Reversible Watermarking Algorithm of Grid Map Based on Prediction-Error Histogram

Yanqun Zhang
School of Computer Science and Technology, China University of Mining and Technology, Xuzhou, China
zhyq@cumt.edu.cn

Yu Bao
School of Computer Science and Technology, China University of Mining and Technology, Xuzhou, China
baoyu@cumt.edu.cn

Qianping Wang
School of Computer Science and Technology, China University of Mining and Technology, Xuzhou, China
qpwang@cumt.edu.cn

Hui Xu
School of Computer Science and Technology, China University of Mining and Technology, Xuzhou, China
xuhui@cumt.edu.cn

***Abstract*—Reversible watermark is a kind of fragile watermark, and any changes will lead to the change or loss of watermarking information. The modified sensitivity of reversible watermark can be used for the integrity verification of grid map. When the content of carrier data is suspected, the type of manipulation or attack suffered can be judged through extracting the watermarking situation. The reversible watermarking algorithm proposed by this paper aims at the characteristics of grid map, to reduce the impact of low correlation of adjacent pixels, and the pixel values are distributed more intensively after the disposal of prediction-error histogram, thus to increase the embedded capacity. Under the premise of assurance of embedding capacity, there are 3 kinds of changes of pixel values, i.e. -1, 0 and 1, the change of source image is almost invisible, and watermark capacity can be repeatedly embedded. The algorithm simplifies the embedded process, and increases the embedding capacity, so that the complete-undamaged recovery of original image can be achieved.**

***Index Terms*—Reversible watermark, integrity verification, Prediction-Error Histogram**

I. Introduction

At present, digital map used for GIS can be divided into two categories according to data structure: vector structure and grid structure, and the corresponding map data is called “Vector Map” and “Grid Map”[1]. In comparison to vector map, grid map has a wide scope of application. It is one of data types most widely applied in GIS, and is also one of bases for generation of vector map and other type data. It has simple data structure, which can be easily converted, simulated and used for image processing, in favor of analysis of remote sensing data and its matching application with [2]. This paper proposes a space reversible watermarking algorithm to embed watermarking information into grid map. The algorithm introduces a method to modify prediction-error histogram, in which the embedding capacity can be further enlarged; in the meantime, there is less overflow of pixel value, which is appropriate for grid map.

The embedded process is shown in Fig. 1: first of all, according to the entropy and variance, sub-block in grid map is selected for operation with the gentle change of pixel value, good hidden effect and suitable size; each line of pixel value in the sub-block is predicted, to achieve the prediction-error diagram, the peak point in the histogram is more concentrated than that in image histogram; two maximum peak points are chosen in the prediction-error histogram to embed watermarking information; finally, grid map including watermark is reconstructed and recovered.

doi:10.4304/jsw.8.5.1117-1123

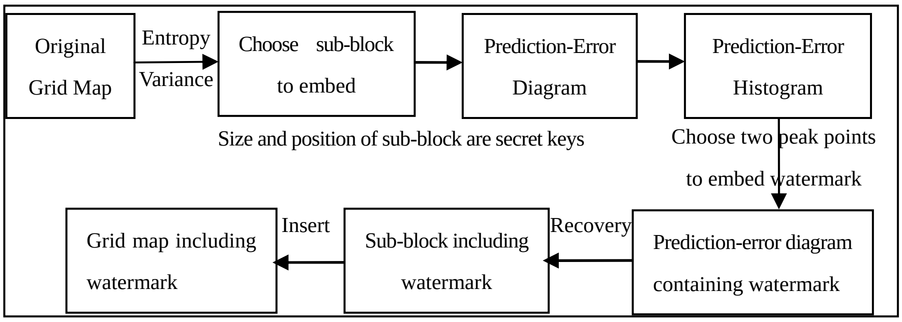

Figure 1. Process of Reversible Watermarking Embedding

II. GENERATING GRID MAP AND PREDICTION-ERROR HISTOGRAM

At first, in the algorithm 8-bit grid gray-scale maps carry out the blocking processing, and calculate the entropy of block image, to select the region with relatively gentle change, hereby the block with larger entropy and smaller variance is selected for watermark embedding. The size and location of block are served as secret key of watermark for saving and transferring. Supposed the size of sub-block in the selected grid map is *r*c*, and *I* is used to express the pixel in the block gray-scale map *I*. According to the sequence from top to bottom and from left to right, conduct the prediction operation of the first *c-1* pixel.

