{bmatrix} + \begin{bmatrix} 0.257 & 0.504 & 0.098 \\ -0.148 & -0.291 & 0.439 \\ 0.439 & -0.368 & -0.071 \end{bmatrix} * \begin{bmatrix} R \\ G \\ B \end{bmatrix}$$

$$\begin{bmatrix} R \\ G \\ B \end{bmatrix} = \begin{bmatrix} 16 \\ 128 \\ 128 \end{bmatrix} + \begin{bmatrix} 1.164 & 0.000 & 1.596 \\ 1.164 & -0.392 & -0.813 \\ 1.164 & 2.0017 & -0.000 \end{bmatrix} * \begin{bmatrix} Y \\ Cb \\ Cr \end{bmatrix}$$

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

3D Lu 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

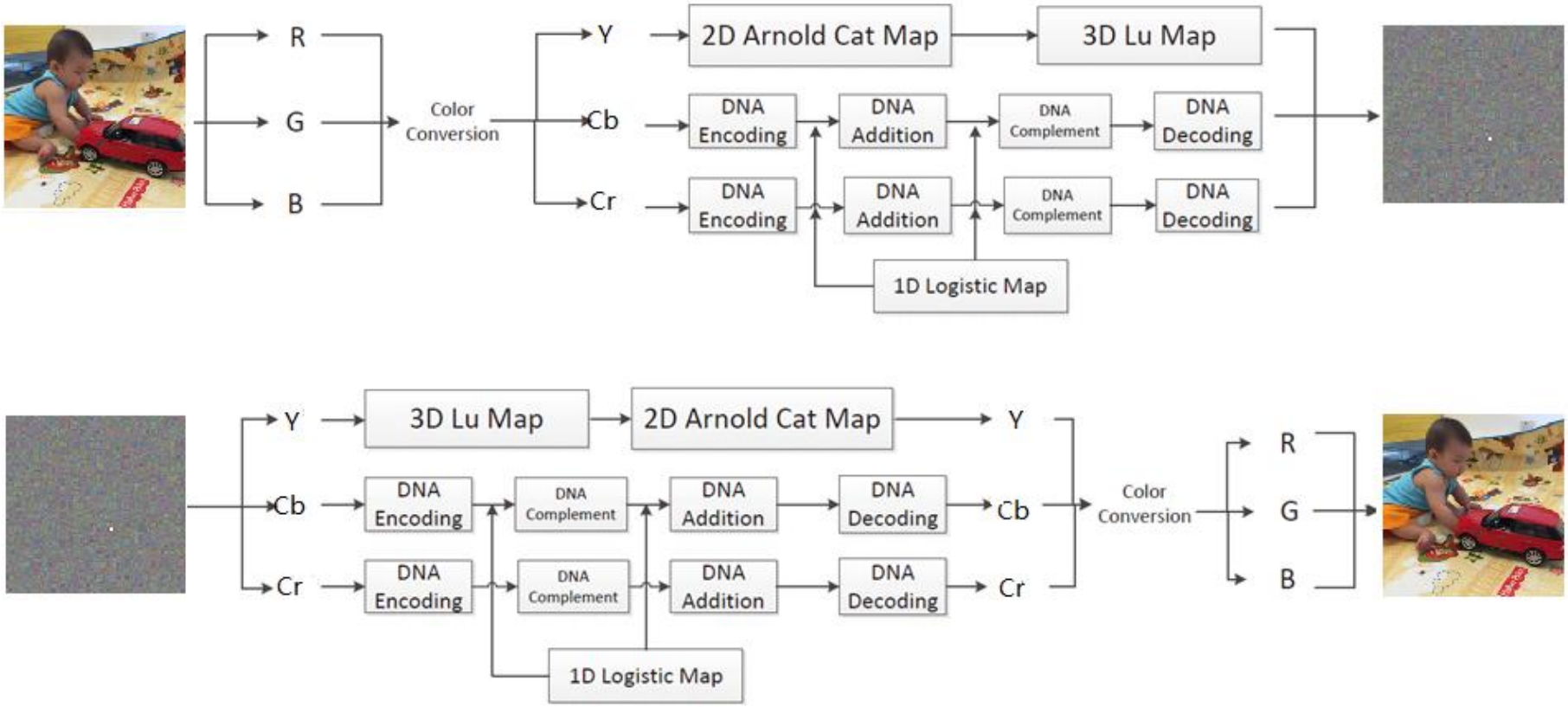
+	T	A	C	G
T	C	G	T	A
A	G	C	A	T
C	T	A	C	G
G	A	T	G	C

