Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/110221

A Digital Image Carrier Preprocessing Scheme based on Energy and Structure Analysis for Information Hiding

ZHANG Tao[1,*], *REN Shuai*[2], *KANG Yuan*[1], *YANG Tao*[2] *and SUO Li*[2]

[1] School of Electronic and Control Engineering, Chang'an University, Xi'an 710064, China
[2] School of Information Engineering, Chang'an University, Xi'an 710064, China

Received: 20 Oct. 2016, Revised: 28 Jan. 2017, Accepted: 29 Jan. 2017
Published online: 1 Mar. 2017

Abstract: The reasonable preprocessing methods based on the characteristics of the carriers can improve the performance of hiding algorithm largely. Respectively related with robustness and invisibility, the energy and structure characteristics of the carriers should be necessarily analyzed before the data hiding. In this paper, the original carrier is filtered by the Gaussian pyramid (GP) to generate sub-images with different energy level, which can be selected as the embedding regions for the information with different robustness. And the Color Field Structure Analysis is used to process the sub-images after GP to obtain the specific space parameters which can be considered as the modified data for the secret information. And at the same time, some optimization theories like the Logistic chaotic map, Knight's Tour traversal and the genetic algorithms are used to improve the consistency between the original and stego carrier. At last, the experimental shows the achievements about robustness, invisibility and the ability against steganalysis of this scheme in the form of data.

Keywords: Information Hiding, Gaussian Pyramid, Color Field Structure Analysis, Logistic Chaotic Map, Genetic Algorithm.

1 Introduction

An important task in information hiding is to balance measures such as robustness, invisibility, capacity, and so on. These measures are closely linked with energy and structural characteristics of cover image. Most information hiding algorithms for digital images are based on spatial domain theories or frequency domain theories. Some algorithms often have advantages to satisfy one or a few requirements [1][2][3][4][5]. But the previous algorithms cannot satisfy most of these requirements at the same time [6][7][8]. This may be due to the fact that those algorithms leave energy and structural characteristics of the cover images out of consideration.

To deal with this problem, the recent research focuses on pretreatment methods based on energy and structure. Some algorithms based on multi-wavelet [9] decompose digital images into sub-images with different energy ratio, so the secret information can be embedded into different regions according to their robustness.

In this article, we put forward hiding generation principles based on energy and structure. By using Gaussian Pyramid theory, we generate ladder-like energy distribution regions to embed information according to invisibility, robustness, anti-analysis and sensitivity. According to color space multi-channel characteristics of digital image, CFSA is proposed based on mode and intensity as a cover image pretreatment method to represent the binary data by its direction. Our objective is to embed different information into regions with different energy ratio, such as follows: embed robust information into high energy region, fragile information into low energy region and the main information into medium energy region with high-capacity.

2 Gaussian Pyramid and CFSA

A Gaussian pyramid (GP) is an effective and simple structure with multi-resolution to explain images [10]. GP is of good visual effect and less computationally intensive. The Figure 1 shows the structure map of GP five layers and GP transformation to the Lena image. The original image G_0 is repeatedly operated to generate the sequence of reduced resolution image G_1,G_2,G_3,G_4.

* Corresponding author e-mail: zt904@foxmail.com

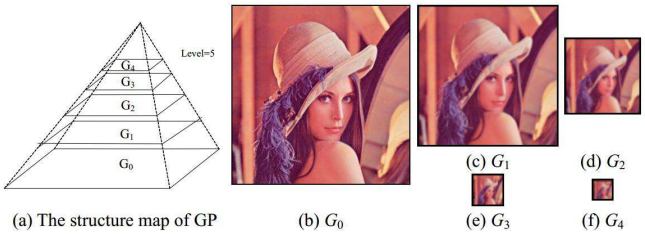


Fig. 1: Structure map of Gaussian Pyramid and Lena Gaussian Pyramid five layers.

Table 1: RTV comparison of filtering and noise.

