The method of Digital Watermarking Based on Improved Singular Value (SV)

Yang Shi

Yunyang Teachers' College, Hubei, China

Keywords: SV; Watermark; Copyright protection

Abstract. In this paper, we introduce a transform domain watermarking algorithm based on SV. It has good robustness. It also describes the principle of this algorithm in detail . With our new algorithm, The intensity of the watermark to be inserted can be adjust easily, and watermark information can be embedded into one image and according to the quality of the image which contains the watermark information, the robustness and capability of watermarking can be adjusted easily. The results show that this algorithm has strong robustness and sensitive fragility, which can realize copyright protection and content authentication at the same time.

Introduction

Digital watermarking is a potential technology, which can solve the problem of multimedia copyright protection etc. One of the main parts of digital watermarking research is about algorithm research. Usually, the watermarking algorithm contains the process of embedding and watermark detection. Normally the general watermarking methods on transform domain become more and more popular, due to its good robustness and resistance to image compression, image filtering and noise etc. While the merit of those algorithms based on spatial domain is simple and fast, together with relatively less robust.

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 2×2, each sub-block is expressed as $\mathbf{I}_{p_i}=\begin{bmatrix} x_{p_i}^1 & x_{p_i}^2 \\ x_{p_i}^3 & x_{p_i}^4 \end{bmatrix}$, where, $x_{p_i}^j$ is pixel.

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

$fw_{p_i}^1=\mathrm{mod}(\mathrm{floor}(10\times\sigma_{p_i}^1),2)$; $fw_{p_i}^2=\mathrm{mod}(\mathrm{floor}(100\times\sigma_{p_i}^1),2)$;

$fw_{p_i}^3=\mathrm{mod}(\mathrm{floor}(10\times\sigma_{p_i}^2),2)$; $fw_{p_i}^4=\mathrm{mod}(\mathrm{floor}(100\times\sigma_{p_i}^2),2)$;

$\mathbf{fw}_{p_i}=\begin{bmatrix} fw_{p_i}^1 & fw_{p_i}^2 \\ fw_{p_i}^3 & fw_{p_i}^4 \end{bmatrix}$, $\mathbf{fw}_{p_i}$ is fragile watermark generated after sub-block $\mathbf{I}_{p_i}$ LSB set to 0;

$fw_{p_i}^{j}$ is the jth 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 $\mathbf{I}_{q_i}^{''} = \mathrm{g}(\mathbf{I}_{q_i}^{'}, \mathbf{fw}_{p_i}) = \begin{bmatrix} x_{q_i}^{''1} & x_{q_i}^{''2} \\ x_{q_i}^{''3} & x_{q_i}^{''4} \end{bmatrix}$. g is the operation of watermark embedding, namely $fw_{p_i}^{j}$ is embedded into the LSB of $x_{q_i}^{'j}$, $x_{q_i}^{''j}$ can thus be gotten. In this way watermarked image can be obtained.

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: $\mathbf{H}$ is divided into non-overlapping sub-block of 2×2. Each block is expressed as $\mathbf{H}_{p_i} = \begin{bmatrix} h_{p_i}^{1} & h_{p_i}^{2} \\ h_{p_i}^{3} & h_{p_i}^{4} \end{bmatrix}$, and $h_{p_i}^{j}$ pixel value.

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

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

$fw_{p_i}^{'1} = \mathrm{mod}(\mathrm{floor}(10 \times \sigma_{p_i}^{'1}), 2)$; $fw_{p_i}^{'2} = \mathrm{mod}(\mathrm{floor}(100 \times \sigma_{p_i}^{'1}), 2)$;

$fw_{p_i}^{'3} = \mathrm{mod}(\mathrm{floor}(10 \times \sigma_{p_i}^{'2}), 2)$; $fw_{p_i}^{'4} = \mathrm{mod}(\mathrm{floor}(100 \times \sigma_{p_i}^{'2}), 2)$; $\mathbf{fw}_{p_i}^{'} = \begin{bmatrix} fw_{p_i}^{'1} & fw_{p_i}^{'2} \\ fw_{p_i}^{'3} & fw_{p_i}^{'4} \end{bmatrix}$

$\mathbf{fw}_{p_i}^{'}$ is fragile watermark extracted after sub-block $\mathbf{H}_{p_i}$ LSB set to 0; $fw_{p_i}^{'j}$ 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 $\mathbf{l}_{q_i}$ of corresponding offset block $\mathbf{H}_{q_i}$, namely $fw_{p_i}^{'j} = l_{q_i}^{j}$ 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.

Experimental Results

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 256×256 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 8×8, the length of robust zero- watermark is 512 bit. The actual PSNR between watermarked image (fig.1) and original image is 50.1535dB, which is bigger than the theoretical minimum value.

Fig 1. original Peppers image

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.

Tamper Testing And Location

In the locating image, we use one point to express a sub-block with the size is of 2×2. 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.2), which means to tamper the content of each pixel within image tampering area and the image is located(see fig.3). The assembling area of white point is the area that encounters tampering. So the algorithm can locate the tampering area exactly.

Fig.2 tamper image

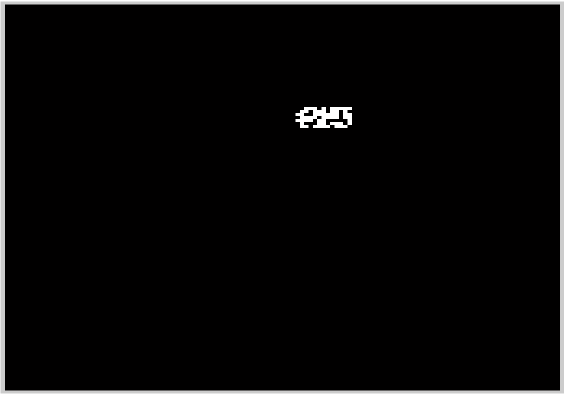

Fig.3 location image

Conclusion

Based on SV, along with the enlarging of its size, more time will be spent in computing the SVs, and experiments show that the distortion in the diagonal direction is conspicuous, due to the calculation error, so we present a watermarking algorithm based on Block-SV, we alse improve on it to add distortion compensation. In this method, the original image is divided into several blocks and the size of each block is 8-by-8. In watermark detection, we propose the idea of detector compensation to distortion. Extensive experiments show that the new method is very robust against image distortion. Based on the quick embedding, for the aspect of big images, such as complicated circuit diagram, mechanical drawing and architectural drawing, we believe it is a promising watermarking technology. At last the method based on Block-SVD is compared to the traditional Cox method, which also shows that the new method is very robust.

Reference

[1] 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, p. 21. ACM, 2014.

[2]Lv, Zhihan, Liangbing Feng, Shengzhong Feng, and Haibo Li. "Extending Touch-less Interaction on Vision Based Wearable Device." Virtual Reality (VR), 2015 iEEE. IEEE, 2015.

[3]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, no. 1 (2009): p84.

[4]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 (page 682-686)

[5]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