# Method of Generating Robust Image Zero-watermark and Fragile Watermark Based on Singular Value

**Li Shao-Hua [1], Feng Jing-Ying [2], Lou Ou-Jun [1], Jing Yu [1]**

*1: Software Colleague, Dalian University of Foreign Languages, Dalian, 116044, China*
*2: Vocational Education Department, Liaoning Police Academy, Dalian, 116036, China*

Corresponding author is Li Shao-Hua

Abstract
The current watermark algorithms have the problem of singleness in function, which only have robustness or fragility. This paper, by using singular value decomposition suggests a new image watermark algorithm which has both robustness and fragility. The robust zero watermark is generated through comparing maximum singular values of adjacent two sub-blocks, and then the fragile watermark is generated by parity of decimal place of singular value, after that, the fragile watermark is embedded to the space of corresponding offset block LSB. The results show that this algorithm has strong robustness and sensitive fragility, which can realize copyright protection and content authentication at the same time.
Keywords: DIGITAL WATERMARK, ROBUSTNESS, FRAGILITY, WATERMARK TAMPERING, CONTENT TAMPERING.

## 1. Introduction

Along with the development of internet, more and more digital products are published to the web, and some problems such as copyright disputes and intentional tampering of digital products also follows. Therefore, the importance of the management of digital copyright is increasing day by day. In some cases, the management of digital copyright not only requires that the rightful owner can protect copyright effectively, but also can test and locate the area which the digital product encounters malicious tampering. However, the current watermark algorithms have the problem of singleness in function, which only has robustness or fragility. But they can't realize copyright protection and content authentication at the same time. For example, robust watermark algorithm only has robustness; it can only meet the requirement of copyright protection; the fragile watermark only has fragility; it can only meet the requirement of content authentication. So the above watermark algorithms all have single function.

Based on this, this paper aims to find out a solution. The literature proposes the concept of zero watermarks. The zero-watermark is produced by extracting the features of original carrier in the premise of not embedding external watermark, so that the conflict between robustness and invisibility can be effectively solved. In this paper, robust zero-watermark is generated by using the stability of Singular Value Decomposition, SVD, so that the algorithm has strong robustness; and the fragile watermark is generated by using parity of decimal place of singular value, so that the algorithm has sensitive fragility.

## 2. Image Sampler

### 2.1. Sampling Formula

The image sampler is the process that choose pixel unit from image. For example, a image with

the size of M x N, can be expressed as I(x,y), here x=0,…,M-1, y=0,…,N-1, two sampled factors $\Delta\mu,\Delta\nu$ are represented as interval space of the rows and columns of image respectively. Each sampling image $S_k$ with the size is of $N/\Delta\mu \times M/\Delta\nu$, it can be gotten from formula (1).

$$S_k(i,j) = I(i\cdot\Delta\nu + floor(\frac{k-1}{\Delta\mu})\cdot j\cdot\Delta\mu + ((k-1)\bmod\Delta\mu)) \quad (1)$$

Where, $i=0,...,M/\Delta\nu-1, j=0,...,N/\Delta\nu-1, k=1,...,\Delta\nu\times\Delta\nu$

**2.2. The Selection of Reference Sub-sample**

It is very important for the selection of reference subsample, because it determines spatial correlation. It can be gotten from the formula (2)

$$S_{ref} = (round(\Delta\mu/2-1)\times\Delta\nu + round(\Delta\nu/2)) \quad (2)$$

Where round(*) means rounding, for example, when $\Delta\mu=\Delta\nu=3$, $S_5$ is selected as reference subsample image.

**2.3. Calculate the Difference of Sample Image**

The differential value can be calculated from formula(3)

$$D_{ref} - des(k_1,k_2) = S_{ref}(k_1,k_2) - S_{des}(k_1,k_2) \quad (3)$$

where, $0\le k_1\le M/\Delta\nu-1, 0\le k_2\le N/\Delta\mu-1$

**3. Generation and Extraction of Robust Zero-watermark and Fragile Watermark**

The generation of robust zero-watermark

The size of original carrier image $\mathbf{I}$ is $M\times M$. The generation of robust zero-watermark is as follows:

Step1: The original image is divided into non-overlapping sub-block of $m\times m$. so the total number of sub-block is $K=M^2/m^2$. Each sub-block can be expressed as $\mathbf{I}_{r_i}, i=1,2,\cdots,K$. Hence, $\mathbf{I}=\bigcup_{i=1}^{K}\mathbf{I}_{r_i}$

Step2: each sub-block is SVD, namely, $I_{r_i}=U_{r_i}\Sigma_{r_i}V_{r_i}^T$. Both $\mathbf{U}_{r_i}$ and $\mathbf{V}_{r_i}$ are orthogonal matrix, $\Sigma_{r_i}$ is diagonal matrix which is composed of singular value $\sigma_{r_i}^p$ ($p=1,2,\cdots m$), the symbol "T"is expressed as transposition.

