A Texture Synthesis Steganography Scheme Based on Super-Pixel Structure and SVM

Weiyi Wei, Chengfeng A, Lizhao Wang, Huifang Ma

A Texture Synthesis Steganography Scheme Based on Super-pixel Structure and SVM

Weiyi WEI , Chengfeng A, Lizhao WANG, Huifang MA

(College of Computer Science and Engineering，Northwest Normal University，Lanzhou，Gansu，730070，China)

Abstract. In order to improve the performance of coverless steganography algorithm against JPEG compression, this paper proposes a texture synthesis steganography scheme based on super-pixel structure and SVM. Firstly, selects a small texture pattern and partition it into overlap block, in addition, each image candidate block is super-pixel segmented, and the average pixel value of each super-pixel block is used as the feature value of this image candidate block which has structured information. Then use the trained SVM classifier to determine the categories to classify into different collections, each collection maps a secret data. Secondly, when hiding the secret information, the pseudo-random sequence is generated with specified key to determine the position of the texture candidate block placed on the white paper, the candidate block is randomly selected from the corresponding set according to the content of the secret information and is placed on the designated position of the white paper, meanwhile, and the remaining blank areas are filled with texture synthesis method. When extracting information, it is no need to restore the original texture patterns, the secret message is picked according to find specified image block and determine which category it is. Experimental results show that the carrier image generated by this method has good invisibility and better effect to anti-compression.

Keywords: Super-pixel, Texture synthesis, Steganography, SVM, Coverless information hiding.

1 Introduction

Information hiding (IH) is a technology that hides secret information in digital media, has become an important research field in information security. Steganography is one of the main research directions in information hiding which main purpose is to hide secret information to avoid the eavesdroppers' suspicious. At present, common image information hiding scheme, it is divided into spatial domain and transform domain according to the difference of hidden ways. There are many classical steganography methods such as the least significant bit (LSB) proposed in [2]. An adaptive LSB method using pixel-value difference (PVD) proposed improving hidden capacity and invisibility in [3]. And the method of changing certain statistical features by modifying the data of the host image [4-5], etc. Meanwhile, steganography can be performed in image transform domain such as DFT domain [6-7], DCT domain [8-9],

DWT domain [10-11], etc. Most of these methods are limited by certain distortions caused by modifying the cover's pixels and the modification trace is inevitably left on the cover, and that the hidden information is also difficult to resist the detection of various steganalysis.

Therefore, in order to resist the steganalysis fundamentally, some new steganography methods have emerged. In May 2014, some scholars proposed the new concept of "coverless information hiding" compared to traditional information hiding. It directly uses secret information as a driver to "generate/acquire" stego cover [12-13]. Representative work is a steganography scheme for generating a texture image. Otori and Kuriyama [14-15] first proposed the idea of data embedding in the texture synthesis process in 2009. This method uses the concept of LBP code to achieve the final information hiding, however, there are also limitations on the low capacity and the extraction of errors. Wu and Wang [16] proposed another new texture steganography method based on index selection in 2015. Re-sampling the smaller texture image during the texture process to construct a new texture image to hide the secret information, but it still has loopholes. Xu et al.[17] proposed a new steganography scheme that hides information through simulated watermark by in 2015. This method utilizes the aggregate deformation to generate the marbling effect, however, it can only hide words and patterns with meaning, and cannot hide binary data. Zhang et al. [18] proposed a new steganography method to achieve higher embedded capacity in 2016. Qian et al. [19] proposed a novel information hiding method based on texture synthesis in 2016. This method calculates the complexity of each block and classifies all candidate blocks into different sets according to the size of the complexity.

The above literature methods makes a good improvement of the texture synthesis information hiding, however, once the stego image is compressed by the tools like JPEG, many errors would happen during message extraction. To overcome this problem, we propose a texture synthesis steganography scheme based on super-pixel structure and SVM. Experimental results have shown that our algorithm can produce a plausible texture images and it is further improved in the anti-compression ability and robustness.

