Use Of Reversible Texture Synthesis Method For Steganography

[1]Vikas D. Chavan, [2]Prof. Deepak S.U

Department of Computer Engineering Rajarshi Shahu School of Engineering and Research Pune ,Maharashtra, India.

Abstract- *A steganography is an art of hiding confidential data into digital media such as image, audio ,video etc. Here we are going to combine the work of steganography along with image processing. To do this a texture synthesis process is used which re-samples input texture image to create a new texture synthesis image.*

Existing steganography process is much expensive and not so robust because if the size of the secret message increases it results into distortion of the image. A texture synthesis process provides embedding capacity so that to hide the large message. With the texture synthesis process the blank image is constructed from input image and the input image is divided into no. of different patches. These patches are given a patch ID and randomly pasted on the blank image. To do this , the index table is constructed which provides an entry for each patch. The index table is constructed by using a secret key so that the person having a secret key can only access the index table. Index table tells where to paste the patch on the blank image.

KEYWORDS- **Data embedding, example-based approach, Changable, steganography, texture synthesis**

1. INTRODUCTION

The steganography is an art of hiding existence of the data in another transmission medium to achieve the secret communication. It is not the replacement for the cryptography but rather it boosts the security. Steganography method used in this project is based on reversible texture synthesis process. In the typical steganography process two parties try to make secure communication and whose success depends on detecting the existence of the communication. Moreover a steganography is a mechanism which conceals the secret messages inside other compatible media so that any enemy could not be able to detect it. There are various steganographic algorithms available in the literature which provides high amount of security with lower distortion. But these algorithms are quite harsh to implement as they fail to provide robustness.

In this project texture synthesis process is widely used which takes source texture image as an input and creates the new stego synthesized image as an output. The stego synthetic image is a composition of secret message as well as the source texture image.

This approach have three main advantages.

1.Preliminary process of synthesizing the texture image of an consistent size can offer an optimal embedding capacity which is proportional to the size of stego structured image.

2. As the stego structured image is composed of source texture, our proposed system is not vulnerable to any kind of hazards generated in steganalytic algorithm.

3. Most importantly, a proposed system can inherit various functionalities to revert the source texture back.

With above advantages, the proposed system will be full-fledged to synthesize source texture image and impose security over it by embedding the secret message over to it.

2. RELATED WORK

The proposed steganography process uses the patch based algorithm. The patch based algorithm works as follows:

1. Take the input image.
We call the input image as source texture image. This image may be captured in a photograph or drawn by an artist to create synthesized texture image which is having similar appearance.

2. Create the blank image from the given input image.
The purpose of creating the blank image from the input image is that the blank image is going to act as workbench where the patches will be pasted at the end.

3. Divide the input image into no. of patches.
First the input image is divided into no. of patches. Each patch is having two areas

1. Kernal boundary
2. Region boundary

4. Generate the index table.
The index table stores the location information of source patch set SP in the synthetic texture. The index table allow us to access the synthetic texture and retrieve the source texture completely. While generating index table we need to provide the secret key for the authentication purpose.

5. Composition image generation.
In this module we construct synthesized image which is a combination of different patches. To construct the synthesized image, appropriate candidate patches must be selected from the patch list. To select the patch the index

table is referred which tells where to paste the in the blank image. The entries represented by green color in index table indicates the piece ID and tells the position where the pieces are pasted onto blank image.

6. Message oriented texture synthesis.
In this module we create stego synthetic texture image which conceals a secret message. To construct stego synthetic image first the message is converted into bytes and taken as input to message oriented texture synthesis process. Along with this source texture image andcomposition image is also taken as input to this process.

3. PROBLEM STATEMENT

To create synthesized stego texture image which conceals secret message by hiding converted bytes of data into an image patches and then storing these bytes by selecting appropriate candidate patch from the list of patches and then paste it onto a blank image.

4. PROPOSED SYSTEM

Experimental results have verifiable that our proposed algorithm can provide various numbers of insert capacities, produce a visually possible texture images, and recover the source texture. Proposed an image reversible data hiding algorithm which can recover the cover image without any misuse from the steganography image after the hidden data have been extracted.
We believe our proposed scheme offers considerable benefits and provides an opportunity to extend steganography applications.

