Color Image Encryption in YCbCr Space

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

[1]Beijing Electronic Science and Technology Institute, 100070, Beijing,China
[2]Xidian University, 710071, xi'an,China
*Corresponding Author: lxd@besti.edu.cn

***Abstract*—Nowadays, with the development of Internet technology and the improvement of safety awareness, image encryption technique has become very important, especially for color image encryption. The direction of research is focused on the RGB color space. There are few researches in other color spaces, such as HSV，L*a*b*, YCbCr. In this paper, we propose a color image encryption method in YCbCr color space. There is much information in Y channel but little information in Cb and Cr channel. Using this feature, we choose different encryption schemes. We first convert the color space from RGB to YCbCr. Then we encrypt the three channels separately. In Y channel, with Arnold cat map, we can do the preliminary image confusion, and then we use three-dimensional Lu chaotic map to do the further image diffusion. In Cb and Cr channels, we use DNA encoding and 1D Logistic chaotic map. Experimental results show that our color image encryption works well, our method in YCbCr space can compare with the RGB and L*a*b* space, and can resist brute-force attacks, differential attacks. The most prominent point is that the speed of encryption and decryption is much faster.**

Keywords—Color Image Encryption；YCbCr color space; Chaos map; DNA encoding .

I. Introduction

With the rapid popularization of cameras, video cameras, smart phones, images, video, 3D and other visual media, big data is rapidly formed, more and more frequent exchange of digital images in the social network is using, the security environment in the cloud of digital images handle network security has become a new challenge to be solved. For example, the digital image obtained through the network will be used for illegal purposes, related to security issues of national security, social security, personal privacy and other aspects. image encryption is the important prerequisite of image retrieval security, video security, video surveillance security, video processing security and other visual media security applications. Therefore, security of image encryption technology became extremely important.

As color images encryption is concerned, many other color spaces except RGB color space, such as HSV, L * a * b *, YCbCr, etc., have not been fully excavated and utilized. This paper designed and implemented a new color image encryption method in the YCbCr color space. And respectively compare the encryption method to that in RGB and L * a * b * space and then give the results of the analysis.

A. *Related Work.*

Chaos encryption technology has been studied for some time, First, because of the features of chaos, such as sensitivity to initial conditions and system parameters, pseudo-randomness and ergodicity, etc. It can be applied to image encryption field due to the high complexity of chaotic systems, and it can improve the image encryption security and reliability.

At present, color image encryption method, is almost all in the classic RGB color space. Since the three channels of RGB space has a strong correlation, there are some problems for this color image encryption algorithm, in the image encryption process, when take the operation for each pixel ,it will have the same input and output. It resulted in the redundancy of cryptographic operations, so its time efficiency is not satisfactory, which would to be further improved. There is little research in other color spaces, Jin studied selective encryption on the L * a * b * space [11] before, the encryption and decryption works well, but the speed of encryption and decryption is relatively slow, which promote us to search for more faster encryption method or in other color spaces.

B. *Our Approach*

In this paper, we encrypt the image in the YCbCr color space, draws on the L * a * b * space selective encryption method [11], we use sophisticated encryption methods in the Y channel contained a large amount of information while simple encryption methods in the Cb and Cb channels contained little information. Our experimental results show that the effect is equally good encryption, and prominent advantage is much faster encryption and decryption speed than that in L * a * b * space.

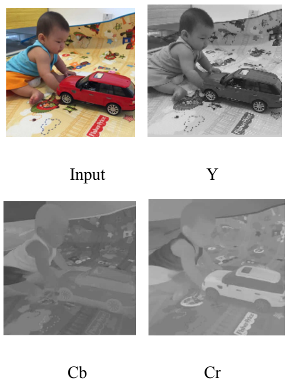

Fig. 1. Inpur image and Y,Cb,Cr channel image

As shown in Fig. 1,this paper make a conversion from RGB to YCbCr space, it is evident that the Y channel contains more information while the Cb channel and Cr channel contains less information.

II. Basic Theory.

In this paper, we adopt 1D logistic map, the 2D Arnold's cat map and the 3D Lu map.

A. 1D Logistic map

1D logistic map is simple,it is defined as follows:

$$f(x)=\mu x(1-x),\quad x\in[0,1] \tag{1}$$

In Eq. 2 where μ is a constant, when $x\in[0,1]$, $f(x)\in[0,1]$, $0\le\mu\le4$,This sequence generated maps shows the characteristics of chaos.