Step3: The robust zero-watermark $rw$ is generated through comparing the maximum singular value of adjacent two sub-blocks. The process is as follows: when $\sigma^1_{r_{2\times j-1}}\ge\sigma^1_{r_{2\times j}}$, then $rw_j=0$; or $rw_j=1$, where, $j=1,2,\cdots,K/2$, $rw_j$ is the $j$ th bit-watermark.

The generation of robust zero-watermark doesn't make any change for original image, it has good invisibility.

**3.1. Extraction of Robust Zero-watermark**

This watermarked image which is attacked is marked as H. The extraction process of robust zero-watermark is similar with the generation process of section 2.

Step1: H is divided into non-overlapping sub-block with the size is of $m\times m$. Each sub-block is marked as $\mathrm{H}_{r_i}$, $i=1,2,\cdots,K$, hence, $\mathrm{H}=\bigcup_{i=1}^{K}\mathrm{H}_{r_i}$.

Step2: Each sub-block is SVD, namely, $\mathrm{H}_{r_i}=U'_{r_i}\Sigma'_{r_i}V'^{T}_{r_i}$. $\sigma'^{p}_{r_i}$ is the $p$ th singular value of diagonal matrix $\Sigma'_{r_i}$.

Step3: The robust zero-watermark **rw** is extracted through comparing the maximum singular value of adjacent two sub-blocks. The process is as follows: when $\sigma^1_{r_{2\times j-1}}\ge\sigma^1_{r_{2\times j}}$, then $rw_j=0$; or $rw_j=1$, where, $j=1,2,\cdots,K/2$.

Step4: Similarity between the original zero watermark sequence **rw** and extracted zero-watermark sequence **rw**' is calculated. The similarity is defined as $s=1-(\sum_{j=1}^{K/2}rw_j\oplus rw'_j)/(K/2)$, where $\oplus$ is expressed as exclusive or operation.

**3.2 The Generation and Embedding Process of Fragile Watermark**

The fragile watermark is generated by taking advantage of the content of image itself, and then it is embedded into image on its own. This adaptability helps to strengthen the sensitivity of tamper of fragile watermark. Because the decimal place of singular value is more sensitive for external disturbance relative to integer, the fragile watermark can be generated by using parity of decimal place. The generation and embedding process of fragile watermark is as follows:

Step1: The original image is divided into non-overlapping sub-block with the size is of $2\times2$, each sub-block is expressed as $\mathbf{I}_{p_i}=\begin{bmatrix}x^1_{p_i} & x^2_{p_i}\\ x^3_{p_i} & x^4_{p_i}\end{bmatrix}$, where, $x^j_{p_i}$ is pixel.

Step2: LSB of pixel in each sub-block is set to 0. The obtained each sub-block is expressed as $\mathbf{I}'_{p_i}=\begin{bmatrix}x'^1_{p_i} & x'^2_{p_i}\\ x'^3_{p_i} & x'^4_{p_i}\end{bmatrix}$, $x'^j_{p_i}$ is the result of $x^j_{p_i}$ LSB set to 0.

Step3: SVD each sub-block, then according to the parity of the first two decimal places of the first two singular values, the fragile watermark $\mathbf{fw}_{p_i}$ is generated. If it is odd number, then the corresponding watermark bit is 1, or it is 0. The whole process is as follows:

$$fw^1_{p_i} = \mathrm{mod}(\mathrm{floor}(10\times\sigma^1_{p_i}),2);$$

$$fw^2_{p_i} = \mathrm{mod}(\mathrm{floor}(100\times\sigma^1_{p_i}),2);$$

$fw^3_{p_i} = \mathrm{mod}(\mathrm{floor}(10\times\sigma^2_{p_i}),2)$;

$fw^4_{p_i} = \mathrm{mod}(\mathrm{floor}(100\times\sigma^2_{p_i}),2)$;

$\mathbf{fw}_{p_i} = \begin{bmatrix} fw^1_{p_i} & fw^2_{p_i} \\ fw^3_{p_i} & fw^4_{p_i} \end{bmatrix}$, $\mathbf{fw}_{p_i}$ is fragile watermark generated after sub-block $\mathbf{I}_{p_i}$ LSB set to 0; $fw^j_{p_i}$ is the $j$ th bit fragile watermark of $\mathbf{fw}_{p_i}$, floor is the rounding function in $-\infty$, mod is remainder function.

