REVERSIBLE TEXTURE COMBINATION STEGANOGRAPHY

Safna Sainudeen

Assistant Professor, Dept. of CSE, Toms College of Engineering , Kottayam , India

---

Abstract— *A sophisticated approach for steganography using texture recovery by reversibility technique is proposed, that is the texture combination synthesis .This technique subdivides the source image or cover image into patches and make variety of combinations of cover images called composition images. Generally the existing cover image is used for data hiding and finally the image in which data is hided will be discarded as it gets distorted naturally after stego synthesis and there by does not allow another round of steganography using the same cover image. Usually authentications are not provided with steganography as like in cryptography since steganography itself is more secure and protected from the attackers.*

Keywords—Steganography.Cover image,Texture combination synthesis,Stego Synthesis,Patches,Composition images.

1. INTRODUCTION

Steganography is the science of hiding information under digital media such as images like binary images, grayscale images and color images, audios or videos It is useful in confidential communications that requires secrecy such as military communications .Steganography is usually done by exploiting the natural features of images known as textures, which are normally used as cover images. In general data is hided inside the texture of an image, that means inside the cover image and the hided data can be recovered or retrieved at the destination successfully. But the texture in which data is hided will be discarded and thus cannot be retrieved and thus misses the chance of another round of steganography with the same cover image. This is a demerit and can overcome by using the method called texture combination synthesis which helps to subdivide the source textures accordingly .

In this approach of texture combination synthesis, the main focus is on synthesizing texture combinations from source images with maximum embedding capacity without compromising the image quality as cover images. The resultant image obtained after data hiding are called stego images and it naturally can possess image distortions. It adversely affects the features such as quality and capacity of cover images. This scheme deals with such problems effectively. The texture combination steganography subdivides the source texture into patches of desired size. That is the size of the source images is not fixed so that can embed datas of desired capacity. This approach helps to conceal source texture and embed the messages to be hided using reversible texture combinations, hence we can recover not only the cover image but also the secret message successfully for the the opportunity of another round of steganography.

In reversible texture combination synthesis process, patch based algorithms are used instead of pixel based algorithms for the creation of texture image. In patch based approaches patches are pasted to the target with small overlapping during synthesize process. The patches should not overlap with its neighboring patches .Patch stitching method like image quilting is used to create textures. At the same time authentications are provided with data embedding and data extraction makes the scheme secure and cannot be broken by the attackers. For making such a secured scheme it requires mainly three modules such as 'data embedding module', 'data extraction module' and an 'authentication module' for both embedding and extraction of datas with a result of source texture without any distortions. All the artifacts of secret messages and cover images are protected and they are visually similar without any degradation of embedding capacity and quality.

The paper can be organized in 4 sections. First section describes related works, second section describes proposed system, and third section describes solution methodology, fourth section describes the discussion of the paper and the last section deals with conclusion regarding the paper.

2. RELATED WORK

Here we are discussing some Steganographic techniques.

1. Data Embeddable Texture Synthesis

This work uses the method of feature learning of sample image. By using the method of feature learning of sample image, we can create or generate the texture of repetitive patterns and can embed arbitrary data, The synthesized image pattern can be used to conceal or embed the data patterns. The patterns can be perfectly captured from the photographs. Also we can use images scanned from original materials. The data hiding technique referred in this paper helps to protect copy rights or sending secret messages. [1]

2. Information Hiding – A Survey

This is one work that already done to understand the important possibilities of steganographic techniques that can be utilized at a maximum embedding capacities. The information hiding techniques have become very much popular in variety of fields including hospital fields ,military fields etc. Generally digital images, videos, audios etc are used as cover images in case of information hiding and they are encrypted. Also binary images, gray scale images, and color images are also become cover images for secret data embedding.