—	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

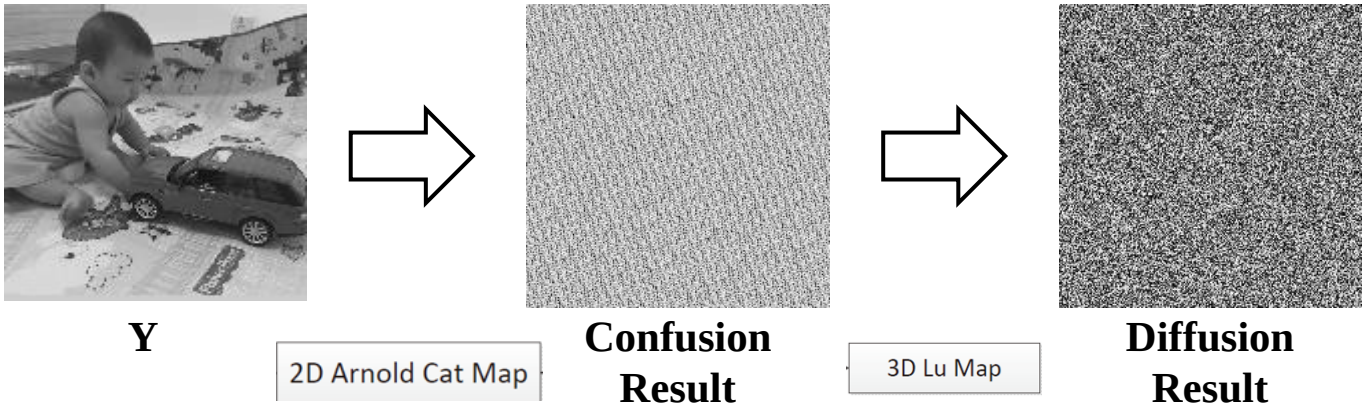
Outline

Color Image Encryption in YCbCr



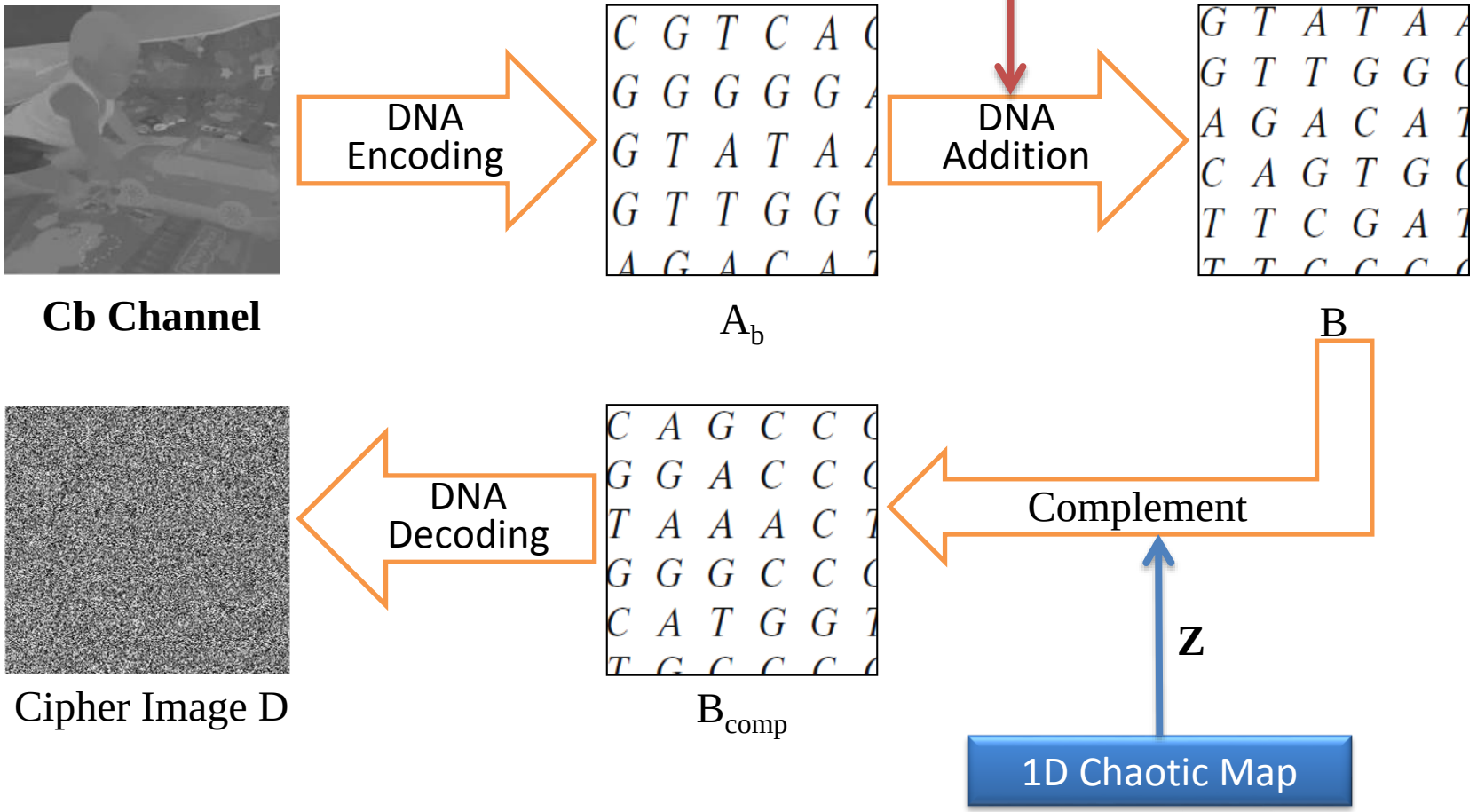
Color Image Encryption in YCbCr

The Y Channel



Color Image Encryption in YCbCr

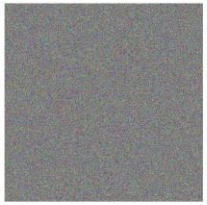
The CbCr Channel



Outline

The Encryption Results


lena

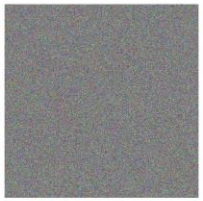



peppers


couple