The remainder of this paper is organized as follows:
in Section II, We illustrate the basic framework of this algorithm. In Section III, we detail our algorithm including embedding and extracting procedures. We describe experimental results and theoretical analysis in Section IV, followed by our conclusions presented in the concluding section.

2 Proposed Method

The texture synthesis steganography scheme based on super-pixel structuring and SVM proposed in this paper mainly consists of three parts, super-pixel partitioning (SLIC)[20], train SVM classifiers, information hiding and extraction algorithms. Framework of the proposed method is showed in Fig. 1.

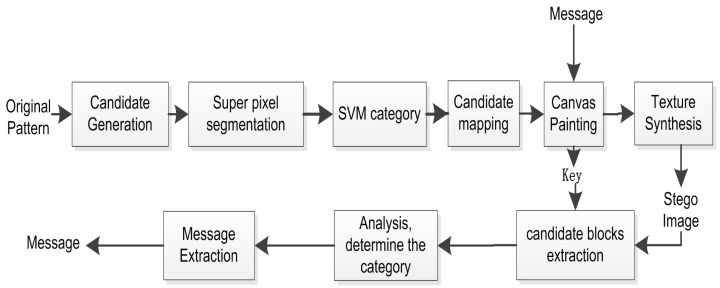

Fig. 1. Framework of the proposed method

Firstly, selects a small texture pattern and partition it into overlap block, in addition, each image candidate block is super-pixel segmented, and the average pixel value of each super-pixel block is used as the feature value of this image candidate block which has structured information. Then use the trained SVM classifier to determine the categories to classify into different collections. Each collection maps a secret data. Secondly, when hiding the secret information, the pseudo-random sequence is generated with specified key to determine the position of the texture candidate block placed on the white paper, the candidate block is randomly selected from the corresponding set according to the content of the secret information and is placed on the designated position of the white paper, meanwhile, and the remaining blank areas are filled with texture synthesis method. When extracting information, it is no need to restore the original texture patterns, the secret message is picked according to find specified image block and determine which category it is.

3 Steganography Algorithm

3.1 Data Hiding

The texture synthesis steganography algorithm based on super-pixel structure and SVM is:

Step1: Given a source texture pattern with the size of $S_{\mathrm{r}} \times S_{\mathrm{c}}$, and divides this pattern into overlapped blocks.

Step2: The size of each image block is $T_r \times T_{\mathrm{c}}$, we further divide this image block into kernel area and boundary area, as shown in Fig. 2.

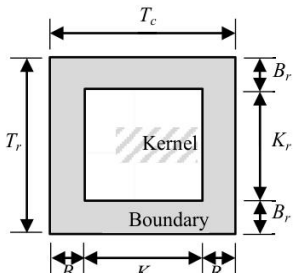

Fig. 2. A block containing the kernel area and the boundary area

Each image candidate block is super-pixel segmented with the same number, and the average pixel value of each super-pixel block is used as the feature value of this image candidate block. Then identify which category it belongs to by means of the trained SVM classifier, each category maps a secret data.

Step3: When hiding the secret information, the pseudo-random sequence is generated with the specified key to determine the position of the texture candidate block placed on the white paper.

Step4: The candidate blocks are randomly selected from the corresponding set according to the content of the secret information, in other words, the category label of candidate block selected as equals to a secret value. Then put it on the designated position of the white paper, meanwhile, the remaining blank areas are filled with texture synthesis method. We use the "image quilting" algorithm proposed by Efros and Freeman in [21]. In [21], synthesis is realized by iteratively padding chosen identical sized candidates to a blank window. Since there are overlapped regions, errors between the chosen block and the existing blocks from the overlapped region are computed. Generally, a best tile that has the smallest mean square errors (MSE) of the overlapped parts are selected. A diagram is illustrated in Fig. 3(a). Regions in gray color stand for the synthesized contents. When synthesizing the content of "C", MSE of the overlapping regions between "C" and the upper tile "A", and MSE between "C" and the left tile "B" are calculated. One candidate that has the smallest MSE is selected as the best. Then, the minimum cost path along the overlapped surface is computed to find the seam, see the red curves on the overlapped region, and the content is pasted onto the canvas along the seams.