Step4: Fragile watermark $\mathbf{fw}_{p_i}$ is embedded in pixel LSB of the corresponding offset $\mathbf{I}_{q_i}$ of $\mathbf{I}_{p_i}$, the offset sub-block $\mathbf{I}_{q_i}$ is gotten from the method in secion3. The block of embedded watermark is expressed as $\mathbf{I}''_{q_i} = \mathrm{g}(\mathbf{I}'_{q_i}, \mathbf{fw}_{p_i}) = \begin{bmatrix} x''^1_{q_i} & x''^2_{q_i} \\ x''^3_{q_i} & x''^4_{q_i} \end{bmatrix}$. g is the operation of watermark embedding, namely $fw^j_{p_i}$ is embedded into the LSB of $x'^j_{q_i}$, $x''^j_{q_i}$ can thus be gotten. In this way watermarked image can be obtained.

### 3.3. Extraction, Tamper Detection and Positioning of Fragile Watermark

The extraction of fragile watermark is similar with the its generation process in section 4. The specific process is as follows:

Step1: H is divided into non-overlapping sub-block of $2\times2$. Each block is expressed as $\mathrm{H}_{p_i} = \begin{bmatrix} h^1_{p_i} & h^2_{p_i} \\ h^3_{p_i} & h^4_{p_i} \end{bmatrix}$, and $h^j_{p_i}$ pixel value.

Step2: Extract the LSB of each block, it can be expressed as $\mathbf{l}_{p_i} = \begin{bmatrix} l^1_{p_i} & l^2_{p_i} \\ l^3_{p_i} & l^4_{p_i} \end{bmatrix}$, where $l^j_{p_i}$ is the LSB of $h^j_{p_i}$

Step3: LSB of pixel in each sub-block is set to 0. The obtained each sub-block is expressed as $\mathrm{H}'_{p_i} = \begin{bmatrix} h'^1_{p_i} & h'^2_{p_i} \\ h'^3_{p_i} & h'^4_{p_i} \end{bmatrix}$, $h'^j_{p_i}$ is the result of $h^j_{p_i}$ LSB set to 0.

Step 4: SVD each sub-block, then according to the parity of the first two decimal places of the first two singular values, the fragile watermark $\mathbf{fw}_{p_i}$ is extracted. If it is odd number, then the corresponding watermark bit is 1, or it is 0. The whole process is as follows:

$fw'^1_{p_i} = \mathrm{mod}(\mathrm{floor}(10\times\sigma'^1_{p_i}),2)$;

$fw'^2_{p_i} = \mathrm{mod}(\mathrm{floor}(100\times\sigma'^1_{p_i}),2)$;

$fw'^3_{p_i} = \mathrm{mod}(\mathrm{floor}(10\times\sigma'^2_{p_i}),2)$;

$fw'^4_{p_i} = \mathrm{mod}(\mathrm{floor}(100\times\sigma'^2_{p_i}),2)$;

$\mathbf{fw}'_{p_i} = \begin{bmatrix} fw'^1_{p_i} & fw'^2_{p_i} \\ fw'^3_{p_i} & fw'^4_{p_i} \end{bmatrix}$

$\mathbf{fw}'_{p_i}$ is fragile watermark extracted after sub-block $\mathrm{H}_{p_i}$ LSB set to 0; $fw'^j_{p_i}$ is the $j$ th bit fragile watermark of $\mathbf{fw}'_{p_i}$.

Step5: Tamper detection and location. If fragile watermark $\mathbf{fw}'_{p_i}$ is extracted from $\mathbf{H}_{p_i}$ sub-block is in accordance with LSB $\mathbf{I}_{q_i}$ of corresponding offset block $\mathbf{H}_{q_i}$, namely $fw'^j_{p_i} = l^j_{q_i}$ is set up when $j = 1,2,3,4$, which means this block doesn't tamper; if any of bits don't inconsistent, it means this block have tampered.