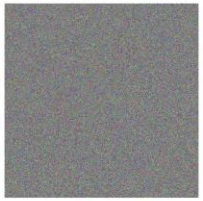

girl


airplane

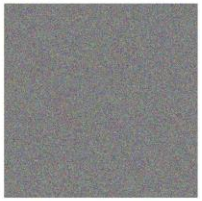



gorilla


sunset




snow



Key Space

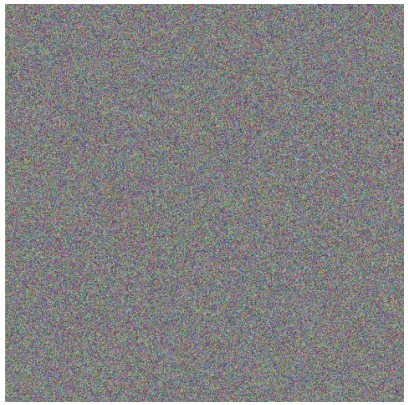
$$\begin{cases} \text{1D logistic: } 3.569945672... < \mu \leq 4, x_0 \in [0,1] \\ \text{2D Arnold: } N_{iteration} > 15, p, q \ are \ positive \ integers \\ \text{3D Lu:} a = 36, b = 3, c = 20, -40 < x_0 < 50, -100 < y_0 < 80, 0 < z_0 < 140 \end{cases}$$

