

Image Steganography in a Karhunen-Loeve Transform Optimization Model

Li-Yangbo¹ and Guo-Zuhua¹

¹. *Department of Computer Science and Technology, Henan Institute of Technology, Henan, China*
qianmorenjia2015@sina.com

Abstract

In allusion to such problems as large perceptual distortion and high error rate caused by high image compression ratio in existing steganography technology in the information security field, an image Steganography based on Karhunen-Loeve transform optimization is proposed in this paper. Specifically, the iterative clustering algorithm is adopted for this method to solve the covariance matrix and the clustering mean value, and relevant values are adjusted for image segmentation; then, KLT algorithm is introduced to compress the image data and the least significant bit is adopted to replace the ciphertext data for data hiding. During information extraction, the reverse linear transformation operation and the original pixel matrix are adopted to obtain the effective hidden image information. The experiment result shows: compared with common algorithms, the proposed method has improved capacity and PSNR, and the image data extracted thereby has small distortion.

Keywords: *Information security; Steganography; KLT; Least significant bit; Capacity*

1. Introduction

Along with the rapid progress of the communication network technology promoted by the unremitting efforts of many scholars in recent years, relevant technologies are also rapidly developed, such as file transfer technology [1]. However, due to the application of communication medium for confidential information transmission, such unlawful act as bugging behaviors frequently appears. Actually, information can be easily attacked under general conditions, thus providing convenience to the unlawful personnel for information interception. Specifically, the unlawful personnel usually take the measure of increasing redundant data for information interception, and the information leakage can bring immeasurable losses to the users. In allusion to the above problem, several experts in China have carried out relevant deep researches. For example, after a series of researches, Chen Jiayong, *et al.* [6] have proposed the high-performance $\pm k$ self-adaption image steganography and the texture isotonic function, wherein the technology covers current existing methods and the function is based on freedom degree to make self-adaption steganography information have significant improvement in the aspects of synchronicity and rapidity; meanwhile, multilayer embedding and wet-paper coding thoughts are integrated therein, and relevant experiment has proven that this algorithm can ensure the modification unavailability of the sensitive area of the vector, thus to significantly improve the information security. After a series of researches, Zhang Jun and other experts [7] have established the rich domain model and verified that rich domain model and digital evidence acquisition process can provide better solution thoughts to steganalysis, wherein the rich domain model aims at integrating different characteristics of various domains and accordingly adopting the integrated classifier to distinguish the

ciphertext image and vector, and the digital evidence acquisition process aims at adopting the digital evidence acquisition method to identify the image type and then adopting the steganographic analyzer to detect the image so as to avoid the occurrence of image source mismatching phenomena, thus to improve detection performance and verify the good effectiveness of the algorithm. Zhang Min Qing[8] and other relevant experts have introduced feature fusion in their research to explain the steganalysis based on mutual information and feature fusion; in this way, the covert communication goal can be achieved under the condition of comprehensively keeping the sensing performance of the vector, and the experiment has proven the strong performance of this algorithm.

2. Execution Process of Steganography Algorithm

2.1. Substitution of Ciphertext Information by Image Pixel Value

The hidden secret information is a RGB pixel matrix with the size of $m \times n$, wherein m and n respectively represent height and width. Image A [10] is described by the following formula:

$$A = \begin{bmatrix} P_{1,1} & P_{1,2} & \cdots & P_{1,n} \\ \vdots & \vdots & & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ P_{m,1} & P_{m,2} & \cdots & P_{m,n} \end{bmatrix} \quad (1)$$

In order to improve the processing efficiency, the image pixels are respectively divided into R, G and B components. Therefore, image A includes $3m \times n$ elements and is specifically expressed by the following formula:

$$A' = \begin{bmatrix} R_{1,1} & R_{1,2} & \cdots & R_{1,n} \\ G_{1,1} & G_{1,2} & \cdots & G_{1,n} \\ B_{1,1} & B_{1,2} & \cdots & B_{1,n} \\ \vdots & \vdots & \ddots & \vdots \\ R_{m,1} & R_{m,2} & \cdots & R_{m,n} \\ G_{m,1} & G_{m,2} & \cdots & G_{m,n} \\ B_{m,1} & B_{m,2} & \cdots & B_{m,n} \end{bmatrix} \quad (2)$$

