Data security using Steganography and Reversible Texture Synthesis

[1]Prajakta N. Akhare, [2]Kajal R. Gaikwad, [3]Kiran M. Taikar, [4]Sapna S. Tirpude, [5]Jyoti M. Shahu

[1]Prajakta N. Akhare, B.E., CSE , Gurunanak Institute of Engineering and Technology, Nagpur, India
[1]prajaktaakhare1995@gmail.com

[2]Kajal R. Gaikwad, B.E., CSE, Gurunanak Institute of Engineering and Technology, Nagpur, India
[2]kajalgaikwad17@gmail.com

[3]Kiran M. Taikar, B.E., CSE, Gurunanak Institute of Engineering and Technology, Nagpur, India
[3]kirantaikar95@gmail.com

[4]Sapna S. Tirpude, B.E., CSE, Gurunanak Institute of Engineering and Technology, Nagpur, India
[4]sapna.tirpude1997@gmail.com

[5]Jyoti M. Shahu, B.E., CSE, Gurunanak Institute of Engineering and Technology, Nagpur, India
[5]jmshahu@gmail.com

ABSTRACT

We propose a novel approach for steganography using a reversible texture synthesis. A texture synthesis process takes the small unit of the texture image, that leads to a new texture image with a smaller portion of old texture and with arbitrary size. We weave the texture synthesis process into steganography to hide secret messages. In contrast to using an existing cover image to hide messages, our algorithm hides the source texture image and embeds secret messages through the process of texture synthesis. This allows us to extract the secret messages and source texture from a stego synthetic texture. It offers three main advantages. The first advantage is the embedding capacity which is greater than or equal to the size of the stego texture image. Second is that our steganographic approach is not defeated by any steganalytic algorithm. Third is the reversible capability which allows recovery of the source texture. Thus our proposed algorithm can provide embedding capacities, produce a visually acceptable texture images, and recover the source texture.

Keywords: steganography, texture synthesis, patch

1.INTRODUCTION

Steganography is a data hiding technique. It embeds messages into a host medium in order to hide secret messages so an unauthorized person can not get access to our data. The application of steganography includes displayed communication between two parties but the communication is not open the existence of Parties are unknown to the possible attacker and who can get success depends on the detection of the existence of this communication [1]. Secret messages are embedded into the cover image and that can lead to damage of image in the stego image. Hence it reduces the embedding capacity and quality of the cover image The one who wants to hack the hidden message in a stego image can be successful by applying any image stegnalytic algorithm. steganography technique is used to improve the level of protection of data.This cause development of new algorithms having strong security, capability and imperceptibility [2]. The image is the most popular object of the steganography. Patch-based algorithms describe the steganography and reversible texture synthesis [3].Patch-based algorithm increases the quality of the image of pixel based synthetic texture.

2.RELATED WORK

In [3] . A texture synthesis process takes the small unit of the texture image, that leads to a new texture image with a smaller portion of old texture and with arbitrary size steganography technique is used to improve the level of protection of data. This cause development of new algorithms having strong security, capability and imperceptibility

In [2] authors advanced MSB (Most Significant Bit method) steganography method with random pixel selection. In the color image, By using Most Significant Bit method we can embed more secret data. The algorithm that we proposed is totally based on different size image segmentations (DSIS) algorithm and modified least significant bits (MLSB) algorithm. The DSIS algorithm is applied to hide secret image randomly instead of serially. Before of hiding secret data the DSIS approach is applied. The advantage of this algorithm is working against attack by generating undetectable stego

image.

Pixel-based algorithms [4], [5], [6] can form the synthesized image pixel by pixel. We can use spatial neighborhood comparisons to select the most common pixel as the output pixel in a sample texture. If a single pixel get affected, it will affect rest of the result.

In [6]**,** It embeds messages into a host medium in order to hide secret messages so an unauthorized person can not get access to our data.The cover communication between the patches is caused by the use of steganalytic algorithm and also used to extract the source texture, secret message from the original image. The encrypted image looks as that of original image. To embed the data, line based cubism like image segmentation technique is used. The image after embedding the data on the cover image is called as stego image. Reversible texture synthesis process on pixels of the smaller textures or the original image and generate the output as that of the original image. This increases the arbitrary size of texture synthesis which is good for improvement of the embedding efficiency. Second advantage is it provides the source texture without any alteration. Reversible data hiding technique is used to provide the capacity of better embedding process**.** Steganalytic algorithm is used to extract the source texture.

In [8] in this paper, a reversible steganographic algorithm using texture synthesis is proposed. According to that algorithm, the original source texture is converted into a large stego synthetic texture which hides the secrete message.The method provides reversibility for retrieving the original source texture from the stego synthetic textures, making possible a second round of texture synthesis if needed. Visually plausible stego synthetic textures are produced. The explained algorithm is secure and robust against a Regular Singular (RS) steganalysis attack.

3.PROPOSED SYSTEM

Our proposed algorithm can provide various numbers of embedding capacities, produce a visually plausible texture images, and recover the source texture. The image reversible data hiding algorithm is proposed which can recover the cover image without any distortion from the stego image after the hidden data have been extracted. The basic unit used for our steganographic texture synthesis is called as a "patch."

The project consist of two techniques-

A. Message Embedding Technique

B. Message Extracting Technique

A. Message Embedding Technique - The process of hiding the message behind the image is called as message embedding

B. Message Extracting Technique- The process of a retrieving message from the image is called as message extracting.

4. CONCLUSION

Steganography is a different way to secure the communication. By Giving an original source texture, our scheme can generate a large stego synthetic texture which hides the secret messages. Our method provides the reversibility for retrieving the original source texture from the stegosynthetic textures, and also if their is need of second round of texture synthesis then it can be easily done by using proposed approach. Using this approach we recover the original image. The main drawback of this technique is that time complexity as compare to the another technique.

5. REFERENCE

[1]. F. A. P. Petitcolas R. J. Anderson and M. G. Kuhn "Information hiding survey." Proc IEEE vol. 87, no. 7, PP 1062-1078, Jul 1999.

[2].Hamdan Lateef Jaheel and Zou Beiji, A Novel Approach of combining steganography Algorithms" International Journal on smart sensing and Intelligent systems vol. 8, no. 1, March 2015

[3]. Kuo-Chen Wu, and Chung-Ming Wang,"Steganography Using Reversible Texture Synthesis,"IEEE Transactions on Image Processing, vol. 24, January 2015.

[4]. L-Y Wei and M. Levoy, "fast texture Synthesis using tree-structured vector quantization," in proc of the 27th Annual Conference on computer graphics and interactive techniques, 2000, pp.479-488

[5] A. A. Efros and T. K. Leung, "Texture synthesis by non-parametric sampling," in Proc. of the Seventh IEEE International Conference on Computer Vision, 1999, pp. 1033-1038.

[6] C. Han, E. Risser, R. Ramamoorthi, and E. Grinspun, "Multiscale texture synthesis," ACM Trans Graph, vol. 27, no. 3, pp. 1-8, 2008.

[7] Geetha. P, and Priya. K, N. Abirami, "Steganalytic Algorithm Using Reversible Texture Synthesis for Embedding Data".

[8] Munshidha K K1, and Anju Augustine, "Efficient Steganographic Method Using Reversible Texture Synthesis".