B. 2D Arnold's cat map

Arnold's cat map is a chaotic map from the torus into itself, 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.

C. 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 pa-rameters. When a = 36, b = 3, c = 20, the system contain a str-ange attractor and being in chaotic state.

III. Privacy Preserving ViBe.

A. Our method

In this section of the paper, we will explain the detail of the process of encryption and decryption in YCbCr color space, as shown in Fig. 2.

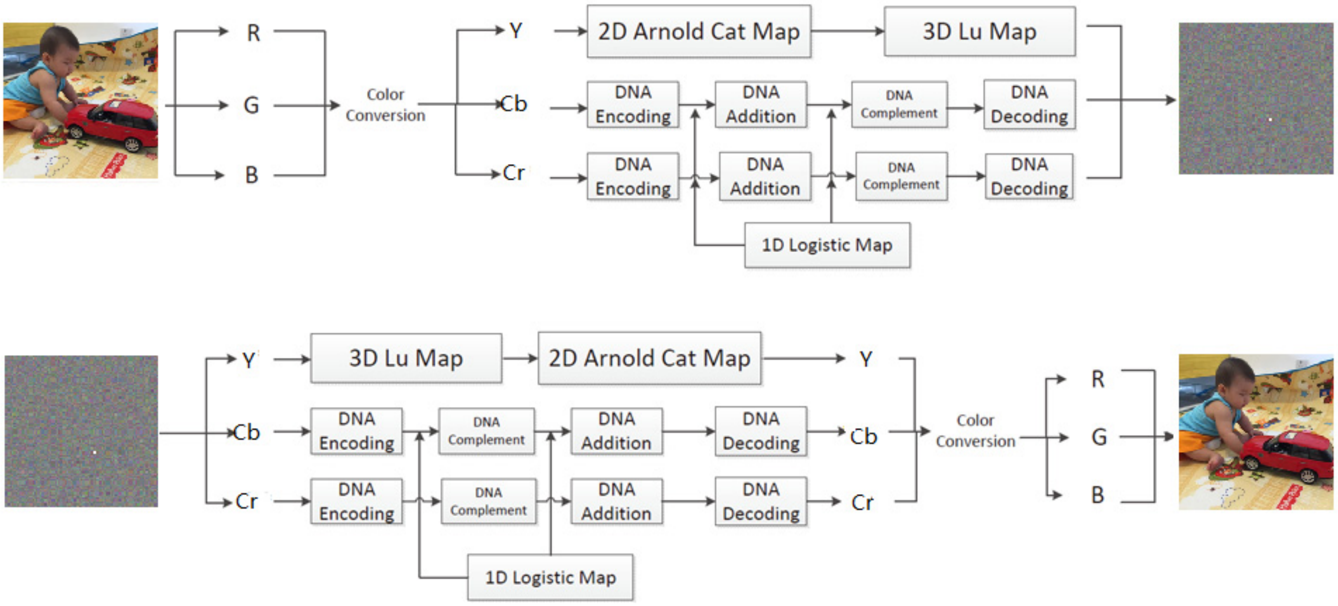

Fig. 2. Our proposed method for color image encryption in YCbCr space.

B. *Color space conversion （RGB toYCbCr）*

YcbCr model is defined as follows.

Y represents the luminance value, its range is [16,235]，and it can be learned by the weighting and calculation of RGB.

Cb component is obtained by the difference between blue and luminance component, its range is [16,240].

Cr component is obtained by the difference between red and Y component, its range is [16,240].

The convert model is defined in Eq. 5 and Eq. 6.

$$\begin{bmatrix} Y \\ Cb \\ Cr \end{bmatrix} = \begin{bmatrix} 16 \\ 128 \\ 128 \end{bmatrix} + \begin{bmatrix} 0.257 & 0.504 & 0.098 \\ -0.148 & -0.291 & 0.439 \\ 0.439 & -0.368 & -0.071 \end{bmatrix} * \begin{bmatrix} R \\ G \\ B \end{bmatrix} \tag{5}$$

$$\begin{bmatrix} R \\ G \\ B \end{bmatrix} = \begin{bmatrix} 16 \\ 128 \\ 128 \end{bmatrix} + \begin{bmatrix} 1.164 & 0.000 & 1.596 \\ 1.164 & -0.392 & -0.813 \\ 1.164 & 2.0017 & -0.000 \end{bmatrix} * \begin{bmatrix} Y \\ Cb \\ Cr \end{bmatrix} \tag{6}$$

C. *Color 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. 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, which can enhance the safety.