For the pixel value prediction of each pixel, $\tilde{s}_{i,j}$ indicates pixel prediction of the subscript of *i* and *j*: the pixel prediction is expressed by the subsequent pixel value of $S_{i,j+1}$, thus every pixel (except for the last pixel of every line) forms a prediction-error, expressed as:

$$\tilde{s}_{i,j} = s_{i,j+1} \quad 1<=i<=r,\ 1<=j<=c \tag{1}$$

$$P_{e,i} = s_{i,j} - \tilde{s}_{i,j} \tag{2}$$

After processing pixel prediction-error of each line, a prediction-error matrix *D* with a size of *r*(c-1)* is formed, and then the prediction-error matrix histogram *T* is calculated. Two pixel values at the maximum peak point, i.e. t_1 and t_2 are determined, and their relationship is $t_1 > t_2$.

III. WATERMARKING INFORMATION GENERATION

The watermarking information in grid map can be any symbol sequence, image production date, image shooting longitude and latitude, etc. Reversible digital watermarking information *W* is comprised by three parts: digital watermark *M* to be embedded; 128-bit information *P* generated by the original carrier by means of the MD5 algorithm for self-authentication; the content *Y* of data overflow processing. This paper selects as 256 * 256 binary image as watermark image shown in Fig. 2.

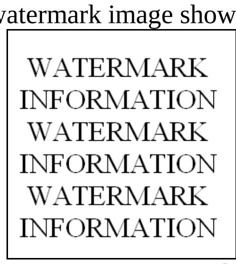

Figure 2. Binary Watermark Image

IV WATERMARKING INFORMATION EMBEDDING

A. Watermarking Information Embedding

The pixel value in the prediction-error histogram T is greater than the pixel point of t_1, its pixel value $T_{(i,j)}$ (1<=i<=r, 1 <=j<=c-1) conducts the operation of $T_{(i,j)}+1$. If the pixel value is less than a pixel point of t_2, the pixel value $T_{(i,j)}$ is changed into $T_{(i,j)}-1$. What is reflected in the histogram is that the pixel value is greater than the pixel of t_1, and its corresponding pixel value moves backward a bit. If pixel values of other pixels meet the condition of $t_2 <= T_{(i,j)} <= t_1$, and the corresponding pixels in the histogram remain unchanged. After the completion of the above operations, we can get the modified differential matrix *D'*, thus in the *D'*, the pixel value of t_1+1 and the pixel value of t_2-1 are zero.

When pixel value is equal to pixel points of t_1 and t_2 in the *D'*, watermark embedding is executed use(3), to achieve *D"*: each pixel is reconstructed use (4). The reconstruction does not include the last row of pixels of source image, after reconstruction, source image I', which includes watermark information, is formed.

$$T''_{i,j} = \begin{cases} T'_{i,j} + m & T_{i,j} = t_1 \\ T'_{i,j} - m & T_{i,j} = t_2 \\ T'_{i,j} & \text{others} \end{cases} \tag{3}$$

$$s_{i,j} = \tilde{s}_{i,j} + T''_{i,j} \tag{4}$$

B. Overflow Handling

The embedding operation of "the pixel greater than t_1, its corresponding pixel value moves forward a bit; the pixels less than t_2, its corresponding pixel moves backward a bit" can also cause the overflow of pixels. That is to say, for an 8-bit gray-scale image, after embedding watermark information, the pixel value may be less than 0 or greater than 255. In order to eliminate the effect of pixel value overflow, keep a record of positions and specific changes of maximum and minimum pixels overflow after processing in the differential image histogram, expressed by *Y* sequence. There are only three possible changes of pixel value caused by the algorithm, i.e. - 1, 0, 1, so only the maximum and the minimum pixel values are overflow after recovery. According to the order and end mark, watermark information *M*, authentication information *P* and sequence *Y* form a sequence to be embedded in pixel points corresponding to two peaks in the error histogram.