## 4. Experimental Results

### 4.1. Invisibility

Firstly, the invisibility is analyzed from theory. Peak signal noise ratio PSNR is used to measure the invisibility between watermarked image and original image. According to the embedded process of fragile watermark, when neither the LSB original image nor LSB watermarked image are same, PSNR is obtained the minimum value 48.13dB.

In the experiment, the Peppers image with the size is of $256\times256$ and the gray level is of 256 is taken as the original carrier image. When robust zero watermarks are generated, the image will be divided into non-overlapping blocks with the size is of $8\times8$, the length of robust zero- watermark is 512 bit. The actual PSNR between watermarked image (Fig.2) and original image is 50.1535dB, which is bigger than the theoretical minimum value.

**Figure 1**. Original Peppers Image

**Figure 2**. Watermarked Peppers Image

**4.2 Robustness**

Robust zero watermark is used to test the robustness of algorithm for anti-attack. The similarity $s$ between original robust zero-watermark and extracted robust zero-watermark is used to judge its robustness. The similarity between the two is 1, when there is no attack, which indicates that the embedment of LSB fragile watermark has no influence on the maximum of singular value of adjacent two blocks. Then watermarked image is made various attack to test its robust of anti-attack.

(1) pepper noise is added

Watermarked image is attacked by pepper noise. Table 1 shows the attack power and similarity obtained from the experiment.

**Table 1**. Pepper Noise is Added

| attack power | 0.02 | 0.03 | 0.04 |
|---|---|---|---|
| similarity | 0.9434 | 0.9082 | 0.9219 |

(2) Gaussian noise is added

Watermarked image is attacked by Gaussian noise. Table 2 shows variance of Gaussian noise and similarity obtained from the experiment.

**Table 2**. Gaussian Noise is Added

| variance | 0.01 | 0.02 | 0.03 |
|---|---|---|---|
| similarity | 0.9238 | 0.8926 | 0.9082 |

(3) Median filter

Watermarked image is attacked by median filter. Table 3 shows the size of window and similarity obtained from the experiment.

**Table 3**. Median Filter

| window size | [2,2] | [3,3] | [4,4] |
|---|---|---|---|
| similarity | 0.9609 | 0.9922 | 0.9512 |

(4) low-pass filtering

Watermarked image is attacked by low-pass filtering. Table 4 shows standard deviation and similarity obtained from the experiment.

**Table 4**. Low-Pass Filtering

| standard deviation | 0.3 | 0.4 | 0.5 |
|---|---|---|---|
| similarity | 0.9980 | 0.9980 | 0.9941 |

(5) JPEG compression

Watermarked image is attacked by JPEG compression. Table 5 shows compression quality factor and similarity obtained from the experiment.

**Table 5**. JPEG Compression

| quality factor | 10 | 20 | 30 | 40 | 50 | 60 |
|---|---|---|---|---|---|---|
| similarity | 0.8965 | 0.9453 | 0.9766 | 0.9844 | 0.9844 | 0.9883 |

(6) shear

Watermarked image is attacked by shear. Table 6 shows shearing area and similarity obtained from the experiment.

**Table 6**. Shear

| area | 1/16 top left corner | 1/8 Top left corner | 1/4 Top left corner |
|---|---|---|---|
| similarity | 0.9668 | 0.9355 | 0.8711 |

(7) Rotation

Watermarked image is attacked by rotation. Table 7 shows rotation angle and similarity obtained from the experiment.

**Table 7**. Rotation

| angle | 1 | 2 |
|---|---|---|
| similarity | 0.9043 | 0.8301 |

According to the requirement of actual application, threshold value of $s$ is $\mathrm{th}$. When $s > \mathrm{th}$, it is thought that the algorithm meets the requirement of robustness. Here, we set $\mathrm{th}=0.83$. From Table 1-7, we can see that the algorithm has strong robustness for various attack.

**4.3 Tamper Testing and Location**

In the locating image, we use one point to express a sub-block with the size is of $2\times2$. The black is regarded as background color, it is used to express the original watermarked image, and the white point is used to locate tamper area. To convenient for observation, we double the locating image. Then the highest order and the seventh order of each pixel of watermarked image (70:81,135:159) area are set to zero(see Fig.3), which means to tamper the content of each pixel within image tampering area and the image is located(see Fig.4). The assembling area of white point is the area that encounters tampering. So the algorithm can locate the tampering area exactly.