2.2. Image Segmentation Technology

Image segmentation aims at separating the foreground and the background through corresponding technology, wherein the pixels in various areas are corresponding to some features, such as texture and color. The maximum likelihood classification method is most widely applied for image segmentation. Specifically, the iterative clustering algorithm is firstly adopted to solve the covariance matrix and the clustering mean value, and then relevant values are adjusted.

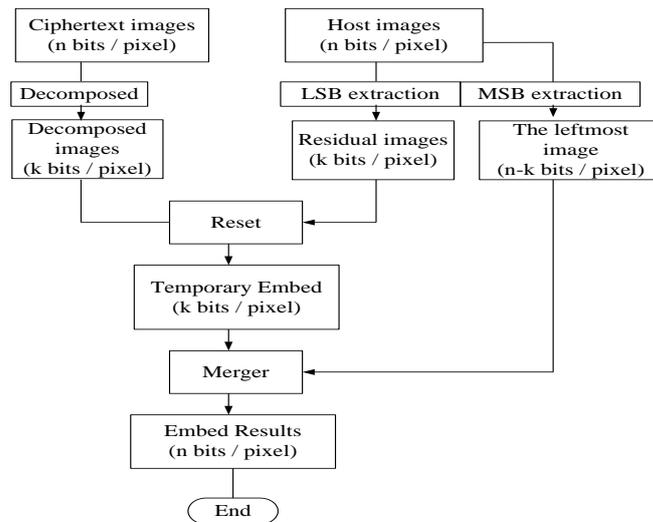


Figure 1. Simple Flow Diagram of LSB Substitution Method in Embedding Process

2.3. KLT application

KLT can be adopted to compress the image matrix so as to improve the hiding capacity of the image. Meanwhile, the image is divided into s segments, and the first segment mentioned above is corresponding to matrix A^* .

$$A^* = \begin{bmatrix} x_{1,1} & x_{1,2} & x_{1,3} & \cdots & x_{1,n-1} & x_{1,n} \\ x_{2,1} & x_{2,2} & x_{2,3} & \cdots & x_{2,n-1} & x_{2,n} \\ x_{3,1} & x_{3,2} & x_{3,3} & \cdots & x_{3,n-1} & x_{3,n} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ x_{3s-2,1} & x_{3s-2,2} & x_{3s-2,3} & \cdots & x_{3s-2,n-1} & x_{3s-2,n} \\ x_{3s-1,1} & x_{3s-1,2} & x_{3s-1,3} & \cdots & x_{3s-1,n-1} & x_{3s-1,n} \\ x_{3s,1} & x_{3s,2} & x_{3s,3} & \cdots & x_{3s,n-1} & x_{3s,n} \end{bmatrix} \quad (3)$$

Therein, $x_{3i-2,j} = R_{i,j}$, $x_{3i-1,j} = G_{i,j}$ and $x_{3i,j} = B_{i,j}$ ($i \in \overline{1,s}$, $j \in \overline{1,n}$).

Covariance of eigenvalue and eigenvector is solved in subsequent operation process, and then the information of the distribution eigenvector of matrix A^* is expressed by eigenvalue. Meanwhile, Jacobian matrix eigenvalue algorithm is introduced in this paper. Various eigenvalues are in direct proportion to each other and the eigenvector thereof is taken as the storage capacity, and this matrix is as the same as Formula (6). Additionally, the eigenvector can form $(3s) \times (3s)$ orthogonal matrix $V = [v_1 \ v_2 \ \dots \ v_{3s}]$, and the main attributes thereof are as follows:

$$V \cdot V^T = V^T \cdot V = I_{3s} \quad (4)$$

In formula (4), V represents the orthogonal matrix; V^T represents the transposed matrix; I_{3s} represents unit matrix including $3s$ elements.