D. *Color Image Diffusion*

We use the 3D Lu map for the diffusion. The steps are as follows [9]:

(1) Give the initial value x_0, y_0, z_0 of the Lu map, let the system iterate N ×N times, produce three sequence values each time.

(2) Take the decimal fraction of three values, and put fourths of the three fractions together and constitute a new integer A.

(3) The remainder of A(mod 256) is converted binary, so the result of A(mod 256) must be in this scope.

(4) Convert the encrypted value to binary, and let two binary values exclusive or processing, total N × N times.

(5) convert the decimal again. It will return to the 2D image, and than complete the second encryption.

IV. Experimental Results

A. *Color image encrption results*

We can see from the experimental results, as shown in Fig.3. In this paper YCbCr space encryption effect is very good. Just because the encryption of different photos, the effect can not be exactly the same.

B. *Resistance to the brute-force Attack*

The key space is defined as Eq.7.

$$\begin{cases} \text{1D logistic: } 3.569945672... < \mu \leq 4, x_0 \in [0,1] \\ \text{2D Arnold: } N_{iteration} > 15, p, q\ are\ positive\ integers \\ \text{3D Lu:} a = 36, b = 3, c = 20, -40 < x_0 < 50, -100 < y_0 < 80, 0 < z_0 < 140 \end{cases} \tag{7}$$

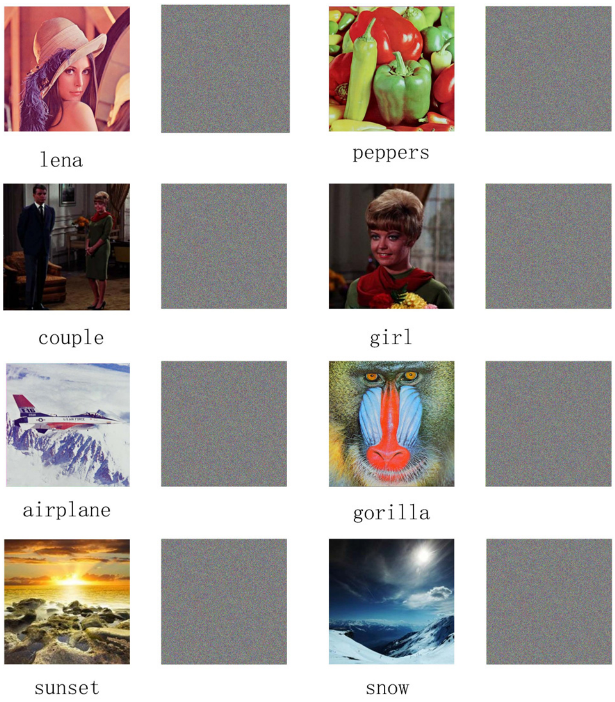

Fig. 3. Our experiment results

We can know that the key space is $(10^{15})^8 = 10^{120} \approx 2^{399}$, while the key space of practical symmetric encryption of the AES is 2^{256}, thus . Our key space is large enough to resist brute-force attack.

If we change the secret key as follow, We can see that the decrypted image is completely different from the original image. As shown in Fig. 4.

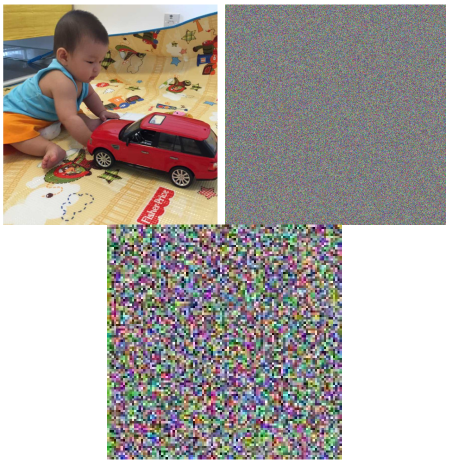

Fig. 4. Decrypted with wrong key

C. *Resistance to the Statistic Attack*

The histogram is used to analyze the distribution of the image intensity, image encryption is to make the image intensity evenly distributed, to resist to the Statistic Attack. The flatter the histogram encrypted, the better the encryption effect, the worse the contrary.

