CTM based Encryption in Steganography

Mohseena.AV  
PG Scholar,  
Department of Computer Science and Engineering  
Royal College of Engineering and Technology  
mohseenasina@gmail.com

Sneha.K  
Assistant Professor,  
Department of Computer Science and Engineering  
Royal College of Engineering and Technology  
snehanair88@gmail.com

Fepslin AthishMon  
Assistant Professor,  
Department of Computer Science and Engineering  
Royal College of Engineering and Technology  
fepslin@gmail.com

K. Suthendran  
Associate Professor  
Department of Information Technology  
Kalasalingam Academy of Research and Education  
k.suthendran@klu.ac.in

Abstract—Steganography is actually the art of hiding secret information within an image. The texture synthesis process re-samples smaller texture image, and which synthesizes a new texture image with a similar local appearance and an arbitrary size. And the process is used to conceal secret messages. This allows extracting the secret messages and source texture from a stego synthetic texture. In this proposing a novel image encryption scheme along with steganography. For this a combination of the rectangular transform and the CTM principle is used. This can improve the embedding capacity. This method will encrypt the three channels of the plain image. Further the key-sensitivity can be improved. The security of the proposed scheme can be verified by security analysis, and the results show that drawbacks of pure CTM-based schemes can be overcome.

Keywords—Steganograph; message embedding; Chaotic tent maps (CTM); Rectangular transform (RT)

I. INTRODUCTION

Steganography is a remarkable topic in the way of communication. One of the most important requirements of it is detectability; the concealed messages should be perfectly disguised. Steganography is the art and hiding messages which may be a text or audio or video within an image. The hiding process in a steganographic system done by identifying cover medium redundant bits. By replacing these redundant bits with data from the hidden message the embedding process creates a stego medium. After embedding the secret message into the cover-image, a stego image will be obtained. The file formats that can be used for steganography are: Text steganography, Image steganography, Audio steganography, and Protocol steganography.

The applications of Texture synthesis are computer vision, graphics, and image processing. The considerable thing is that Texture images are usually scanned photographs, and these photographs may be too small to cover the entire object surface. So, a simple tiling may introduce unacceptable artifacts in the forms of visible repetition. This problem is solved by generating textures of the desired sizes.

The texture synthesis process [1] of re-sampling a smaller texture image and synthesizing a new texture image with a similar local appearance and an arbitrary size. Secret messages are embedded through the process of texture synthesis. So that will allows to extract the secret messages and source texture from a stego synthetic texture.

In this work, an algorithm based on a rectangular transform (RT)-enhanced CTM system, has been proposed that can overcome the defects of the pure CTM-based scheme. This new scheme generates the key-streams they are not only related to the secret keys but the plain image. The secret keys are the same, the key-streams are different when different plain images are encrypted, so it can effectively resist the known plaintext attack (KPA) and also the chosen plaintext attack (CPA). So when encrypting colour images, it encrypts three channels of the plain image and these channel encryptions associate with each other. More security and robust can be get from these designs.

II. LITERATURE REVIEW

Steganography is the process of hiding secret message with in a larger image such a way that someone cannot know contents of the hidden message. The main purpose of steganography is making communication secure between two parties. In this work proposing the method of steganography using a reversible texture synthesis. This work provides three distinct advantages. First, the embedding capacity of the proposed system is proportional to the size of the stego texture image. Second, a steganalytic algorithm should failed to defeat this steganographic approach. Third, it is possible to recover the source texture by the help of reversible capability of texture synthesis. The main applications of the system include military area and banking.

Jessica Fridrich et al. [2] implemented the technique of Least Significant Bit embedding (LSB) for message hiding in 24-bit, 8-bit color images and grayscale images. It is based on the belief that changes to the LSBs of colors cannot be detected due to noise which is always present in digital images. In this paper, describing a new highly accurate and
A reliable method that can detect LSB embedding. They are randomly scattered pixels in both 24-bit color images and 8-bit grayscale or color images. It is based on lossless data embedding. By determining the differences in the number of regular and singular groups for both the LSB and the “shifted LSB plane”; it is possible to detect messages as short as 0.03bpp.