2.4. Data Hiding

A^* has n (n is an integer number) elements, so it can contain single byte. The pixel values at the block edge may not be influenced, but the number of the elements of the projection matrix will be changed, so the storage capacity thereof

shall be at least 4 bytes. In practice, byte compression ratio is $\frac{4k}{3s}$, and in order to meet relevant compression ratio requirement, P_j used for linear transformation shall meet the following conditions [9-10]:

$$P'_{j,i,j} = (P_{j,i,j} - \min P_j) / (\max P_j - \min P_j) \cdot 255 \quad (5)$$

In Formula (5), P_j represents the j th pixel; $P'_{j,i,j}$ represents the transformed pixel.

Similarly, V^* shall be also provided with at least 4 bytes as the storage capacity, as shown in the following formula:

$$V^{*'}_{i,j} = V^*_{i,j} \cdot 32767 \quad (6)$$

Afterwards, the information can be hidden through LSB substitution method, wherein the hidden data capacity of an image is mainly determined by the hidden bits, namely: how to obtain the versions of the three algorithms from the hidden information through these bits --- I, II and III bits, wherein the bit at higher order can hide more information and can also hide vector error.

2.5. Information Extraction

The extraction of the hidden information is started at the least significant bit of the steganography image, wherein the eigenvector matrix and the linearly processed projection obtained by each segment can be adopted to calculate the size of the segment concerned. Reverse linear transformation operation [12] is adopted for the information extraction process. The specific process is as follows:

$$aP_{j,i,j} = \frac{P'_{j,i,j} \cdot (\max P_j - \min P_j)}{255 + \min P_j} \quad (7)$$

$$aV^*_{i,j} = \frac{V^{*'}_{i,j}}{32767} \quad (8)$$

In Formulae (7) and (8), a as the approximate value of the initial matrix represents reduced eigenvector matrix and projection matrix; relevant matrixes can be recombined to obtain the approximate value of matrix A^* , specifically as shown in the following formula:

$$aA^* = aV^* \cdot aP_j \quad (9)$$

Approximate RHS:

$$aV^* \cdot aP_j \cong V^* P_j \quad (10)$$

Formula (10) is combined to obtain the following formulae:

$$V^* \cdot P_j = V^* \cdot (V^*)^T \cdot A^* \quad (11)$$

$$V^* \cdot (V^*)^T \cdot A^* \cong I_{3s} \cdot A^* = A^* \quad (12)$$

3. Experiment Result

The configuration of the experiment for verifying the effectiveness of the steganography algorithm is as follows: Intel®Core i5, dominant frequency 3.5GHz, dual core, memory 4GB, operating system Windows XP. Three sets of vector and information images are introduced for this algorithm, and LSB values of the three sets are different from each other.

Pixel errors of the vector image and the information image before and after recovery are compared in the experiment, and the larger error indicates the poorer algorithm performance. In the experiment, the relation among compression ratio,

compression times and split size is researched in order to analyze the algorithm performance. The specific value of the size of the compressed image file and the size of the original image file is called as the compression ratio. If the compression ratio is smaller, then the algorithm performance is better, namely: if the image split size is larger and the image is more compressed, then the corresponding compression ratio is smaller and the algorithm performance is better. The evaluation standard PSNR (unit: dB) adopted in this paper refers to $(2^n-1)^2$ logarithm of the mean square error between the original image and the processed image, wherein $(2^n-1)^2$ is the square of the maximum signal value and n refers to bits of each sampling value. The image module data bit embedded at the transmitting terminal refers to the embedding capacity.