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

$$\begin{cases} x_0 \text{ from } -6.045 \text{ to } -6.045000000000001 \\ x_0^{a*} \text{ from } 0.62 \text{ to } 0.620000000000001 \\ x_0^{b*} \text{ from } 0.26 \text{ to } 0.260000000000001 \end{cases}$$

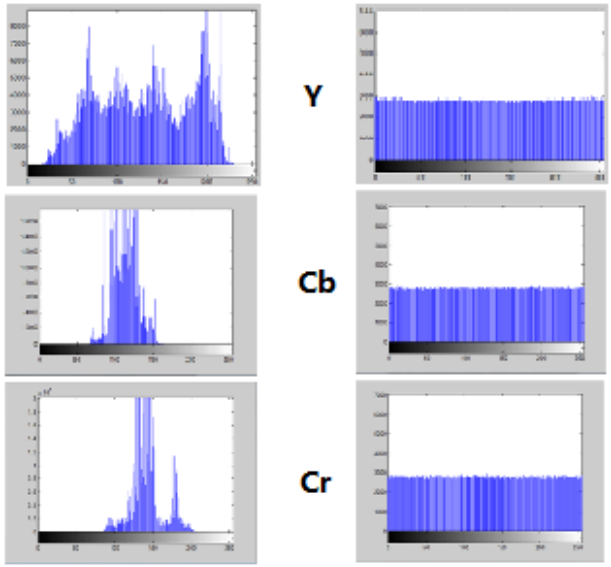
dubao

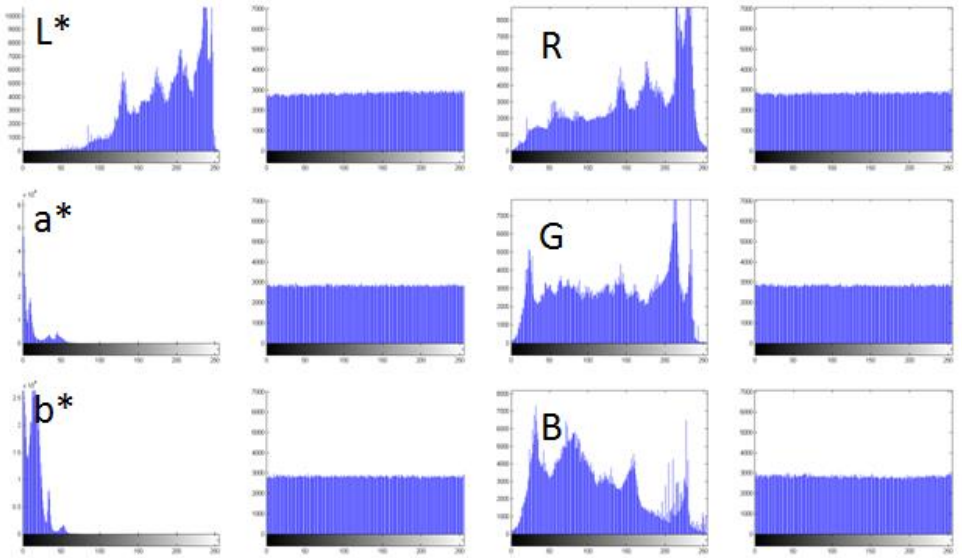


Cipher *dubao*

Decrypted with wrong key

The Histogram Analysis



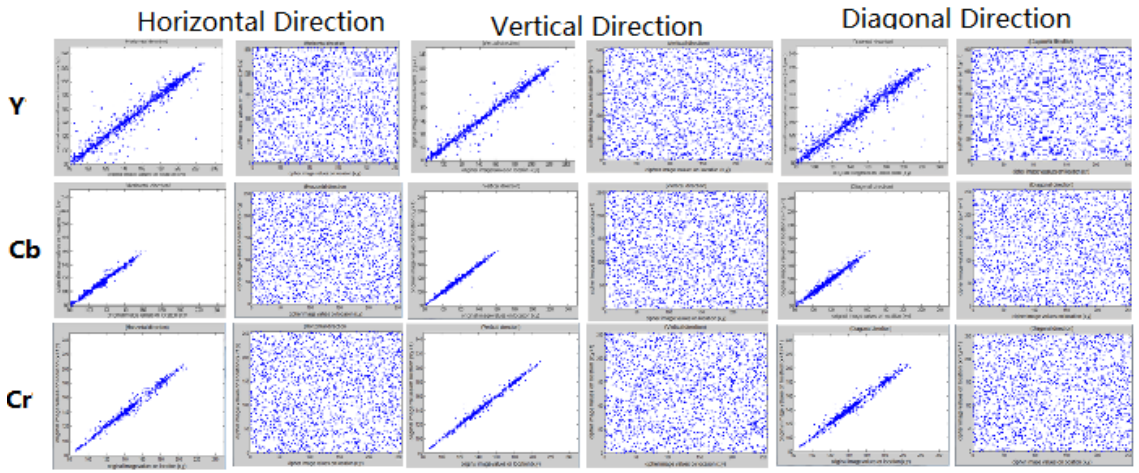


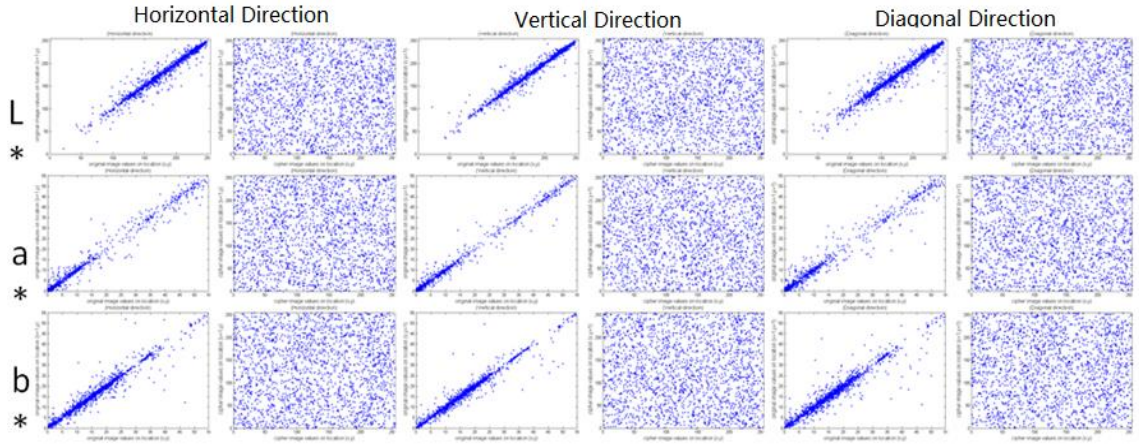