Integration Factor		Relationship	Integration Rule	Matrix
Texture	Entropy	Direct	Weights $h \geq 1$	H
	Contrast	Direct	Weights $d \geq 1$	D
	Energy	Direct	Weights $e \geq 1$	E
	Uniformity	Inverse	Weights $r \leq 1$	R
Gradient		Direct	Weights $h \geq 1$	G

The CFSA use direction $[0, 2\pi]$ to express the color and structure information of digital image. It can map color intensity into the direction of space field structure according to color space multi-channel characteristics. CFSA can inherit the characteristics of color space properties. The greatest advantage of $l\alpha\beta$ color space is to eliminate the correlation between each color component of RGB. Compared with ordinary color information, $l\alpha\beta$ color space has advantages in the application of information hiding technology. In this paper, choose $l\alpha\beta$ space as input matrix of CFSA.

DEFINITION 1. Color Space Matrix is the row matrix which is made up of multi-channel color components of image, and the definition is shown in Eq.1 which chooses $l\alpha\beta$ Color Space:

$$C = [l, \alpha, \beta] \tag{1}$$

DEFINITION 2. Integration Module is a matrix set, and contains image structure weights which are closely related to the performance of information hiding. Integration Module is used to generate the Integration Matrix. Integration factors include texture and gradient information, and the integration rule of Integration Module in CFSA is proposed in Table 1.

DEFINITION 3 . Integration Matrix is the weight matrix which is generated by Integration Module according to the application requirements. Integration Matrix is denoted T, shown in Eq.2:

$$T = W \times Z^T \tag{2}$$

in which W is the weight matrix of Integration Factor and $W = [hderg]$, Z is Integration Factor Matrix and $Z = [HDERG]$.

Table 2: Embedding rules based on CFSA.

Stand For	Vector Direction
00	$[\lambda\pi/2^{k-1}, (1+4\lambda)\pi/2^{k+1})$
01	$[(1+4\lambda)\pi/2^{k+1}, (1+2\lambda)\pi/2^{k})$
10	$[(1+2\lambda)\pi/2^{k}, (3+4\lambda)\pi/2^{k+1})$
11	$[(3+4\lambda)\pi/2^{k+1}, (1+\lambda)\pi/2^{k-1})$

DEFINITION 4 . Informaion Matrix is a color information matrix based on structure. The elements composed of image pixel information. The position is the same as cover image matrix. The value of pixel (i, j) is denoted as a_{ij}. Computational formula is defined in Eq.3. Information Matrix is denoted as I.

$$a_{ij} = C_{ij}T \tag{3}$$

DEFINITION 5. Color Modeling is used to convert color information into Color Field Structure, and computational formula is defined in Eq.4.

$$M = I \bmod 2\pi \tag{4}$$

3 Information hiding algorithm

The direction value of CFSA represents the data information of cover image. Embed information by changing the direction. Table 2 lists the embedding rules, where $\lambda = (0, 1, \ldots, 2^k - 1), k = (0, 1, \ldots, +\infty) \in Z^*$

Change the direction according to the proximity principle. It can be seen from Table 2 that the maximum variation is $\pi/2^k$. Fig. 2 is the schematic diagram of embedding rules when k=2. For example, every black area is stands for 00.

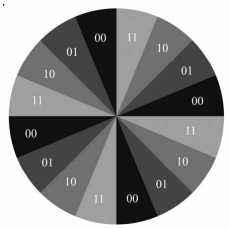


Fig. 2: Embedding Express.

Energy ratio of G_1, G_2, G_3, and G_4 of GP is approximately 8.1:4.2:2.4:1.6. Based on this feature, Fig. 3 shows embedded region strategy of GP-CFS: G_1 is robustness region, G_2 and G_3 are data embedded regions, and G_4 is a fragile sign region. The process of GP-CFS has nine steps:

Step1 . Transform the cover image with GP to obtain four sub-images;

Robust Information G_1	Embed Information G_2
Embed Information G_3	Fragile Sign G_4

Fig. 3: Embedding Region.