Proposed System Algorithms:

A large number of image steganographic algorithms have been investigate with the increasing popularity and use of digital images.

Algorithm:

- Image steganographic algorithm
- pixel-based algorithm

Typical image steganography process reduces the image quality as if the size of secret message is large enough .So in the previous steganography technique it is expected that the size of the data must match the size of the image. If the size exceeds, it leads to image distortion.

Our proposed approach provides high quality image even if the size of the secret message is much large and reduces the image distortion.

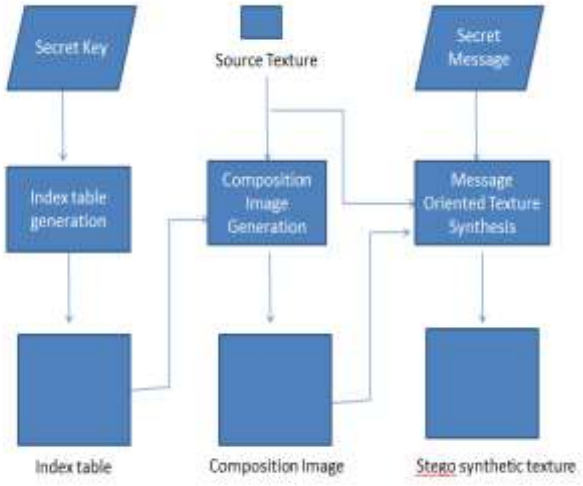

Figure 1.0: System Architecture.

5. MOTIVATION

Typical image steganography process reduces the image quality as if the size of secret message is large suitable. So in the existing steganography technique it is expected that the size of the data must match the size of the image. If the size exceeds, it leads to image distortion.

Our proposed approach provides high quality image even if the size of the secret message is much large and reduces the image distortion.

6. OBJECTIVE

Following are the modules to be developed:

1] Index table generation
Index table contains an entry for each patch and tells where to paste the patch onto the blank image.

2] Composition image generation
Image is composed of multiple patches. We select appropriate candidate patches and paste it onto blank image so to create synthesized image which is composition of multiple patches.

3] Message oriented texture synthesis
In this module we take converted bytes of secret message, source texture and composed image together to create stego synthesized texture image.

4] Stego synthetic texture
Finally we get the stego synthesized image which conceals secret message

7. CONCLISION

With the proposed system we can embed the size of the image and provide high quality image which avoids the distortion of image quality which the existing system can not..The proposed system is much more robust against any kind of attack and provide high degree of security to the confidential data hidden inside the image patches. The proposed system can be combined with other

steganographic systems to provide high degree of security. With this system the message can not be accessed by any person except the authorized person and who is having a secure key with him.

REFERENSES

[1] Kuo-Chen Wu and Chung-Ming Wang 'Steganography Using Reversible Texture Synthesis' IEEE Transactions on image processing vol: 24 no: 1 year 2015

[2]S.-C. Liu and W.-H.Tsai, "Line-based cubism-like image—A new type of art image and its application to lossless data hiding," *IEEE Trans. Inf.Forensics Security*, vol. 7, no. 5, pp. 1448-1458, 2012.

[3]H. Otori and S. Kuriyama, "Texture synthesis for mobile data communications," *IEEE Comput. Graph. Appl.*, vol. 29, no. 6, pp. 74-81,2009.

[4]H. Otori and S. Kuriyama, "Data-embeddable texture synthesis," in *Proc.of the 8th International Symposium on Smart Graphics*, Kyoto, Japan,2007, pp. 146-157.

[5]Y.-M. Cheng and C.-M.Wang, "A high-capacity steganographicapproachfor 3D polygonal meshes," *The Visual Computer*, vol. 22, no. 9, pp.845-855, 2006.

[6]Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 16, no. 3, pp. 354-362, 2006.

[7]N. Provos and P. Honeyman, "Hide and seek: an introduction to steganography," *Security &Privacy, IEEE*, vol. 1, no. 3, pp. 32-44, 2003.