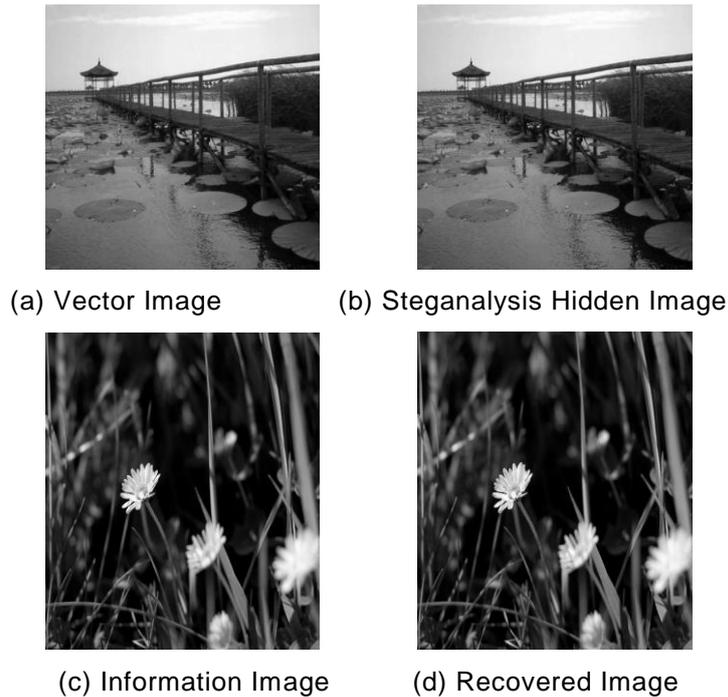


Figure 2. The First Set of Images

The first set of images is the experiment materials employing one bit of LSB, and the minimum vector error is 0.35583, and the specific experiment result is as shown in Figure 2. According to the figure, we can know that the hidden image and the recovered image both have good effect, wherein the information error is 1.02531; the hiding time and the recovery time are respectively 2.30927s and 1.21945s.

The second set of images is the experiment materials employing two bits of LSB, and the specific experiment result is as shown in Figure 3. The vector error is 0.581927 which is 0.5 times of the previous vector error; the effect of the recovered image is poorer than that of the previous recovered image, the recovery time is relatively long and the information error is 2.48456. Additionally, the hiding time and the recovery time are respectively 3.20534s and 1.436968s.

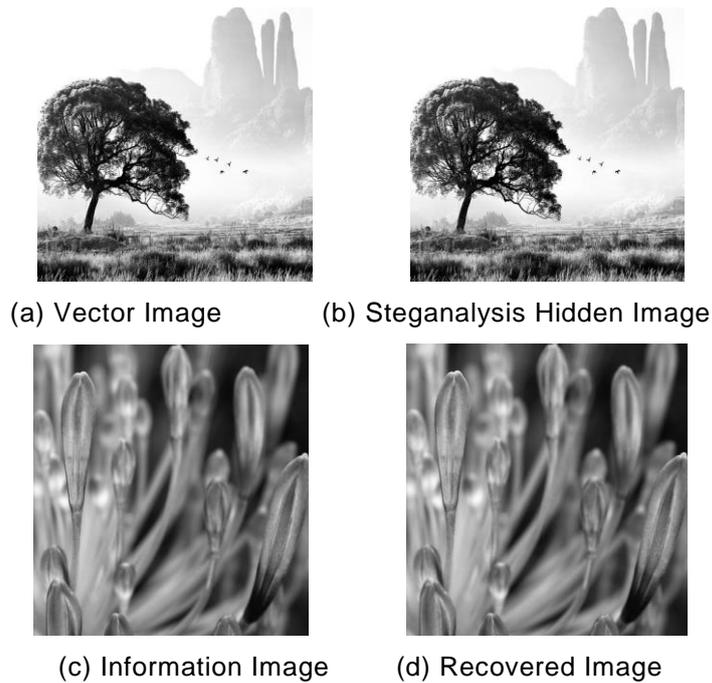


Figure 3. The Second Set of Images

The third set of images is the experiment materials employing four bits of LSB, and the specific experiment result is as shown in Figure 4. According to the figure, we can know that the vector error is 1.829591 which is the maximum value among the three vectors errors, and the third set has the poorest hiding effect; the corresponding information error is 1.54972; the hiding time and the recovery time are significantly increased as 6.89284s and 2.83218s.