V. WATERMARK INFORMATION EXTRACTION AND CARRIER IMAGE RECOVERY

The extraction of watermark information is an inverse process of watermark embedding, as shown in the Fig.3.

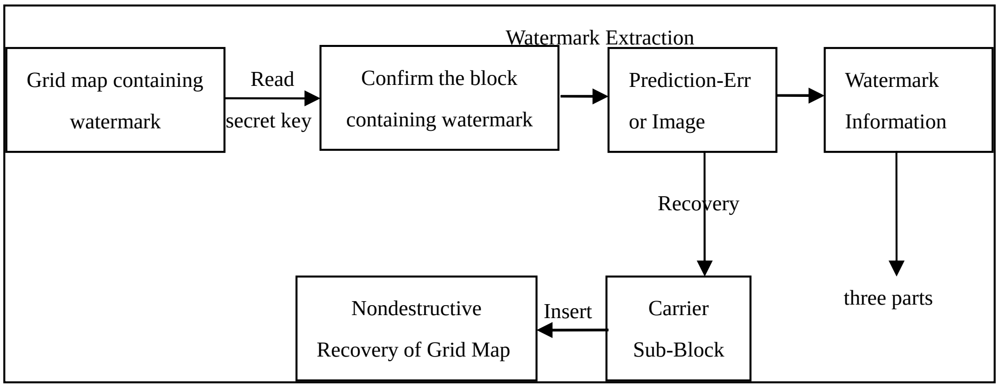

Figure 3. Process of Reversible Watermark Extraction

A. Watermark Extraction

According to secret key of algorithm, confirm the position and size of block sub-graph *I'* containing watermark information in the whole grid map. According to the same order in the above figure, scan sub-graph including watermark information, and prediction value $\tilde{S}^*_{i,j}$ of current pixel $S^*_{i,j}$ can be obtained use (5), error value $P^*_{e,i}$ (1 < = i < = r, 1 < = j < = c - 1) can be calculated use (6):

$$\tilde{S}^*_{i,j} = S^*_{i,j+1} \quad (5)$$

$$P^*_{e,i} = S^*_{i,j} - S^*_{i,j+1} \quad (6)$$

The size for differential image (matrix) *T'* formed is *r*(c-1)*, in the *T'*, select the points of pixel value t_1, t_1+1 as well as t_2, t_2-1 to extract watermark information, and the extraction formula is as (7):

$$W = \begin{cases} 0 & P^*_{e,i} = t_1 or t_2 \\ 1 & P^*_{e,i} = t_1 + 1 or t_2 - 1 \end{cases} \quad (7)$$

The extracted digital content is composed of three parts, i.e. watermark information itself, authentication information and overflow data. In order, read digital content until the first end mark, and obtain the content of watermark information. The content between the first end mark and the second one is 128-bit authentication information, and the residual content is to record the information of overflow data. Clear up the first part of watermark information, and reconstruct binary watermark image.

B. Carrier Image Recovery

In the *T'*, all the pixel values of t_1+1 and t_2 *-1* are recovered to t_1 and t_2 respectively, and all other pixel values more than t_1+1 subtract 1, all pixel values less than t_2 *-1* add 1, and the differential matrix is expressed as *T**. In the *I'*, the last row of pixels remain unchanged, and all other rows of first *c-1* pixels are recovered in the inverted sequence:

$$S_{i,j} = T^*_{i,j} + S^*_{i,j+1} \quad (8)$$

Here by 1 < = i < = r, 1 < = j < = c - 1, after gradual recovery, replace the overflow pixel by the information recording overflow data which is extracted in the first step, and then the source image *I** is recovered without any loss.

The last row of image *I'* containing watermark remains unchanged, each row can acquire prediction value from back to front in each position use (5), and the prediction-error image *T'* is obtained by (6). In the *T'*, in the order from top to bottom and from left to right, select the points with pixel value of 2, 3 and 3, -4, to extract watermark information, and the extraction formula is just as (7).

In the T', the operation of all rows is completed to get watermark information; in the meantime, the inverse process is recovered from *T'* to *T**. According to *T**, each row recovers the pixel value on each position from back to front.

In order to illustrate the algorithm embedding step, here is one simple example specific to the embedding process.