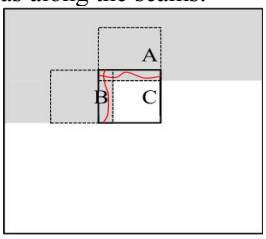

Fig. 3. Synthesizing the blank regions

3.2 Data Extraction

The method of extracting secret information in the stego image is:

Step1: Extract the stego image block according to the pseudo-random sequence generated with same key.

Step2: The extracted image block is determined which category it belongs to by the trained SVM classifier, and the category of the information block is obtained.

Step3: Read the secret information.

4 Experimental results and analysis

In order to verify the performance of the proposed algorithm, experiments were performed by loading several texture images from "Brodatz Textures" [21] texture library, randomly extract small blocks and use the SLIC segmentation algorithm to perform super-pixel segmentation on each image block, then cluster with K-means algorithm, classifiers are trained using image blocks and class labels as input and output of the SVM classifier, respectively. The trained SVM classifier is used as a typical texture image classifier to determine the class of image candidate blocks.

In this paper, different texture images are selected from the "Brodatz Textures" [21] texture library. Figure 5 (a) ~ (h) are two types of source texture images, the size of which is 128×128 , Figures 5 (i) ~ (p) are generated stego image of size 653×653 . The results show that the generated stego image have a good visual effect.

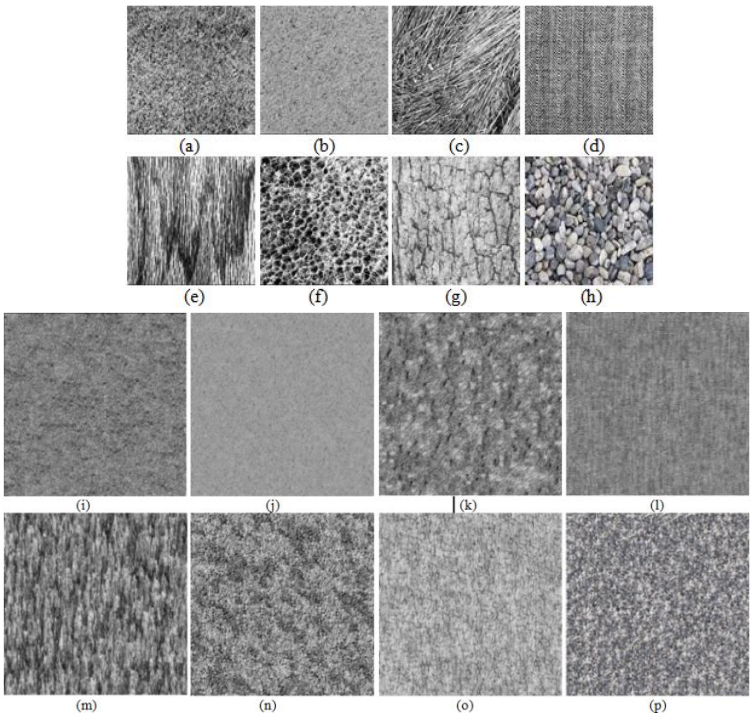

Fig. 4. Source patches and the stego textures. (a)~(h) are the source patches. (i)~(p) are the synthesized textures containing secret messages.

In this paper, we use SLIC super-pixel segmentation algorithm to process each image candidate block, and use the already trained SVM classifier to determine the class, so the method proposed in this paper has better robustness, as shown in Figure 5, steganography image size is 653×653, candidate block size is 16×16, kernel size is 3×3, and different M values (from 2 to 16), then use JPEG to compress using different quality factors (from 10 to 40), after extracting the hidden bits from the compressed stealth signal, the average error rate of the extracted bits in these images is calculated.