**Figure 3**. Tamper Image

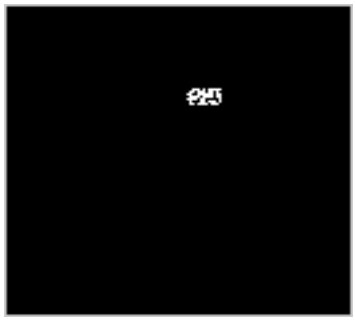

**Figure 4**. Location Image

**5. Summary**

The current watermark algorithm has the problem of singleness in function, which only has robustness or fragility. In order to solve this problem, this paper, on the basis of SVD, proposes an image watermark algorithm which has both robustness and fragility. The experimental result indicates that: this new algorithm has strong robustness and sensitive fragility; moreover, it can realize the copyright protection and content authentication.

**Acknowledgements**

The research is supported by the Scientific Research Project of Liaoning Province Educational Department No. L2012408, No. L2013432; Doctoral Scientific Research Foundation of Science and Technology Commission of Liaoning Province No. 20121037;Dalian University of Foreign Languages Studies General Project No. 2012XJYB27

**Reference**

1. J. He, Y. Geng and K. Pahlavan, Modeling Indoor TOA Ranging Error for Body Mounted Sensors, 2012 IEEE 23nd International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC), Sydney, Australia Sep. 2012, 682-686p.
2. Li, Xiaoming, Zhihan Lv, Baoyun Zhang, Ling Yin, Weixi Wang, Shengzhong Feng, Jinxing Hu. Traffic Management and Forecasting System Based on 3D GIS Cluster, Cloud and Grid Computing (CCGrid), 2015 15th IEEE/ACM International Symposium on. IEEE, 2015.
3. Li, Xiaoming, Zhihan Lv, Baoyun Zhang, Weixi Wang, Shengzhong Feng, Jinxing Hu. WebVRGIS Based City Bigdata 3D Visualization and Analysis. In Pacific Visualization Symposium (PacificVis), 2015 IEEE, 2015.
4. Lv, Zhihan, Liangbing Feng, Haibo Li, and Shengzhong Feng. Hand-free motion interaction on Google Glass. In SIGGRAPH Asia 2014 Mobile Graphics and Interactive Applications, 2014, ACM, 21p.
5. Lv, Zhihan, Liangbing Feng, Shengzhong Feng, and Haibo Li. Extending Touch-less Interaction on Vision Based Wearable Device. Virtual Reality (VR), 2015 IEEE, 2015.
6. S. Li, Y. Geng, J. He, K. Pahlavan. Analysis of Three-dimensional Maximum Likelihood Algorithm for Capsule Endoscopy Localization, 2012 5th International Conference on Biomedical Engineering and Informatics (BMEI), Chongqing, China Oct. 2012, 721-725.
7. Su, Tianyun, Zhihan Lv, Shan Gao, Xiaolong Li, and Haibin Lv. 3D seabed: 3D modeling and visualization platform for the seabed. In Multimedia and Expo Workshops (ICMEW), 2014 IEEE International Conference on, 2014, pp. 1-6.
8. Tek, Alex, Benoist Laurent, Marc Piuzzi, Zhihan Lu, Matthieu Chavent, Marc Baaden, Olivier Delalande et al. Advances in Human-Protein Interaction-Interactive and Immersive Molecular Simulations. InTech, 2012.
9. Y. Geng, J. Chen, K. Pahlavan, Motion detection using RF signals for the first responder in emergency operations: A PHASER project[C], 2013 IEEE 24nd International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC), London, Britain Sep. 2013.
10. Y. Geng, J. He, H. Deng and K. Pahlavan, Modeling the Effect of Human Body on TOA Ranging for Indoor Human Tracking with Wrist Mounted Sensor, 16th International Symposium on Wireless Personal Multimedia Communications (WPMC), Atlantic City, NJ, Jun. 2013.
11. Y. Geng, J. He, K. Pahlavan, Modeling the Effect of Human Body on TOA Based Indoor Human Tracking [J]. International Journal of Wireless Information Networks, 20(4), 306-317p.
12. Zhang, Mengxin, Zhihan Lv, Xiaolei Zhang, Ge Chen, and Ke Zhang. Research and Application of the 3D Virtual Community Based on WEBVR and RIA. Computer and Information Science 2, 2009, no. 1: 84p.
13. Zhong, Chen, Stefan Müller Arisona, Xianfeng Huang, Michael Batty, Gerhard Schmitt. Detecting the dynamics of urban structure through spatial network analysis. International Journal of Geographical Information Science 28, 2014, no. 11: 2178-2199p.