Steganography Methods For Hiding Information In Images

Ms. Swapnali Bhujbal[1], Prof. P.B. Sahane[2]
Department of Computer Engineering
[1]Research Scholar, PK Technical Campus, Pune, India,
[2]Assistant Professor , PK Technical Campus, Pune, India,

Abstract-*We invent a novel approach for steganography using a reversible texture synthesis. A texture synthesis process regenerates a smaller texture image, which synthesizes a new texture image with a similar local appearance and an any size. We set the texture synthesis process into steganography to conceal private messages. In contrast to using an existing cover image to hide information, our algorithm conceals the source texture image and embeds secret information through the process of texture synthesis. This allows us to extract the secret infomation and source texture from a stego synthetic texture. Our approach offers three distinct advantages. First, our scheme offers the embedding capacity that is proportional to the size of the stego texture image. Second, a steganalytic algorithm is not likely to defeat our steganographic approach. Third, the reversible capability inherited from our scheme provides functionality, which allows recovery of the source texture. Experimental results have verified that our proposed algorithm can provide various numbers of embedding capacities, produce a visually plausible texture images, and recover the source texture.*

Keywords*-*reversible, steganography, texture synthesis.

I. INTRODUCTION

In the most recent decade numerous advances have been made in the range of computerized media, and much concern has emerged with respect to steganography for computerized media. Steganography is a solitary system for data concealing strategies. It implants messages into a host medium keeping in mind the end goal to cover mystery messages so as not to excite suspicion by a meddler. A normal steganographic application incorporates secretive correspondences between two gatherings whose presence is obscure to a conceivable assailant and whose achievement relies on upon identifying the presence of this correspondence. When all is said in done, the host medium utilized as a part of steganography incorporates significant advanced media, for example, computerized picture, content, sound, video, 3D model, and so forth. Countless steganographic calculations have been researched with the expanding notoriety and utilization of advanced pictures. Most image steganographic calculations receive a current picture as a spread medium. The cost of installing mystery messages into this spread picture is the picture bending experienced in the stego picture. This prompts two disadvantages. To begin with, since the span of the spread picture is settled, the more mystery messages which are inserted take into account more picture twisting. Hence, a bargain must be came to between the inserting limit and the picture quality which brings about the constrained limit gave in any particular spread picture. Review that picture steganalysis is a methodology used to distinguish mystery messages covered up in the stego image[2]. A stego image contains some twisting, and paying little respect to how minute it is, this will meddle with the regular elements of the spread picture. This prompts the second disadvantage on the grounds that it is still conceivable that a picture steganalytic calculation can crush the picture steganography and in this way uncover a concealed message is being passed on in a stego image.

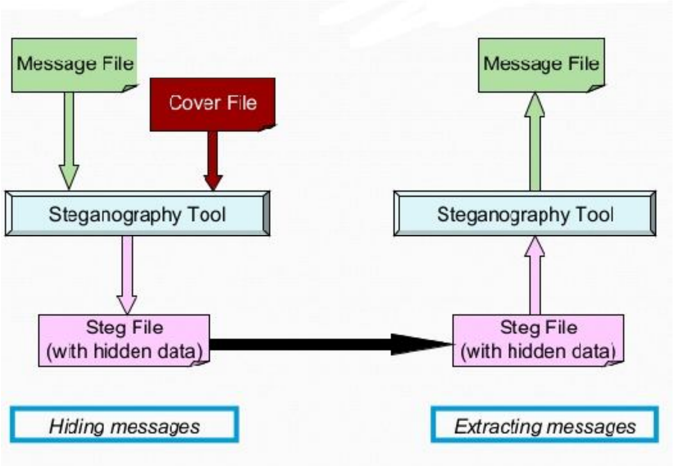
Most image steganographic algorithms take an existing image as a cover . The expense of embedding secret information into this cover image is the image distortion encountered in the stego image. This leads to two drawbacks. First, since the size of the cover image is fixed, the more secret messages which are embedded allow for more image distortion. Consequently, a compromise must be reached between the embedding capacity and the image quality which results in the limited capacity provided in any specific cover image. Recall that image steganalysis is an approach used to detect secret messages hidden in the stego image. A stego image contains some distortion, and regardless of how minute it is, this will interfere with the natural features of the cover image. This leads to the second drawback because it is still possible that an image steganalytic algorithm can defeat the image steganography and thus reveal that a hidden message is being conveyed in a stego image.

This approach have three main advantages.

1. Preliminary process of synthesizing the texture image of an arbitory 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.