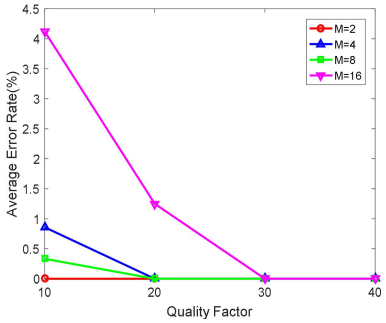

Fig .5. anti-compression performance

Stego image generated after embedding secret information, after JPEG compression, there is bound to be information loss. The smaller the quality factor, the greater the loss of information, loss of information may also result in the loss of confidential information, therefore, the anti-jamming ability of the algorithm is reflected by the quality factor and the extracted error curve. As can be observed in Figure 5, when the quality factor increases, the average error rate approaches zero. At the same time, the smaller M (candidate block class), the smaller the error rate. It can be seen that fewer categories of candidate blocks, the stronger the ability to resist compression. When there are just two types, stego image can even resist JPEG compression with a quality factor of 10.

At the same quality factor (QF), under JPEG compression attacks, We compare the algorithm in [19] and the algorithm of this paper. As showed in Figure 6 and Table 1.

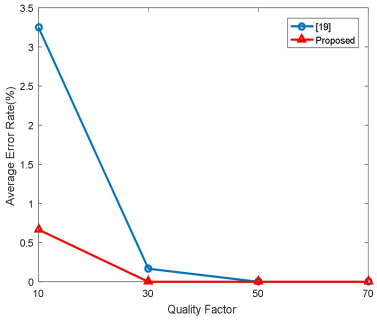

Fig.6. Algorithm and document algorithm anti-compression performance ratio

Table 1. The average error rate of data extraction after compressing hidden images

QF	[19]	Proposed
1	0.23083	0.04
10	0.0325	0.0066667
25	0.00083333	0
30	0.0016667	0
40	0	0

QF means the degree of loss of compressed loss of information. The smaller the value, the more it loses, the less information it retains, the higher the requirements imposed on the algorithm for embedding the secret message, because lossy compression may damage the secret information. So under the fixed quality factor, the smaller the average error rate of the algorithm is the better, because the smaller, it means that there is less information about error the confidential information that can be extracted. Similarly, the smaller the QF value, the better the anti-jamming ability of the algorithm. Experiments show that the steganography algorithm proposed in this paper has a better effect on the anti-compression ability and robustness.

As the stego images are constructed by texture synthesis, sometimes it is somewhat weird to transmit a texture over internet. In real applications, the stego can be used as the backgrounds of some images. Two examples are shown in Fig. 7. Background of Fig. 7(a) is the synthesized grass containing secret message, adding a football as the foreground. The secret message is hidden in the content outside the blue square. In Fig. 7(b), the synthesized stego texture is used as the background of a pop star, in which secret messages can be extracted from the regions squared by red rectangles.

Fig. 7. Applications of texture synthesis based steganography. Backgrounds of both (a) and (b)are the synthesized stego textures.

5 Conclusion

This paper proposes a texture synthesis steganography method based on super-pixel and SVM. Select a original small-size texture pattern and partition it into overlap block, in addition, each image block is super-pixel segmented, and the average pixel value of each super-pixel block is used as the feature value of this image candidate block which has structured information, the secret message is represented by different types candidate block. Controlled by a secret key, candidate blocks category mapping secret bits are placed in assigned positions in the blank canvas. With image quilting algorithm, the canvas is then filled with appropriate candidate blocks to construct a texture image with good visual appearance. When extracting information, it is no need to restore the original texture patterns, the secret message is picked according to find specified image block and determine which category it is. Different from the traditional steganography methods, the steganography schemes proposed in this paper have a better effect in anti-compression and robustness. As a new camouflage way, stego image by texture synthesis can be used in many applications.