The attackers try to break the security if they get any clue so that most of the methods are not so safe from the attackers. Thus arise the importance of steganography. It deals with information hiding in more secure manner than any other information hiding techniques.[2]

3. Texture Synthesis for Mobile Data Communications

This paper proposes a data hiding method by the use of image coding method and utilizes the advantage of texture image synthesis. A mobile phone with digital camera is the input device for the purpose. The embedded data can be obtained pattern analysis of image code data. Image code data may be a two

dimensional bar code. Given a texture sample, pick out the dotted patterns and painted with colors, which have same features corresponding to embedded data. Then the texture synthesis process camouflages the pattern of dots which are painted. Thus this technique can be applied to mobile data communications. [3]

4. Video texture synthesis with multi-frame LBP-TOP and diffeomorphic growth model

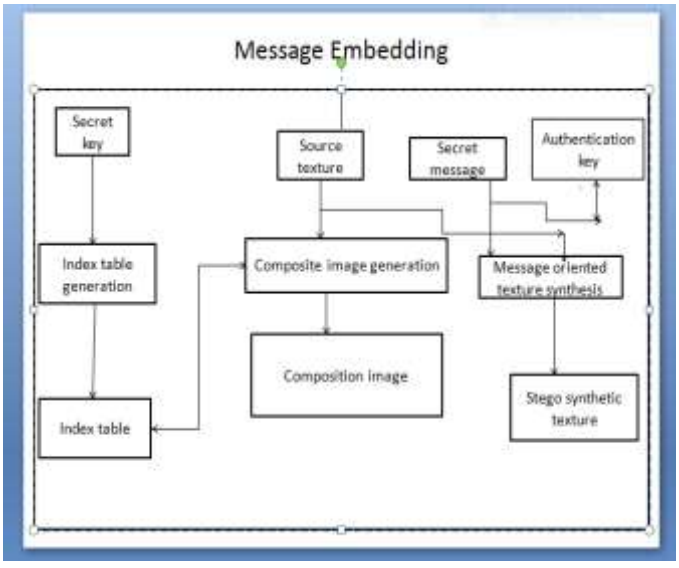
Video texture synthesis is an important approach that provides a stream of frames which are continuous and infinitely varying. It plays vital role in the field of computer applications especially in the field of graphics and animation. The perfect working of synthesis performance is a challenging task, the correct representation of effective frames for perfect image appearance and quality of the synthesis. There are two modules of video texture synthesis including video stitching and transition smoothing. The first module helps the creation of video flow that is infinite. The second module improves the quality and continuity of synthesis. [4]

5. *Exploring steganography: Seeing the unseen*

Steganography is the science or art of data hiding by the usage of digital medias such as images, audios, videos etc .Cryptography and steganography are somewhat related. Cryptography leads to message scrambling and cannot be identified so easily as they are encrypted and steganography leads to data hiding or message hiding and it cannot be seen. These makes the messages more secure from the attackers or eavesdroppers.[5]

3. PROPOSED SYSTEM

Here we are proposing a method which uses texture combination steganography for concealing secret or confidential messages and datas. Steganography combines with texture synthesis and authentication of secret messages are explained in this paper . The system mainly divided into different modules such as data embedding module, data extracting module, both with authentication modules for ensuring security. The following diagrams describe the architecture in more detail.



In **data embedding module** , three processes have to be done for secret data embedding.

A. Index table generation

An index table is created which gives location of source patch set that is in the synthetic texture .This created index table helps us to access the texture that is synthesized and allows us to recover the source texture from which cover image is created. Also the secret messages are authenticated using the authentication key.