II. BACKGROUND

A. Liturature survey

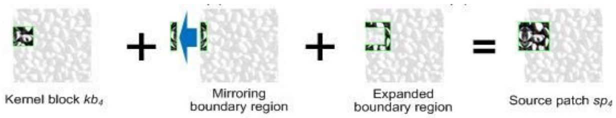
Texture synthesis has received a lot of attention recently in computer vision and computer graphics [8]. The most recent work has focused on texture synthesis by example, in which a source texture image is re-sampled using either pixel-based or patch- based algorithms to produce a new synthesized texture image with similar local appearance and arbitrary size.

Pixel-based algorithms [9], [10], [11] generate the synthesized image pixel by pixel and use spatial neighborhood comparisons to choose the most similar pixel in a sample texture as the output pixel. Since each output pixel is determined by the already synthesized pixels, any wrongly synthesized pixels during the process influence the rest of the result causing propagation of errors.

Texture synthesis has attained a lot of heeds presently in computer vision and computer graphics[1].Most of the present work has concentrated on texture synthesis for example, in which a source texture image is re-sampled using either pixel-based or patch-based algorithms to create a new synthesized texture image with similar appearance and variable size. Pixel-based algorithms create the generated image pixel by pixel and use spatial neighborhood comparisons to select the most closely related pixel in a sample texture as the output pixel. Since each output pixel is identified by the already generated pixels, any wrongly generated pixels during the process influence the rest of the result causing propagation of errors.

The work of integrating data coding using pixelbased texture synthesis. Secret messages to be hided are encoded into colored dotted patterns and they are directly painted on a blank image. A pixel-based algorithm tunic the rest of the pixels by the pixel-based texture synthesis method, thus masking the existence of dotted patterns. To withdraw messages the printout of the stego synthesized texture image is photographed before applying the datadetecting technique. The capacity given by the method of Otori and Kuriyama depends on the number of the dotted patterns. However, their method has a small error rate of the message extraction[4].

To the best of our knowledge, we were unable to disclose any literature that related patch-based texture synthesis with steganography. In this paper, we present our work which takes advantage of the patch-based methods to embed a secret message during the synthesizing procedure. This allows the source texture to be recovered in a message extracting procedure[4], providing the functionality of reversibility. We detail our method in the next section.see the following fig.



B. Objective

A typical steganographic application includes covert communications between two parties whose existence is unknown to a possible attacker and whose success depends on detecting the existence of this communication. Most image steganographic algorithms adopt an existing image as a cover medium. The expense of embedding secret messages into this cover image is the image distortion encountered in the stego image. In recent work, the pixel based approach is used. In the pixel based approach, first the blank image is constructed from the given input image and the secret message to conceal is encoded onto that blank image by glowing appropriate pixels. Remaining pixels are coated as it is based on the input image. With this technique we can hide the data upto large extent. The capacity provided by the method depends on the number of the dotted patterns.

C. Motivation

Typical image steganography process reduces the image quality as if the size of secret message is large enough

.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.

Most image steganographic algorithms adopt an existing image as a cover medium. The expense of embedding secret messages into this cover image is the image distortion encountered in the stego image. This leads to two drawbacks. First, since the size of the cover image is fixed, the more secret messages which are embedded allow for more image distortion. Consequently a compromise must be reached between the embedding capacity and the image quality which results in the capacity provided in any specific cover image. Recall that image steganalysis is an approach used to detect secret messages hidden in the stego image. A stego image contains some distortion, and regardless of how minute it is, this will interfere with the natural features of the cover image. This leads to the second drawback because it is still possible that an image steganalytic algorithm can defeat the image steganography and thus reveal that a hidden message is being conveyed in a stego image.

D. 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.

III. METHODOLOGY

The proposed steganography process uses the patch based algorithm. The patch based algorithm

1. Take the input image:- We call the input image as source texture image. This image maybe 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
   _ Kernal boundary
   _ 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 allows 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.

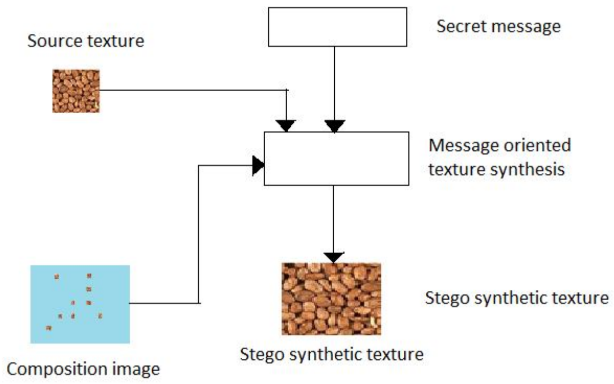


Fig. Generation of Stego synthetic image

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 patch ID and tells the position where the patches 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 and composition image is also taken as input to this process.