The Information Entropy

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

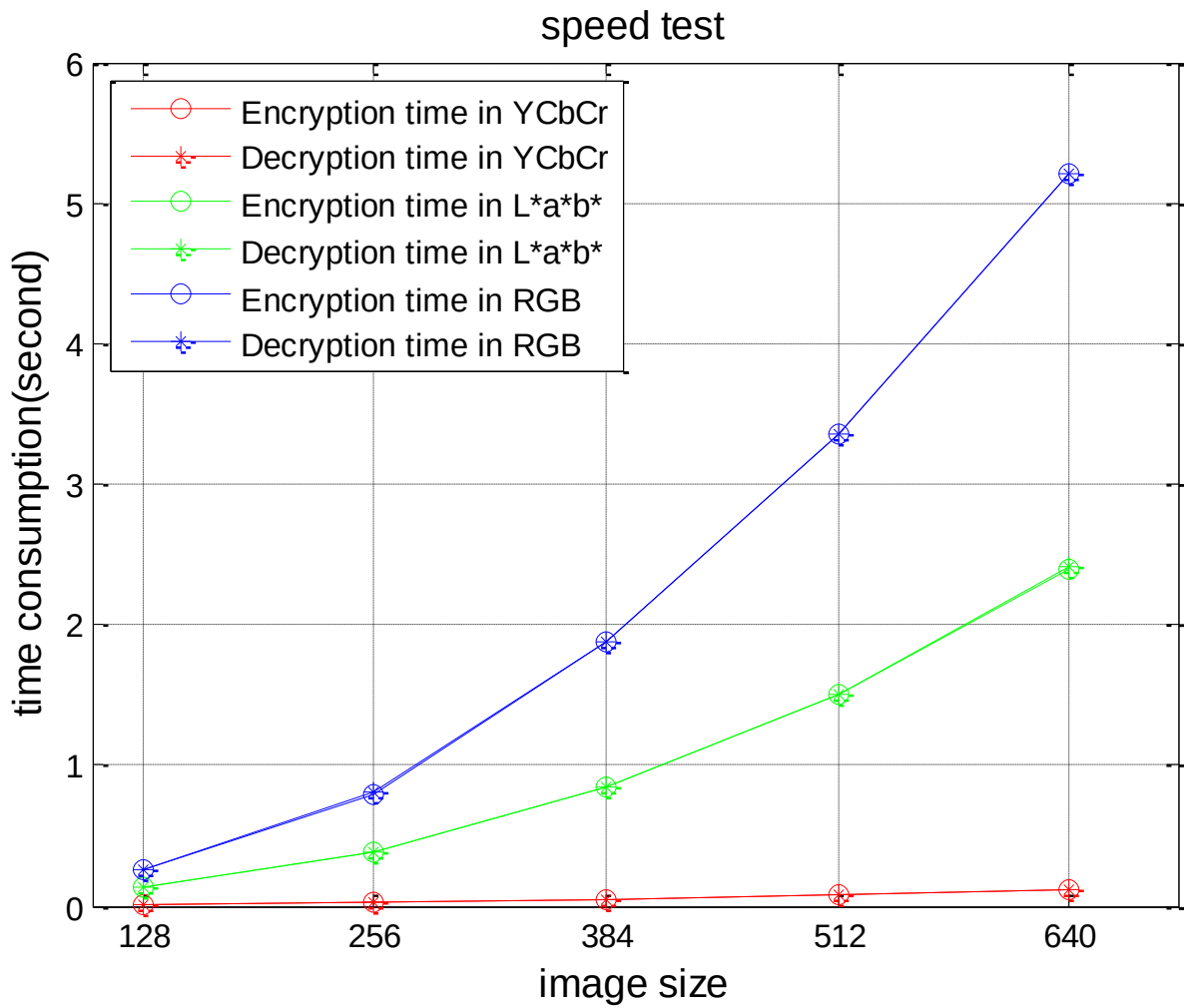
YCbCr	H(m)	L*a*b*	H(m)	RGB	H(m)
Y	7.9996	L*	7.9961	R	7.9815
Cb	7.9998	a*	7.9952	G	7.9815
Cr	7.9997	b*	7.9815	B	7.9815