152	155	150	153	155	151	154	152
151	151	150	153	152	150	153	154
149	150	153	156	154	156	155	158
148	152	150	154	153	156	159	157
153	151	154	158	156	157	155	154
150	149	151	149	149	152	152	151
151	150	153	153	154	157	156	154
151	149	149	152	150	153	153	150

Figure 4. Original Image I of 8*8

-3	5	-3	-2	4	-3	2
0	1	-3	1	2	-3	-1
-1	-3	-3	2	-2	1	-3
-4	2	-4	1	-3	-3	2
2	-3	-4	2	-1	2	1
1	-2	2	0	-3	0	1
1	-3	0	-1	-3	1	2
2	0	-3	2	-3	0	3

Figure 5. Prediction-error Image D of 8*7

Fig.4 is a original carrier image size of 8*8. Predict the first 7 elements of each line use(1), and calculate their prediction-error use(2), then obtain the prediction-error matrix as shown in Fig.5. Generate the histogram *T* of prediction-error image *D* as shown in Fig.6.

Select the maximum peak point t_1=2 and t_2= -3. There are 12 pixels of value 2 and 16 pixels of value -3 in Fig.6. That is most 28 bits watermark information can be embedded. Hypothesis watermark information is $(1101010011111110110111111000)_2$. The pixels greater than 2 plus 1 and the pixels less than -3 reduced 1, then generate the prediction-error Image *D'* as shown in Fig.7. Then the watermark information can be embedded corresponding.

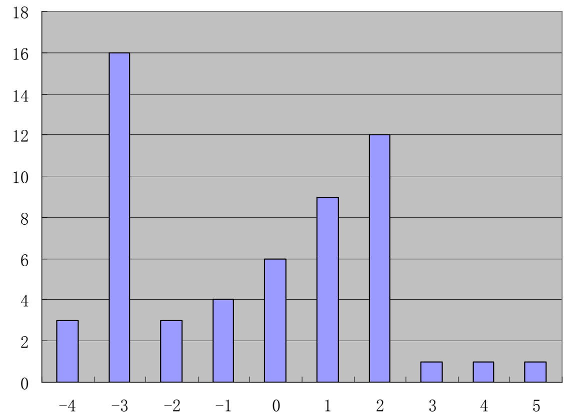

Figure 6. Histogram T of Prediction-error Image

-3	6 √	-3	-2	5 √	-3	2
0	1	-3	1	2	-3	-1
-1	-3	-3	2	-2	1	-3
-5 √	2	-5 √	1	-3	-3	2
2	-3	-5 √	2	-1	2	1
1	-2	2	0	-3	0	1
1	-3	0	-1	-3	1	2
2	0	-3	2	-3	0	4 √

Figure 7. Prediction-error Image D' Improved

Select the pixels of value 2 and value 3 in D' form top to bottom and left to right, embed 0 or 1 into D' use (3) , a new Prediction-error Image D'' is obtained as shown in Fig.8. Because pixels of last column remain unchanged, combined with D'' and reconstruction formula, the image I' embedded with digital watermark is obtained in Fig.9.

-4	6	-4	-2	5	-3	3
0	1	-3	1	3	-3	-1
-1	-3	-4	3	-2	1	-4
-5	3	-5	1	-4	-4	2
3	-4	-5	2	-1	3	1
1	-2	3	0	-4	0	1
1	-4	0	-1	-4	1	2
2	0	-3	2	-3	0	4

Figure 8. New Prediction-error Image D''

153	157	151	155	157	152	155	152
152	152	151	154	153	150	153	154

148	149	152	156	153	155	154	158
146	151	148	153	152	156	160	158
153	150	154	159	157	158	155	154
150	149	151	148	148	152	152	151
150	149	153	153	154	158	157	155
152	150	150	153	151	154	154	150

Figure 9. Carrier Image I' Embedded with Digital Watermark

VI Analysis of Algorithm Performance

The experiment adopts grid map shown in the Fig. 10 as carrier image.