As show in Fig. 5 and Fig. 6, The histogram of each channel of YCbCr, L*a*b* and RGB before and after encryption.

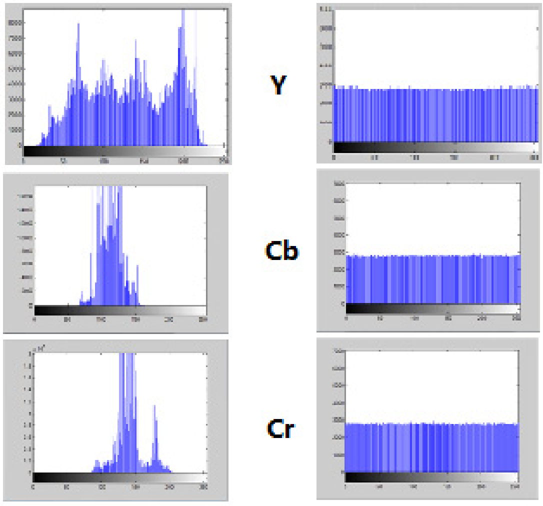

Fig. 5. Decrypted channel in YCbCr space

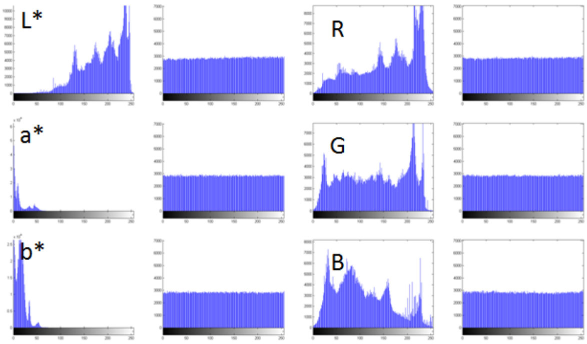

Fig. 6. Decrypted channel in L*a*b* space and RGB space

We can see that our approach is comparable with the L * a * b * and RGB space.

D. *The Histogram Analysis*

The histogram is used to show the distribution of pixel values of a gray image. The more concentrated the correlation diagram shows, the stronger the correlation is, and the more dispersed, the weaker correlation is. Image encryption is to diminish its relevance, and thus protect against statistical attacks.

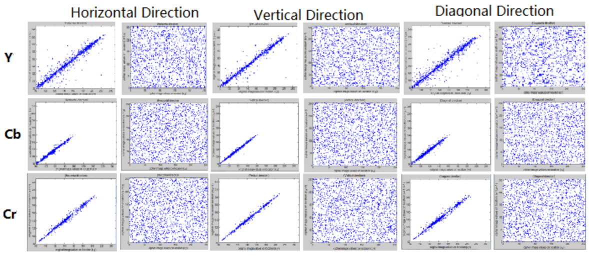

Fig. 7. Histogram in YCbCr space

As Fig. 7 shows, we can see that after encryption the correlation is very weak, which indicates that the encryption effect is very good.

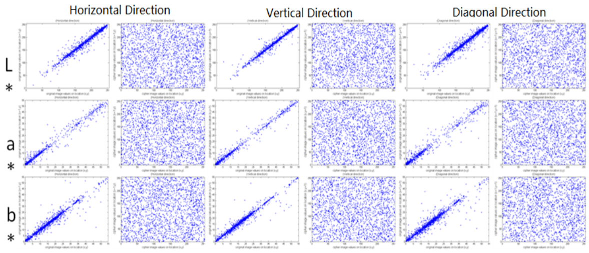

Fig. 8. Histogram in L*a*b* space

Comparing Fig. 7 with Fig. 8, we can see that in this paper the encryption in YCbCr space is as well as L * a * b * space.

E. *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:

$$H(m) = -\sum P(m_i)\log_2 P(m_i) \tag{8}$$

The information entropy of an ideal random image is 8, The information entropy of the cipher image should be close to 8 after encryption.

In this paper, the information entropy of all channels is shows in Table 1:

Table 1. the information entropy of all channels in three color spaces

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 results show that our method performs as well as the RGB method (the entropy is very close to 8), and both outperform the L*a*b* method [11].