Step2 . Obtain the CFS of four sub-images separately based on Eq. (1)-(3) and express them as G'_1 ,G'_2 ,G'_3 and G'_4

Step3. Code G'_2 and G'_3 with row traversal method based on the rule listed on Table 1 and symbolize them separately as $G'_2 = t'_1, t'_2, \ldots, t'_k, t'_i$ and $G'_3 = t''_1, t''_2, \ldots, t''_k, t''$ Get the final coding of units G_2 and G_3 from G'_2 and G'_3, and represent them as $G = t'_1, t''_1, t'_2, t''_2, \ldots, t'_k, t''_k, t'_i, t''_i = t_1, t_2, ..., t_n$, $n = 2i$;

Step4. Use Logistic mapping of chaotic map algorithm to optimize information, as defined in Eq. (4). Suppose the parameter is μ and initial value is x_k The bit series after the logistic mapping is $G^x_{IN} = b^x_1, b^x_2, \ldots b^x_{n-1}, b^x_n$.

$$x_{k+1} = \mu x_k (1 - x_k), \; x_k \in (0,1) \tag{5}$$

Step5. In order to optimize the sequence of embedded bits with genetics algorithm, suppose F as the amount of the same bit value in matched positions between G^x_{IN} and C. Optimize x_k using genetic algorithm to maximize F. The optimization model based on GP-CFS is Eq. (5). Get the optimal solution y by genetic algorithms optimization. Put y into G^x_{IN} to obtain the optimal embedded bits $G^y_{IN} = b^y_1, b^y_2, \ldots b^y_{n-1}, b^y_n$;

$$F(y) = MaxF(x_k) = Max \sum (t_n \bar{\oplus} b^x_n) \tag{6}$$

Step6. Change the direction of CFSA based on the rules listed in Table 2. Embed G^y_{IN} into G_2 and G_3 with RAID4 row traversal. The basic data unit of RAID4 is composed by eight bits;

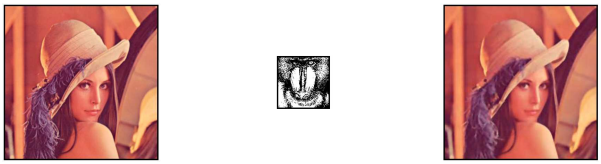
Step7. G_1 is the most robust region in four GP sub-images. In order to judge and recover the imperfect information, we embed the cyclic redundancy check (CRC) of RAID4 (recorded as R^L), the optimization scrambling parameters y and μ in G_1;

Step8. G_4 is the most vulnerable region in four GP sub-images. Embed the CRC of RAID4 (recorded as R^H) in G_4. Information receiver can judge quickly by comparing R^L and R^H when the stego image is attacked;

Step9. Restore the modified images into Stego images by GP inverse operation.

4 Simulation Experiment

Simulation environment is Matlab7.0.0.19920. Cover image is Lena (256×256) (Figure 4(a)). Secret image is binary image Baboon (64×64) (Figure 4(b)). Get the stego image shown in Figure 4(c) which is based on the GP-CFS when $k = 10$.



(a) Cover image (b) Hiding information (c) Stego image

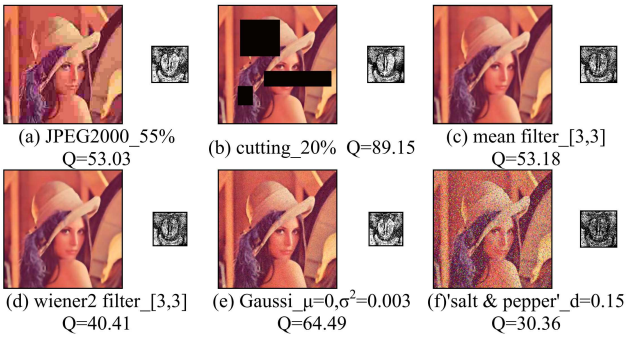
Fig. 4: Hiding and result of GP-CFS.

k determines density division of embedding area. The more density of area division, the smaller of the direction of CFSA changed, and the better invisibility performance of this scheme. However, the bigger of k is, the higher of computational cost is. Inspect and verify k in the 100 images randomly selected. It can be proved that when $8 \le k \le 17$, invisibility is fine under considering cost.

Robustness test algorithm is defined in Eq. (6). Q is robustness test value (RTV).

$$Q = \frac{\sum_{i=0}^{n-1}\sum_{j=0}^{n-1} f(i,j) \oplus f'(i,j)}{\sum_{i=0}^{n-1}\sum_{j=0}^{n-1} f(i,j) \oplus f(i+\mu, j \pm \eta)} \tag{7}$$

Operated object is stego image Figure 4 (c). Figure 5 shows the result of different attacks such as JPEG2000 compression, cutting, filtering and noise. Information extraction is the most preserved when Q=100.