Qil Ke et al.[3] presents a new steganographic scheme for 3D point cloud models which makes use of using self-similarity partition. This scheme partitions the 3D point cloud model in to patches using self-similarity measures, and generates a codebook. From the codebook the representative patches and similar patches are taken out for every similar patch chain as the reference patches and the message patches. And finally, finding every message point in the similar image is synthesized based method of generating visual appearance. In this scheme the reference pixels are selected based on the distribution characteristics of the content of the image. The texture synthesis process provides reversible functionality. In this paper proposing a Reversible texture synthesis algorithm which produces good results for a wide range of textures. This paper demonstrates how an image can be re-rendered in the style of a different image. This method works directly on the images and it does not require 3D informations. Despite its simplicity, this method works well when applied to texture synthesis. Also the method allows to texture transfer in a general setting with some very promising results. The optimal boundary between the chosen candidate patch and the synthesized patch produces visually plausible patch stitching.

III. PROPOSED SYSTEM

In this paper proposing a Reversible texture synthesis process along with image encryption (fig.1). The reversible texture synthesis process provides reversible functionality. In order to embed the secret messages the method uses DCT embedding. But compared to other methods DCT has some disadvantages too. DCT has moderate Imperceptibility and less Capacity. So we have to improve the embedding capacity and the security of existing steganographic methods. For this security analysis of the pure CTM-based scheme [7] issued.

Here a combination of the rectangular transform and the CTM principle is proposed [8]. And it provides the functionality of encrypting the three channels of the plain image. And more message bits are embedded into detail subbands.

A. RT-ENHANCED CTM BASED ALGORITHM

I. ENCRYPTION ALGORITHM

- Step(1): Choose the secret keys, from the set{µi;xi0;a,b,c,d;rm,ri0;ti =1 ,2,3}, here µi and xi0 are the control parameters and initial values of the CTM system.
- Step (2): Read the colour plain image Pm×n×3
- Step(3): Stitch the three components to form a gray image.
- Step(4): Permute the gray image by for t rounds, and get a permuted image.
- Step(5): Split the permuted image into three matrices then further convert these three matrices to three 1D vectors.
- Step(6): Form three chaotic sequences of length N.
- Step(7): Calculate three key-streams.
- Step(8): Encrypt R,G,B to obtain their corresponding

Quilting is a fast and very simple texture synthesis algorithm which produces good results for a wide range of textures. This paper demonstrates how an image can be re-rendered in the style of a different image. This method works directly on the images and it does not require 3D informations. Despite its simplicity, this method works well when applied to texture synthesis. Also the method allows to texture transfer in a general setting with some very promising results. The optimal boundary between the chosen candidate patch and the synthesized patch produces visually plausible patch stitching.
II. DECRYPTION ALGORITHM

- Step(1): Receive the secret keys
- Step(2): Receive the colour cipher image
- Step(3): Form three chaotic sequences of length N.
- Step(4): Calculate three key-streams
- Step(5): Reshape the three matrices to three 1D-vectors
- Step(6): Inversely diffuse R0,G0,B0 and obtain three new vectors R,G,B
- Step(7): Reshape R,G,B to three matrices, then stitch the mix of original image
- Step(8): Inversely permute the gray image to obtain an un-permutated gray image
- Step(9): Split gray image into three matrices
- Step(10): Finally, the deciphered colour image

Here the key-streams are related to both the secret keys and the plain image. And the channel encryptions are associate with each other. And also it can resist the known and chosen plaintext attack. Each cipher text of plain image is related to its former cipher text. There are two main parts in the message embedding process:
- data embedding with CCE in spatial domain
- data embedding in Haar IWT domain

The preprocessing phase needs to be used to prevent the overflow/underflow. Along with the secret message location map, as side information, should be embedded into the cover image.

In the decryption phase (fig.2) the message is extracted using source texture, composition image and received stego synthetic texture.

IV. CONCLUSION

The steganographic algorithm using reversible texture synthesis is one of the best embedding techniques. But has some disadvantages too. In this an original source texture produces a large steo synthetic texture. The secret messages are embedded within this large steo synthetic texture. And one of the important advantages is that the system also provides the functionality of reversibility to retrieve the original source texture from a stego synthetic texture. In order to improve the capacity and security an image encryption scheme based on RT-enhanced CTM has been proposed. That can improve the embedding capacity of the image. Which encrypts the three channels of the plain image and further key-sensitivity can be improved. And also it can resist the known and chosen plain text attack.

REFERENCES