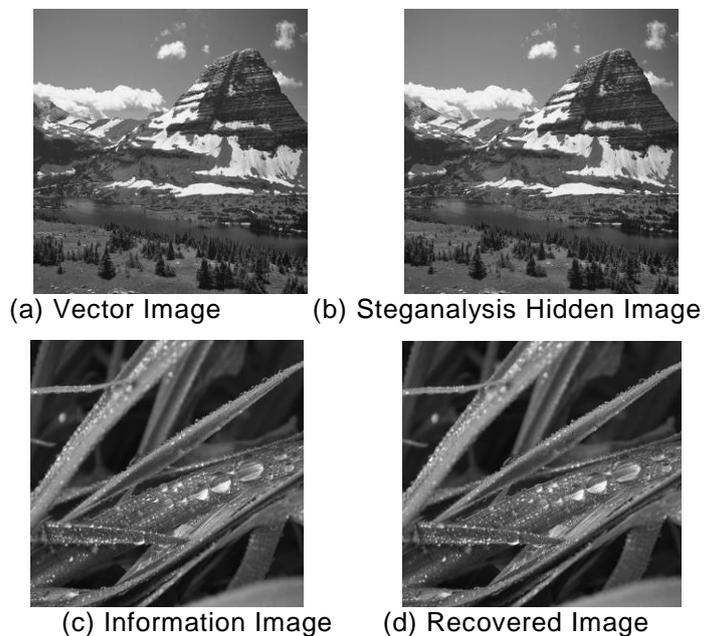


Figure 4. The Third Set of Images

In order to effectively compare the performances of the above images, three parameters- compression ratio, information error and vector error are introduced in

this paper to describe this algorithm. According to Figure 5, we can find that the first set has maximum compression ratio and minimum errors.

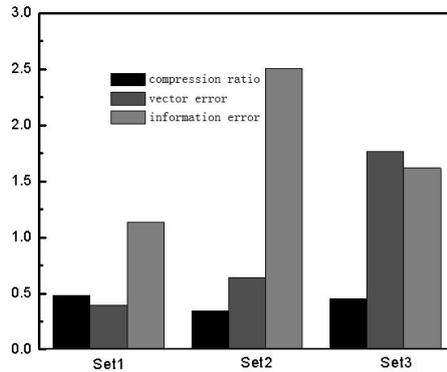


Figure 5. The Graphical Representation of the Three Sets of Parameters

According to Figure 6, we can find the relationship between the compression ratio and the split size, namely: the compression ratio is mainly determined by the split size. If the split size is larger, then the compression ratio is smaller; namely: if the split size is smaller, then the compression ratio is poorer, thus indicating that the compressed information is not suitable for the vector image.

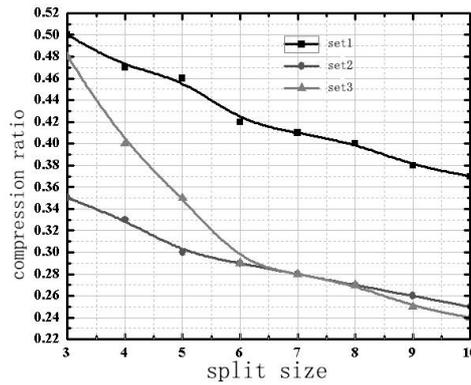


Figure 6. The Relationship between Split Size and Compression Ratio of the Three Photos

According to Figure 7, we can find the directly proportional relationship between the compression times and the split size.