Figure 10(a). Original GRB Grid Map

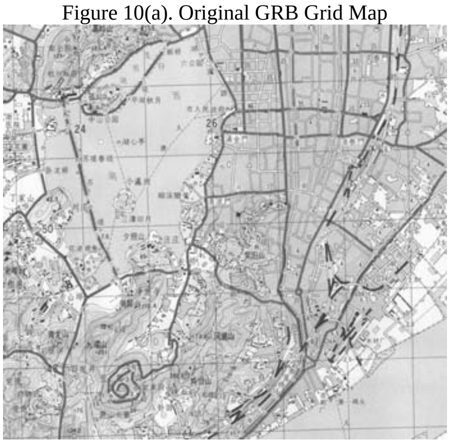

Figure 10(b). Original Gray Grid Map

Fig.10(a) is a common type map. In order to experiment more expediently and analysis result data accurately the RGB type map is transformed into the gray type map just shown as Fig.10(b) .The watermark algorithm is operated as below.

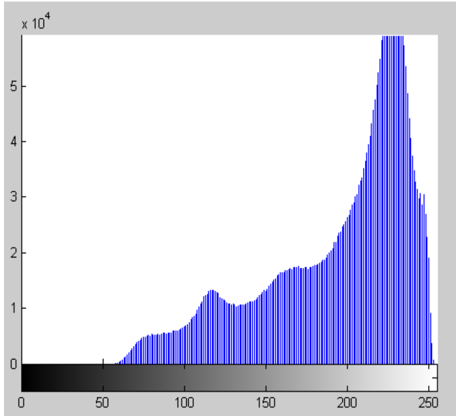

Figure 11. Histogram of Fig.10

The Fig.10 is gray-scale grid map with the size of 2133*1866, accounting for 912K storage space, and its histogram is shown in the Fig.11. It can be seen that the pixel order of magnitude is 10^4 of the same pixel value; i.e. in theory, the binary watermark image with size of 256*256 can be fully embedded.

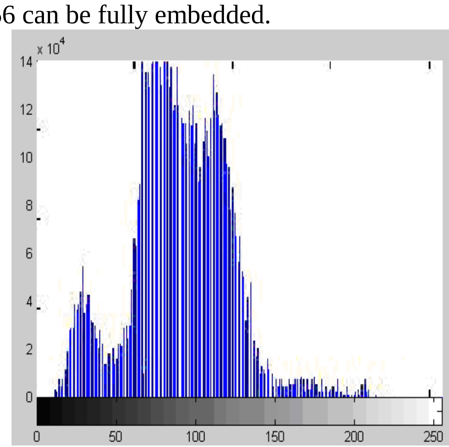

Figure 6. Prediction-Error Histogram

The algorithm in this paper is used for watermark embedding; first of all, request differential image and difference image histogram for the Fig.10, and differential image histogram is shown in the Figure12. It can be seen that, after prediction-error processing of original image, the histogram shows that, on the one hand, the number of pixels with same pixel value has increased to the greater extent, probably, 3 times as the number of pixels with the same pixel value in the original image; on the other hand, pixel peak is more centralized than that in the original image, and it is easy to deal with data overflow. This algorithm adopts the watermark embedding in the prediction-error histogram and the pixels corresponding to two peaks, and provides more embedding positions, to improve the embedding rate. The Fig.13 shows us the image after embedding watermark information by means of this algorithm.

Figure 13. Image after this algorithm embeds watermark

When this algorithm in the paper embeds watermark image as shown in the Fig. 2 into the Fig.10(b), the analysis will be conducted of actual embedding bit, embedding rate, PSNR, watermark similarity, length of generated secret key, etc. as shown in the Table 1.

Because watermark image adopted in the experiment is 256*256 binary image, watermark information itself is 65536 bits, adding 128-bit authentication information and a small amount of data overflow information, ultimately, watermark information to be embedded is 67263 bits. The difference in the proportion of watermark itself and the embedded content has great effect on actual watermark capacity and the quality of carrier data.