IV. PROPOSED SYSTEM

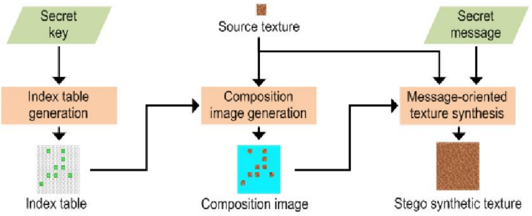


Fig.Compression image

We illustrate our proposed method in this section. First, we will define some basic terminology to be used in our algorithm[5]. The basic unit used for our steganographic texture synthesis is referred to as a "patch." A patch represents an image block of a source texture where its size is user-specified. We can denote the size of a patch by its width (P_w) and height (P_h). A patch contains the central part and an outer part where the central part is referred to as the kernel region with size of $K_w \times K_h$, and the part surrounding the kernel region is referred to as the boundary region with the depth (P_d).

Next, we describe the concept of the kernel block. Given a source texture with the size of $S_w \times S_h$ we can subdivide the source texture[6] into a number of non-overlapped kernel blocks, each of which has the size of $K_w \times K_h$,. Let *KB* represent the collection of all kernel blocks thus generated,and $\|KB\|$ represent the number of elements in this set. We can employ the indexing for each source patch kb_i, i.e., $KB=\{kb_i|\ i = 0$ to $\|KB\|-1\}$. As an example, given a source texture with the size of $S_w \times S_h$ =128×128, if we set the size $K_w \times K_h$ as 32×32, then we can generate $\|KB\|$=16 kernel blocks. Each element in *KB*our steganographic texture synthesis algorithm[2] needs to generate candidate patches when synthesizing synthetic texture. The concept of a candidate patch is trivial: we employ a window $P_w \times P_h$and then travel the source texture ($S_w \times S_h$) by shifting apixel each time following the scan-line order. Let $CP=\{cp_i|i=0, 1, \ldots, CP_n-1\}$ represent the set of the candidate patches where $CP_n=\|CP\|$ denotes the number of elements in *CP*. We canderive CP_n using (2).

When generating a candidate patch[3], we need to ensure that each candidate patch is unique; otherwise, we may extract an incorrect secret message. In our implementation, we employ a flag mechanism. We first check whether the original source texture has any duplicate candidate patches. For a duplicate candidate patch, we set the flag on for the first one. For the rest of the duplicate candidate patches we set the flag off to ensure the uniqueness of the candidate patch in the candidate list.

V. MATHEMATICAL MODULE

A. Relation and Function

Let S be a Steganography of the image and it is mathematically represented as, S = f s, e, X,
Y,F_{me}, DD, NDD, ; g

Where,
s set of Initial State s= fs0, s1, s2,...g
s0=Wait State
s1= Accept Request State s2= Process Request State
s3= Return Request State for the system
E is End State e0 i.e. last state of execution.

X stands for Input. In our System, the input is the data sent by user bounded with the image.

Y is Output. OutPut of our system is the secured massage inside the image.

F_{me} is the exact algorithm of system. In the proposed system there are two algorithms Encryption and Decryption Algorithm

DD is deterministic Data i.e. number of instructions or space complexity of system. Space required for the system is nothing but the space required to store number of instructions. The number of instruction will be assumed as 2.1 KLOC specified in section 3.7.1

NDD is Non-deterministic Data i.e. the time required for the execution of system. In other words Time complexity. Failure or success of system. Success is the desired output of the system means the information is secured bby using the images for hiding information which minimizes the computation overhead and communication delay. Failure means if the system is not giving one of the desired output.

VI. CONCLUSION

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/her.

One possible future study is to expand our scheme to support other kinds of texture synthesis approaches to improve the image quality of the synthetic textures. Another possible study would be to combine other steganography approaches to increase the embedding capacities.

REFERENCES

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

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

[3] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, “Information hiding-a survey,” Proceedings of the IEEE, vol. 87, no. 7, pp. 1062-1078, 1999.

[4] Y.-M. Cheng and C.-M. Wang, “A high-capacity steganographic approach for 3D polygonal meshes,” The Visual Computer, vol. 22, no. 9, pp. 845-855, 2006.

[5] 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.

[6] I.-C. Dragoi and D. Coltuc, “Local-prediction-based difference expansion reversible watermarking,” IEEE Trans. Image Process., vol. 23, no. 4, pp. 1779-1790, 2014.

[7] J. Fridrich, M. Goljan, and R. Du, “Detecting LSB steganography in color, and gray-scale images,” MultiMedia, IEEE, vol. 8, no. 4, pp. 22-28, 2001.

[8] 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, 2013.

[9] 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.

[10] A. A. Efros and T. K. Leung, “Texture synthesis by non-parametric sampling,” in Proc. of the Seventh IEEE International Conference.

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

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

[13] S.-C. Liu and W.-H. Tsai, Line-based cubism-like imageA 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.

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

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