(a) JPEG2000_55% Q=53.03 (b) cutting_20% Q=89.15 (c) mean filter_[3,3] Q=53.18

(d) wiener2 filter_[3,3] Q=40.41 (e) Gaussi_μ=0,σ²=0.003 Q=64.49 (f)'salt & pepper'_d=0.15 Q=30.36

Fig. 5: Results of robustness experiment.

According to experiment, embedded information can be identified when Q reach about 40. Figure 5 and Figure

Table 3: Detectable rate of attacks.

Attacks	JPEG2000	Cutting	Filtering	Gaussian	'salt pepper'
Detectable rate (%)	90.13	85.21	88.72	98.56	97.48

6 show that GP-CFS is robust against JPEG2000 compression below 64%, cutting below 41%, common filtering and adding noise.

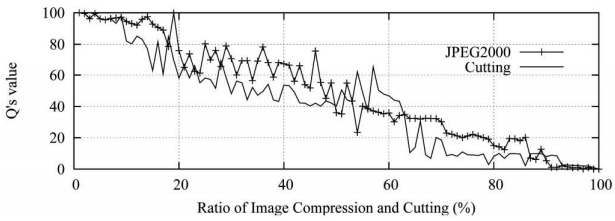
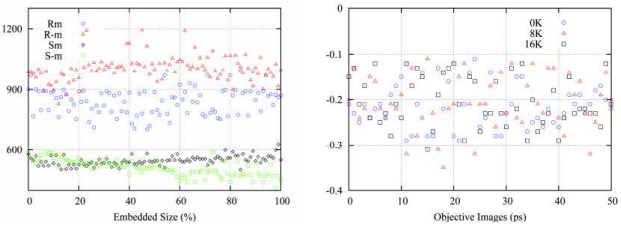


Fig. 6: Robust experiment of JPEG2000 and cutting (Q).

Sensitivity to image attacks is the peculiar characteristic in GP-CFS. Comparison between R^H and R^L indicates the algorithm has excellent sensitivity of image processing. Table 3 lists the detectable rate when JPEG2000 compression ratio is 5%, random cutting ratio is 5%, [3, 3] median filter,Gaussian (μ=0, $\sigma^2 = 0.003$) and $'salt\&pepper'(d = 0.15$). The average of detectable rate is 91.82%

RS can detect whether or not having hiding information by comparing the difference value between R_m and R_{-m} , S_m and S_{-m} . Higher order statistics detection algorithm based on wavelet coefficients (HOSWC) is a general detection algorithm. Use the algorithms above-mentioned to analyze the performance of GP-CFS. Experiment results are shown in Figure 7.



(a) Experiment result of *RS* (b) Experiment result of HOSWC

Fig. 7: Robust experiment results of GP-CFS (RS and HOSWC).

Figure 7 (a) shows that the maximum difference value of R is 332 (except initial difference value about 153). The maximum difference value of S is 155. It indicates that the embedding rate can not directly influence on

Table 4: Invisibility comparison based on PSNR.

Algorithm	GP-CFS	LSB	DCT	DWT	DWT&DCT	DWT&LSB
PSNR	36.4564	24.6581	26.5735	31.5894	30.8332	31.9827

Table 5: RTV comparison of filtering and noise.

Attacks	Information Hiding Algorithm		
	GP-CFS	DCT-LSB	DWT-LSB
[3,3] median filter / [3,3] wiener2 filter	56.28/42.41	50.98/40.40	53.99/42.07
Gaussi ($\mu = 0$,$\sigma^2 = 0.003$) / 'saltpepper' ($d = 0.15$)	60.11/24.81	61.89/20.81	57.94/22.65

difference value. Detect the 50 random pictures which hiding information based on HOSWC. Figure 7 (b) shows that there is no one or more threshold value found to recognize which pictures embedded information. Thus show that GP-CFS resists such analysis.

According to PSNR, GP-CFS has advantages in invisibility compared with the space domain methods such as LSB, frequency domain methods such as DCT and DWT and some developed algorithm. Table 4 shows that invisibility increases by 22.49% averagely when embedding rate is 25%.

Figure 8, Figure 9 and Table 5 show robustness comparison results when embedding rate is 25% based on RTV.