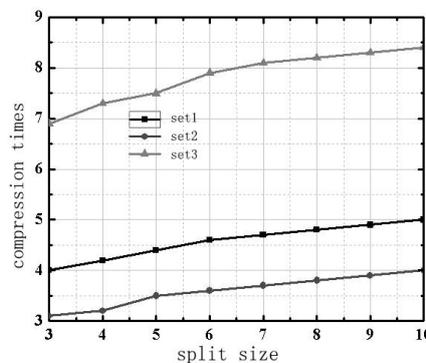


Figure 7. The Relationship between Split Size and Compression Times of the Three Photos

In order to comprehensively verify the algorithm effect, the following control group is set this paper: the technology proposed in literature [13] is adopted to calculate the materials in literature [6]. The vector image verification is specifically as shown in Figures 2(a), 3(a) and 4(a). The experiment results are as shown in Table 1. According to Table 1, we can find that the average embedding capacity of the experiment group is higher than that of the control group, and the average embedding capacities of the two groups are respectively 792.54bit and 576.70bit. Meanwhile, PSNR of the steganography of the experiment group is 0.34dB lower than that of the control group. Therefore, the proposed algorithm has better image recovery quality.

Table 1. PSNR and Embedding Capacity Results of Different Mechanisms

| Vector Image | The Algorithm | | Literature[6] | |
|--------------|---------------|----------|---------------|----------|
| | Capacity/bit | PSNR /dB | Capacity/bit | PSNR /dB |
| Fig.2(a) | 812.62 | 39.78 | 603.25 | 39.52 |
| Fig.3(a) | 795.95 | 38.21 | 581.37 | 37.46 |
| Fig.4(a) | 769.05 | 35.17 | 545.48 | 35.16 |
| Means | 792.54 | 37.72 | 576.7 | 37.38 |

Additionally, in allusion to Figures 2(a), 3(a) and 4(a), the algorithms proposed in literatures [14-15] are also adopted in the experiment and the corresponding parameters thereof are compared with PSNR and embedding capacity of the recovered image of the proposed algorithm. Obviously, the proposed algorithm is still superior to the algorithms proposed in literatures [14-15], with the embedding capacity improvement respectively as 50.14bit and 230.22bit and with PSNR improvement respectively as 1.63dB and 5.84dB. The specific comparison results are as shown in Table 2.

Table 2. PSNR and Embedding Capacity Results of the Proposed Algorithm and the Algorithms in Literature [14-15]

| Vector Image | The Algorithm | | Literature[14] | | Literature[15] | |
|--------------|---------------|----------|----------------|----------|----------------|----------|
| | Capacity/bit | PSNR /dB | Capacity/bit | PSNR /dB | Capacity/bit | PSNR /dB |
| Fig.2(a) | 812.62 | 39.78 | 762.48 | 38.05 | 582.4 | 31.96 |
| Fig.3(a) | 795.95 | 38.21 | 745.81 | 37.93 | 565.73 | 31.82 |
| Fig.4(a) | 769.05 | 35.17 | 718.91 | 34.99 | 538.83 | 31.86 |
| Means | 792.54 | 37.72 | 742.4 | 36.99 | 562.32 | 31.88 |

4. Conclusion

In conclusion, KLT is adopted for data compression in this paper, and the LSB thereof is adopted for the substitution of the ciphertext data so as to realize data coding, thus to establish the corresponding relationship between the coded data and the pixel matrix. According to relevant experiment, we can find that the proposed algorithm has high efficiency, high mean PSNR and capacity and can decode original data.

Acknowledgement

The research is supported by Higher school teaching project of henan province-- The teaching team(2012[1099])