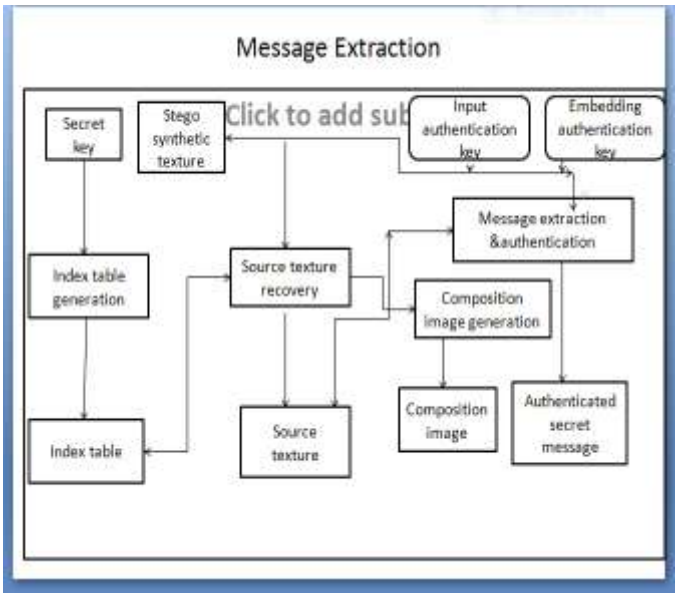
B. Patch composition

In the second process the source patches are pasted to a blank image, that is the workbench and thereby produce composition image. Firstly make a blank image which will be used as workbench for the pasting purpose of synthetic textures. The size of the workbench varies according to the size of synthetic texture. By using table that recorded the positions of source patches we can index the locations of source patches and paste the source patches on to the blank image or workbench directly. If overlapping of patches is found, it can be resolved by the use of image quilting technique. It helps to maintain the images that are visually plausible.

C. Message oriented texture synthesis with authentication

This process allows to embed the secret messages to the synthesized texture image or cover image by the use of index table and composition image.

Message extraction and authentication module will recover the source texture without compromise in embedding capacity and image quality. For the retrieval of cover image generate the index table to find out the locations where the patches are pasted and extract the secret message that is hided inside the stego synthetic texture. Authentications are done before the texture extraction process, in order to maintain security . That is to seek protection against steaganalytic attacks. Thus we can obtain the source texture without any degradation of images.



4. SOLUTION METHODOLOGY

Algorithm

1. Select the texture image which can be used as source image.
2. Create histogram of input image
3. Create index table corresponds to the number of patches in source image for getting location synthetic textures from the source image.
4. Create cover images using texture combination steganography.
5. a. If overlapping of patches is encountered, use image quilting process to resolve the problem and paste image to the workbench
5. b. If no overlapping of patches is encountered, directly paste image to the workbench
6. Hide secret messages in the synthetic textures using message oriented texture synthesis.
7. Composition image is generated.
8. The stego synthetic texture is authenticated with an authentication key.
9. Messages extracted based on the reference of index table and composition image.
10. Texture is recovered after verification of authentication key provided in step 6
11. Verify the histogram of input image and output for distortions.
12. Exit

Thus we can obtain texture recovery by reversibility method of texture synthesis.

5. DISCUSSION

The proposed system can give good quality of embedding and extraction of datas with source texture recovery compared to the previous ones. The relationship between size of source texture image and capacity is directly proportional will be one of the main problems we are facing in the earlier steganographic approaches. So we should have to use large textures as cover images in order to increase the capacity of embedding. In pixel based approach it is not so easy to maintain the size and capacity of images so patch based approach is preferred for the convenience. Generally authentication modules are not provided with steganography as steganography itself is secure against distortions. If we provide authentication stages in data embedding and extraction leads to obtaining double protection. Reversibility of texture combinations gives opportunities to reuse the source textures. Since we are not using existing cover images, protection will be far better than previous approaches of steganography.

6. CONCLUSION

In this paper, we have presented a secure steganographic approach that uses the process of texture combination steganography to conceal confidential datas, messages etc. Additionally we tried to give an authentication stages for data embedding and data extraction. The existing cover images not used as cover image and texture recovery is possible for reusing the source texture. Also maintains the embedding capacity and image quality is an added advantage.

REFERENCES

1. H. Otori and S. Kuriyama, “Data-embeddable texture synthesis,” in Proc.8th Int. Symp. Smart Graph., Kyoto, Japan, 2007, pp. 146–157.Anju E S and Manoj Kumar K V, “Malayalam to English Machine Translation: An EBMT System” vol. 2.2014, pp.18-23.

2. F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, “Information hidinga survey,” Proc. IEEE, vol. 87, no. 7, pp. 1062–1078, Jul. 19992009.

3. H. Otori and S. Kuriyama, “Texture synthesis for mobile data communications,”IEEE Comput. Graph. Appl., vol. 29, no. 6, pp. 74– 81,Nov./Dec. 2009.

4. Y. Guo, G. Zhao, Z. Zhou, and M. Pietikäinen, “Video texture synthesis with multi-frame LBP-TOP and diffeomorphic growth model,” IEEE Trans. Image Process., vol. 22, no. 10, pp. 3879–3891, Oct. 2013.

5. N. F. Johnson and S. Jajodia, “Exploring steganography: Seeing the unseen,” Computer, vol. 31, no. 2, pp. 26–34, 1998.