F. The encryption and decryption speed

The most prominent feature of this paper is that the encryption and decryption speed is very fast, which can been seen from Fig. 9

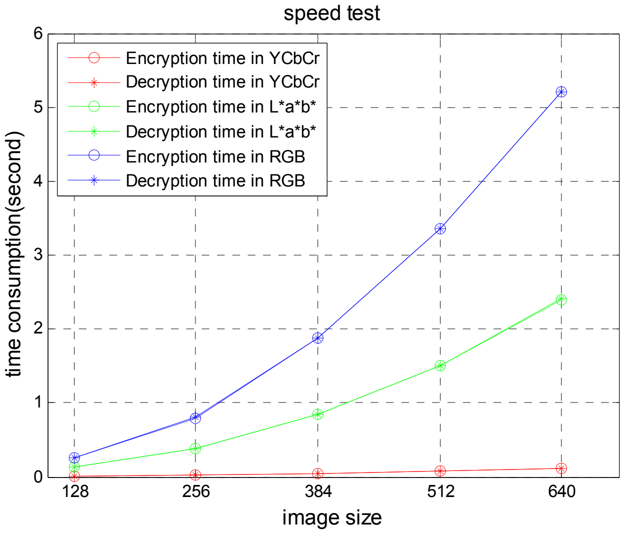

Fig. 9. Encryption and decryption speed in YCbCr, L*a*b* and RGB

The results show that the encryption and decryption speed of YCbCr space is much faster than RGB space and L*a*b* space.

In this paper, we analysis that the reason of so fast is that the conversion from RGB to YCbCr is very fast.

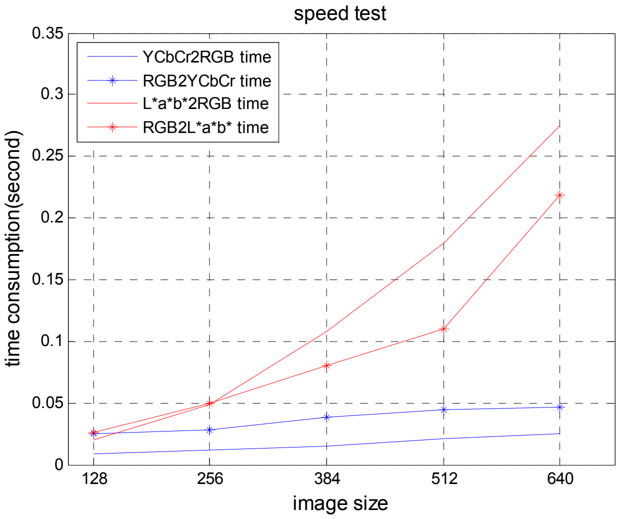

Fig. 10. Conversion speed from RGB to L*a*b* and conversion speed from RGB to YCbCr in several image resolutions: 128*128, 256*256, 384*384, 512*512, 640*640, 768*768, 896*896.

The results shows that the conversion speed from the RGB to YCbCr is approximately 10 times of the speed from RGB to L*a*b* space.

V. Conclusion and Discussion

In this paper, we use a selective encryption method in three channels of YCbCr space. In Y channel, we use 2D Arnold's cat map and 3D Lu Map. In Cb and Cr channels, we use 1D Logistic map and DNA encoding. Thus the encryption and decryption effect is safe, reliable and fast, which can be comparable with RGB and L*a*b*. The most prominent is that the speed is much faster than both RGB and L*a*b*.

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.

VI. Acknowledgements

This work is partially supported by the National Natural Science Foundation of China (Grant NO.61402021, 61402023), the Science and Technology Project of the State Archives Administrator (Grant NO.2015-B-10), the open funding project of State Key Laboratory of Virtual Reality Technology and Systems, Beihang University (Grant NO. BUAA-VR-16KF-09), and the Fundamental Research Funds for the Central Universities (NO. 2014GCYY02, 2014GCYY04, 2016LG03, 2016LG04).

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] 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)

[8] 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)

[9] 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)

[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] Xin Jin, Yingya Chen, Shiming Ge, Kejun Zhang, Xiaodong Li, et al. Color Image Encryption in CIE L*a*b* Space. The 6th International Conference on Applications and Techniques for Information Security (ATIS), Beijing, China, 4-6 November, pp.74-84, 2015