The Correlation Analysis

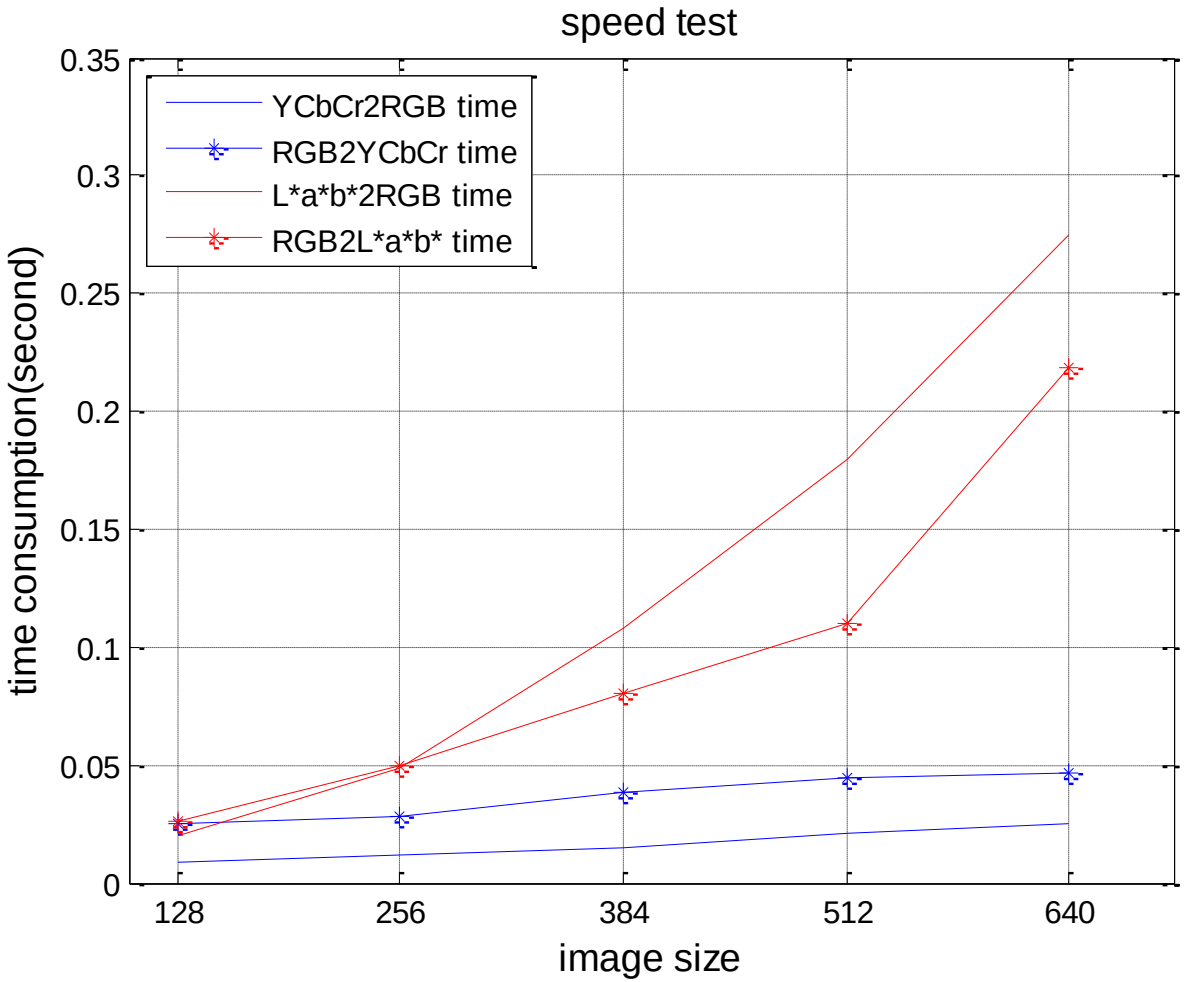




The Speed of the Encryption and Decryption



The Speed of the Encryption and Decryption



Outline

1. Motivation
2. Preliminaries
3. Color Image Encryption in YCbCr Space
4. Results and Security Analysis
5. Conclusion and Discussion

Conclusion and Discussion

- **A color image encryption algorithm in YCbCr space.**

- **In future work, we will utilize the fast speed of the YCbCr method and continue to improve the encryption algorithm to have a better and faster way.**

Thanks !

Scan to visit our
Victory Team
of Besti (WeChat)