TABIE I
ALGORITHM PERFORMANCE

	Embedded Information Bits	Embedding Rate	PNSR	Similarity	Length of Secret Key
Algorithm	67263	0.087	58.87	100%	49

Theoretically, the algorithm’s peak signal-to-noise ratio (PSNR) is analyzed, assuming that all the pixel values are changed to 1 or -1, namely, in the worst case, the mean square error (MSE) is 1; thus the minimum PSNR can be calculated of this algorithm:

$$PSNR\ (db) = 10\log_{10}(\frac{255^2}{MSE}) \approx 48.13$$

Different sizes of watermark images are used to embed in this experiment. When the size of binary watermark image becomes large, the watermark information and the information Y that recording data flow is increased corresponding, and P remains unchanged. So the capacity of watermark information changes in amplitude is relatively slow. Fig.14 shows that with the size of watermark image become large the PSNR variance of this reversible watermarking algorithm is slowly and smoothly.

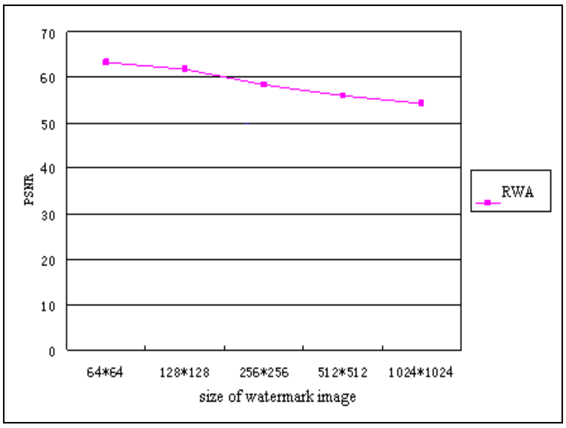

Figure 14. PSNR OF RWA

The experiment also adopts a repeat embedding way to embed multilayer information. The Fig.15 shows us the embedding rate when the given content of watermark

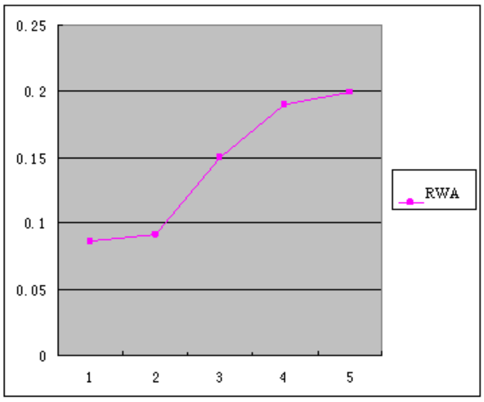

Figure15. Embedding rate when the algorithm repeats embedding

information increases or when multilayer watermarks are embedded (Take the maximum time for repeat embedding as 5), RWA means the algorithm proposed in this paper. It can be seen that the digital watermarking algorithm based on prediction-error histogram has higher embedding capacity and rate.

By integrating the above experimental results, it can be seen that, the algorithm, in which digital watermark is embedded in the differential image histogram after executing the difference for pixel value of grid image, has a higher embedding capacity, especially, the increase of watermarking information content has a little effect on carrier data. In the aspect of dealing with the complexity, due to the removal of concept of location plan, the compression of location plan is reduced, on the one hand, the capacity of embeddable watermark is increased; on the one hand, the time complexity of the algorithm is improved.

VII. CONCLUSION

The algorithm proposed by this paper is a kind of space nondestructive fragile watermarking algorithm, choosing the sub-block with the best hidden effect for operation through the calculation of entropy and variance, to ensure the balance of watermark invisibility and watermark capacity. Due to the stronger discontinuity of grid map, the algorithm selects the pixel prediction error for histogram operation, on the one hand, the pixel peak becomes more concentrated, and the embedding capacity increases; on the other hand, the pixel overflows less, its control is simple, and the original carrier image can be recovered indiscriminately.

The watermark embedding conducts the operation of the least important sign bit for the maximum pixels with same pixel value in the differential image. As the original pixel value is concerned, the maximum amplitude of change is 1, which almost has no influence on visual effect of original map. Finally, through the experiment, the algorithm is analyzed, and the experimental results show that the algorithm has higher embedding capacity and invisibility.

ACKNOWLEDGMENT

The author would like to thank BaoYu, Wang Qianping and Xu Hui. They give author too many aid and supportion. The work in this paper was supported in part by a grant from NSFC（National Natural Science Foundation of China）, No. 51204185.

REFERENCES

[1] Petitolas FAP, Anderson RJ and Kuhn M G. “Information hinding-a survey”, Proceedings of the IEEE, 1999, 87(7), pp:1062-1078.