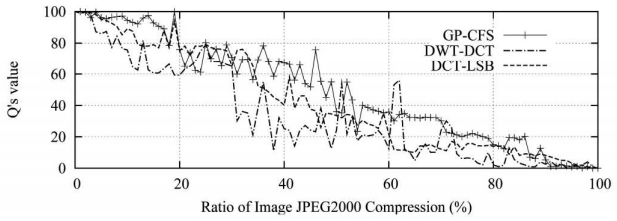


Fig. 8: Compression comparison.

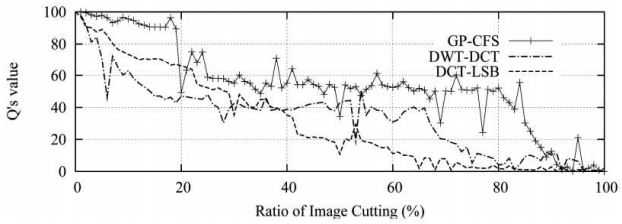
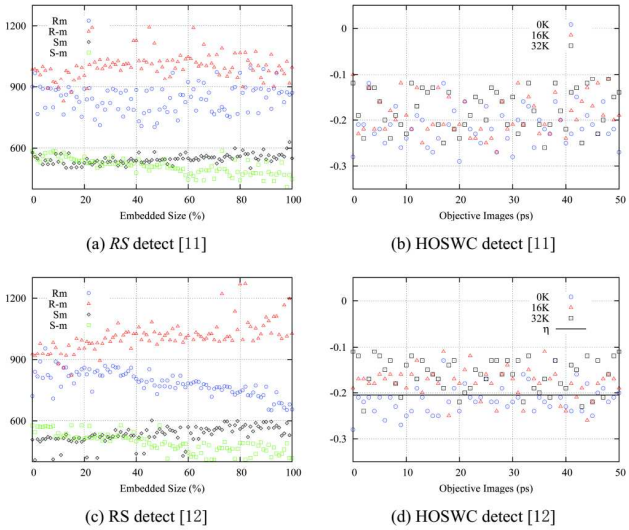


Fig. 9: Cutting comparison.

The results show that RTV of GP-CFS increase by 43.31%, 19.84%,5.13%, 2.85%, 44.80% and 24.76%

averagely compared with DCT-LSB and DWT-LSB under attacks such as JPEG2000 compression, random cutting, [3,3] median filter, [3,3] wiener2 filter, Gaussian and 'salt & pepper' noise.

Sensitivity is the peculiar characteristic in GP-CFS. The current algorithms don't have this feature. Use RS and HOSWC to detect [11] and [12]. Fig. 10 shows the experiment results.



(a) *RS* detect [11] (b) HOSWC detect [11]

(c) RS detect [12] (d) HOSWC detect [12]

Fig. 10: Comparison experiment.

In the case of [10], the experiment results in Figure 10 (b) indicate that it has certain immunity to HOSWC. But R_m has obvious two-branch when the embedding quantity increases in *RS*. In the case of [12], there is no obvious two-direction, but the tendency of two-branch can judge the existence of information in image. There is a threshold $\eta = -0.205$ based on the HOSWC when embedding quantity is 16K or 32K. The misstatement rate of [11] and [12] are 27% and 21% separately. The rate of missing report is 56% and 47% separately. Data mentioned above proves that the GP-CFS is of certain ability against steganalysis.

5 Conclusions

Use color space multi-channel characteristics of digital image to propose a Color Field Structure based on color mode and intensity. Based on the characteristics of the energy ratio of four Gaussian Pyramid sub-images is approximately 8.1:4.2:2.4:1.6, we put forward reversible Information Hiding scheme. In the scheme, we embed information by changing the direction of the vector. Simulation results show that due to the combination of GP and CFSA, and introduction of chaotic map, genetic algorithm and RAID4, this scheme satisfies basic technology indicators of information hiding and also meets the basic security demand of secret information transmission for communication system.

The future work is focus on information area of vector, choosing embedded module and robustness parameters in G_1 in order to improve invisibility, robustness, sensitivity to image attacks and ability against steganalysis. Especially, we will research on applications in information hiding based on the theory of Image Multi-scale Geometric Analysis.