Acknowledge

This work was supported by National Natural Science Foundation of China (Grant 61762080, 61762078), Science and Technology Plan of Gansu Province (17YF1FA119). Corresponding author: Chengfeng A, E-mail: 1640707657@qq.com

References

1. Fridrich, Jessica. Steganography in Digital Media: Principles, Algorithms, and Applications. Cambridge University Press, 2009.
2. Tirkel A Z, R Ankin G A, and Schyndel R V. Electronic Watermark. Digital Image Computing, Technology and Applications, 1993.
3. Yang C H, Weng C Y, and WAng S J. Adaptive data hiding in edge areas of images with spatial LSB domain systems. IEEE Transactions on Information Forensics & Security, vol. 3, no. 3, pp. 488-497, 2008.
4. Bender W R, Gruhl D, and Morimoto N. Techniques for data hiding. IBM Systems Journal, vol. 35, no. (3.4), pp. 313-336, 1996.
5. Shi Y Q. Reversible data hiding. IEEE Transactions on Circuits and Systems for Video Technology, vol. 16, no. 3, pp. 354-362, 2006.
6. Ruanaidh, J. J. K. O, W. J. Dowling, and F. M. Boland. Phase watermarking of digital images. Proceeding of Int.conf. on Image Processing, vol.3, no. 3, pp. 239-242, 1996.
7. Xu D H, Zhu C Q, Wang Q S. A construction of digital watermarking model for the vector geospatial data based on magnitude and phase of DFT. Journal of Beijing University of Posts & Telecommunications, 2011, 34(5):25-28.
8. Si Y S, Yang W T, Zhang S. Information hiding technology research based on digital image. Computer CD Software and Application, vol. 16, pp. 160-161, 2011.

9. Cox I J, Kilian J, and LEighton F T. Secure spread spectrum watermarking for multimedia. IEEE Transactions on Image Processing, vol. 6, no.12, pp. 1673-87, 2010.
10. Hsieh M S, Tseng D C, Huang Y H. Hiding digital watermarks using multire solution wavelet transform. IEEE Transactions on Industrial Electronics, vol. 48, no. 5, pp. 875-882, 2001.
11. Lin W H, Horng S J, KaoT W. An efficient watermarking method based on significant difference of wavelet coeffi cient quantization. IEEE Transactions on Multimedia, vol. 10, no. 5, pp. 746-757, 2008,
12. Zhou and Zhili, Coverless Image Steganography Without Embedding. International Conference on Cloud Computing and Security Springer International Publishing, pp. 123-132, 2015.
13. Chen X, Sun H, Tobe Y. Coverless information hiding method based on the chinese mathematical expression. Cloud Computing and Security. Springer International Publishing, 2015, pp. 133-143.
14. Otori, Hirofumi, and S. Kuriyama. Data-Embeddable Texture Synthesis. Smart Graphics, International Symposium, Sg 2007, Kyoto, Japan, June 25-27, 2007, Proceedings DBLP,146-157, 2007.
15. Otori H, KUriyama S. Texture synthesis for mobile data communications. IEEE Conference Graphics Applications, vol. 29, no. 6, pp. 74-81, 2009.
16. Wu K C, Wang C M. Steganography using reversible texture synthesis. IEEE Transactions Image Processing, vol. 24, no. 1, pp. 130-139, 2015.
17. Xu J, Mao X, Jin X. Hidden message in a deformation-based texture. Visual Computer, vol. 31, pp. 1653-1669, 2015.
18. Pan L, Qian Z, and Zhang X. Digital Steganography Based on Textured Texture Images. Journal of Applied Sciences, vol. 34, no. 5, pp. 625-632, 2016.
19. Qian Z, Zhou H, Zhang W. Robust Steganography Using Texture Synthesis. Advances in Intelligent Information Hiding and Multimedia Signal Processing. Springer International Publishing, 2017.
20. Wang C, Chen J, Li W. A Survey of Super-pixel Segmentation Algorithms. Journal of Computer Applications, vol. 31, no. 1, pp. 6-12, 2014.
21. Efros, Alexei A, and W. T. Freeman. Image quilting for texture synthesis and transfer. Proc. SIGGRAPH, vol. 2001, pp. 341-346, 2001.