[2] Zhu Jingjing, Digital Watermark Technology of Grid Map, Xi An, XIDIAN University, 2007, pp:55.

[3] Z. Ni, Y. Q. Shi, N. Ansari, W. Su, Reversible data hiding, IEEE Trans.Circuits Syst. Video Technol, 2006,16 (3) , pp:354-362

[4] Wong Shaowei, Research on High-Capacity Reversible Watermarking for Digital Images, Bei Jing, Beijing Jiaotong University, 2009, pp.67-78.

[5] Y. Q. Shi, Z. C. Ni, D. K. Zou, C. Y. Liang, G. R. Xuan, Lossless data hiding: fundamentals, algorithms and applications, Proceedings of 2004 International Symposium on Circuits and Syetems,2004,2, pp:33-36.

[6] S. Han. H. L. Jin, M. Fujiyoshi, H. Kiya, “Lossless data hiding in the spatial damain for image tamper detectiom”. Proceedings of International Symposium on Intelligengt Signal Proceeding and Communication Systems, Tottori, Japan, 2006, pp:760-763.

[7] D. K. Zou, Y Q. Shi, Z. C. Ni, “A semi-fragile lossless digital watermarking scheme based on integer wavelet transform”, Proceedings of IEEE 6th Workshop on Multimedia Signal Processing, 2004, 16(10), pp: 195-198.

[8] Deng Minghui, Zeng Qingshuang, Zhou Xiuli, “A Robust Watermarking Against Shearing Based on Improved S-Radon Transformation”, Journal of Computers, Vol 7, No. 10, pp: 2549-2556, October 2012.

[9] Cheng Wang, Shaohui Liu, Feng Jiang, Yan Liu, “A Robust Scalable Spatial Spread-Spectrum Video Watermarking Scheme Based on a Fast Downsampling Method”, Journal of Computers, Vol 7, No. 9, pp: 2256-2261, September 2012.

[10] W.L. Tai, C.M. Yeh, C.C. Chang, “Reversible data hiding based on histogram modification of pixel differences”, IEEE Trans. Circuits Syst. Video Technol. 2009.19 (6) ,pp: 906–910.

[11] Xinmin Zhou, Sichun Wang , Shuchu Xiong, Jianping Yu, “Attack Model and Performance Evaluation of Text Digital Watermarking” Journal of Computers, Vol 5, No. 12, pp: 1933-1941, December 2010.

[12] G.R. Feng, L.Y. Fan, “Reversible data hiding of subsampled model for edge- information prediction”, Proceedings of the International Conference on Multimedia Information Networking and Security, Nanjing, China, 2010, pp: 676–680.

Zhang Yanqun borned in1977, female, Ph.D. She received her doctor degree in Cartography and Geographic Information System from China University of Mining and Technology (CUMT) in 2011, She is an Associate Professor at School of Computer Science and Technology in CUMT. Her research interest is Information Sucrity and Information Hiding et al. She has published 1 book and 6 scientific papers. She has completed her project(NO. OD4494) of Youth Foundation of China University of Mining and Technology. She is a cooperation partners of NSFC project (No. 51204185).

Bao Yu borned in 1977, male, Ph.D. He received his doctor degree in department of computer science and technology from Tongji University in 2011, He is an Associate Professor at School of Computer Science and Technology in CUMT. His research interest is Web Data Mining and Trusted computing et al. She has published 3 books and severl scientific papers. He supported by National Natural Science Foundation of China this year and the project NO is 51204185.

Wang Qianping was born in 1966, male,Ph.D. He is a professor and a Vice President at School of Computer Science and Technology in CUMT. His research interests are Artificial Intelligence and Wireless Sensor Network, and more than 40 research papers in journals and international conferences. He has completed his project (NO. BK2006039) of Natural Science Foundation of Jiangsu Province.

Xu Hui is current a Ph.D .candidate at China University of Mining and Technology(CUMT), China. She received her MS degree in Computer Application Technology from CUMT in 2005, and her BS degree in Computer Science from CUMT in 2002. She is currently a lecture at school of Computer Science and Technology, CUMT. Her research interest is computation intelligence and coalbed methane et al.