References

- [1] Y Geng, J Chen, R Fu, G Bao and K Pahlavan, "Enlighten wearable physiological monitoring systems: On-body rf characteristics based human motion classification using a support vector machine", *IEEE transactions on mobile computing*, vol.1, no.1, (2015), pp. 1-15.
- [2] J He, Y Geng, F Liu, C Xu and CC-KF, "Enhanced TOA Performance in Multipath and NLOS Indoor Extreme Environment", *IEEE Sensor Journal*, vol. 14, no.11, (2014), pp. 3766-3774.
- [3] S Zhou, L Mi, H Chen and Y Geng, "Building detection in Digital surface model", 2013 IEEE International Conference on Imaging Systems and Techniques (IST), (2012).
- [4] J He, Y Geng and K Pahlavan, "Toward Accurate Human Tracking: Modeling Time-of-Arrival for Wireless Wearable Sensors in Multipath Environment", *IEEE Sensor Journal*, vol. 14, no.11, (2014), pp. 3996-4006.
- [5] N Lu, C Lu, Z Yang and Y Geng, "Modeling Framework for Mining Lifecycle Management", *Journal of Networks*, vol. 9, no.3, (2014), pp. 719-725.
- [6] Y Geng and K Pahlavan, "On the accuracy of rf and image processing based hybrid localization for wireless capsule endoscopy", *IEEE Wireless Communications and Networking Conference (WCNC)*, (2015).
- [7] G Liu, Y Geng and K Pahlavan, "Effects of calibration RFID tags on performance of inertial navigation in indoor environment", 2015 International Conference on Computing, Networking and Communications (ICNC), (2015).
- [8] J He, Y Geng, Y Wan, S Li and K Pahlavan, "A cyber physical test-bed for virtualization of RF access environment for body sensor network", *IEEE Sensor Journal*, vol. 13, no.10, (2013), pp. 3826-3836.
- [9] W Huang and Y Geng, "Identification Method of Attack Path Based on Immune Intrusion Detection", *Journal of Networks*, vol.9, no. 4, (2014), pp. 964-971.
- [10] G Bao, L Mi, Y Geng, M Zhou and K Pahlavan, "A video-based speed estimation technique for localizing the wireless capsule endoscope inside gastrointestinal tract", 2014 36th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), (2014).
- [11] D Zeng and Y Geng, "Content distribution mechanism in mobile P2P network", *Journal of Networks*, vol. 9, no.5, (2014), pp. 1229-1236.
- [12] M Zhou, G Bao, Y Geng, B Alkandari and X Li, "Polyp detection and radius measurement in small intestine using video capsule endoscopy", 2014 7th International Conference on Biomedical Engineering and Informatics (BMEI), (2014).
- [13] G Yan, Y Lv, Qiyin Wang and Y Geng, "Routing algorithm based on delay rate in wireless cognitive radio network", *Journal of Networks*, vol. 9, no. 4, (2014), pp. 948-955.
- [14] G Bao, L Mi, Y Geng, K Pahlavan, "A computer vision based speed estimation technique for localizing the wireless capsule endoscope inside small intestine", 36th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), (2014).
- [15] Y Lin, J Yang, Z Lv, W Wei and H Song, "A Self-Assessment Stereo Capture Model Applicable to the Internet of Things. *Sensors*, (2015).
- [16] W Ou, Z Lv and Z Xie, "Spatially Regularized Latent topic Model for Simultaneous object discovery and segmentation", *The 2015 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, (2015).
- [17] W, Ke, "Using Simulation to Explore Distributed Key-Value Stores for Exascale System Services", 2nd Greater Chicago Area System Research Workshop (GCASR), (2013).
- [18] Y Wang, Y Su and G Agrawal. "A Novel Approach for Approximate Aggregations over Arrays", In *Proceedings of the 27th international conference on scientific and statistical database management*, ACM, (2015).
- [19] Z Lv, A Halawani, S Feng, S ur Rehman and H Li, "Touch-less Interactive Augmented Reality Game on Vision Based Wearable Device. *Personal and Ubiquitous Computing*, (2015).
- [20] J Yang, S He, Y Lin and Z Lv, "Multimedia cloud transmission and storage system based on internet of things", *Multimedia Tools and Applications*, (2016).

Authors



Li Yangbo. Li Yangbo received her M.S. degree in computer technique from Wuhan University of Technology in Wuhan, China. HE is currently a lecturer in Henan Mechanical and Electrical Engineering College. Her research interest is mainly in the area of Computer application, Digital media technology. He has published several research papers in scholarly journals in the above research areas and has participated in several books.