Acknowledgments

Our research was funded by several Projects, and the names and numbers of these Projects are as follows: National Natural Science Foundation of China (Grant No. 61402052). National Natural Science Foundation of Tibet (Grant No. 2015ZR-14-20). Natural Science Basic Research Plan in Shaanxi Province of China (Program No. 2014JM2-6105). China Postdoctoral Science Foundation (Grant No. 2015M572510). Shaanxi Province Postdoctoral Science Foundation. The Special Fund for Basic Scientific Research of Central Colleges of Chang'an University (Grant No. 310832151092). National college students' innovative entrepreneurial training fundedation (Grant No. 201510710044)

References

[1] X. Sun, P. Meng, L. Huang, Simple and practical information hiding algorithm for chinese text, Computer Engineering & Applications. **49** (2013), pp.88-91.

[2] J. Q. Xie, Q. Xie, D. Z. Huang, Image information hiding algorithm with high security based on run-length, Computer Science. **41** (2014), pp.172-175.

[3] L. Zhang, J. Wang, Information hiding based on morphological component, Lecture Notes in Electrical Engineering. **287** (2014), pp.491-499.

[4] Z. Wang, X. Zhao, H. Wang, G. Cui, Information hiding based on DNA steganography, Software Engineering and Service Science (ICSESS), 2013 4th IEEE International Conference on IEEE. (2013), pp.946-949.

[5] A. Srinivasan, S. Kolli, J. Wu, Steganographic information hiding that exploits a novel file system vulnerability, International Journal of Security and Networks. **8** (2) (2013), pp.82-93.

[6] J. Yang, X. Lu, H.Zhang, C. Li, Research on network text information hiding technology, Microcomputer & Its Applications. **32** (2013), pp.10-12.

[7] X. Y. Li, L. X. Deng, R. Xu, X. M. Li, An audio information hiding scheme with high capacity based on compressed sensing and psychoacoustic model, Image and Signal Processing (CISP), 2014 7th International Congress on IEEE. (2014), pp.1095-1099.

[8] Z. Huang, W. Kou, K. Chen, Secure and Oblivious Information Hiding in Binary Image, 2013 IEEE 16th International Conference on Computational Science and Engineering (CSE). IEEE Computer Society. (2013), pp. 235-239.
[9] X. G. Xia, J. S. Geronimo, D. P. Hardin, B. W. Suter, Design of prefilters for discrete multiwavelet transforms, Signal Processing IEEE Transactions on. **44** (1996), pp.25-35.
[10] M. Suarez, V. M. Brea, D. Cabello, J. Fernandez-Berni, R. Carmona-Galan, A. Rodriguez-Vazquez, A 176×120 pixel CMOS vision chip for Gaussian filtering with massivelly Parallel CDS and A/D-conversion, Circuit Theory and Design (ECCTD), 2013 European Conference on IEEE. (2013), pp.1-4.
[11] S. Alam, S.M. Zakariya, M.Q. Rafiq, Analysis of Modified LSB Approaches of Hiding Information in Digital Images, Computational Intelligence and Communication Networks (CICN), 2013 5th International Conference on. IEEE. (2013), pp.280-285.
[12] P. F. Liu, B. Z. Liang, C. Peng, A Dwt-Dct Based Blind Watermarking Algorithm For Copyright Protection, Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on. (2010), pp.455-458.

ZHANG Tao obtained her PhD from Northwestern Polytechnical University of China in 2012. She is a lecture in School of Electronic and Control Engineering in Changan University. She has been engaged in Information hiding and Network security for 8 years. She published 20 scientific research articles in international publications and 1 are cited by SCI, 6 are cited by EI. She has carried out 4 tasks to study a plan in all, won patent 1.

REN Shuai obtained his PhD from Northwestern Polytechnical University of China in 2009. He is a lecture in School of Information Engineering in Chang'an University. He has been engaged in Information hiding and Network security for 7 years. He published 23 scientific research articles in international publications and 4 are cited by SCI, 8 are cited by EI. He has carried out 5 tasks to study a plan in all, won patent 2. During the last yearhe has written or co-edited for 5 textbooks.

KANG Yuan was born in 1991, presently in Chang'an university information engineering college, Majored in pattern recognition and intelligent system. Her research direction is information hiding.

YANG Tao was born in 1992, presently in Chang'an university information engineering college, Majored in Intelligent transportation and information system engineering. Her research direction is information hiding.

SUO Li was born in January 1990, presently in Chang'an university information engineering college, Majored in Computer Software and Theory. Her research direction is information hiding.