IPHV8I2002X
International Journal Of Advanced Research and Innovation -Vol.8, Issue .I
ISSN Online: 2319 – 9253
Print: 2319 – 9245

A HIGH CAPACITY STEGANOGRAPHY APPROACH FOR DATA EMBEDDABLE TEXTURE SYNTHESIS

[#1]CHITYALA SRAVANI, M.Tech Student,
[#2]A.SRINISH REDDY, Assistant Professor,
Department Of CSE,
SREE CHAITANYA INSTITUTE OF TECHNOLOGICAL SCIENCES,KARIMNAGAR,T.S, INDIA.

ABSTRACT-A major necessity for any steganography method is to decrease the changes happening in the cover image by the data embedding process. The project proposes a unique way for steganography using a reversible texture synthesis based on edge adaptive and tree based parity check methods to improve the embedding capacity. This approach offers three distinct advantages. First, the 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 this stegnographic approach. Third the reversible capability inherited here provides functionality, which allows recovery of source texture.

Keywords: *Data embedding, Reversible texture synthesis, Tree based parity check (TBPC)*

I.INTRODUCTION

Steganography is the method of hiding a message, file, image, or video within another file, message, image, or video. The word steganography combines from the two Greek words “steganos” means “protected”, and “grapheins” means “writing”. The advantage of steganography than cryptography is that the secret message does not attract the attention of the attackers by simple observation. The cryptography protects only the content of the message, while steganography protects the both messages and communication environment. In most of the image steganographic methods, uses the existing image as their cover medium. This leads to two drawbacks. Since the size of the cover image is fixed, embedding a large secret message will results in the distortion of the image. Thus a compromise should be made between the size of the image and the embedding capacity to improve the quality of the cover image. The distortion of the image results in second drawback, because it is feasible that a steganalytic algorithm can defeat the image steganography and thus reveal that a hidden message is conveyed in a stego image. The paper will proposes a good approach for steganography using reversible texture synthesis based on edge adaptive and tree based parity check to improve the embedding capacity. A texture synthesis process is of creating a big digital image with a similar local appearance of the original image and has an arbitrary size. And the paper is also using another two methods named edge adaptive and tree based parity check to improve the embedding capacity. The paper fabricates the texture synthesis process into steganography concealing secret messages as well as the source texture. In particular, in contrast to using an existing cover image to hide messages, our algorithm conceals the source texture image and embeds the secret messages through the process of texture synthesis. This allows us to extract the secret messages and the source texture from a stego synthetic texture. The proposed approach offers three advantages. First, since the texture synthesis can synthesize an arbitrary size of texture images. Since the Human Visual System (HVS) is less sensitive to changes in sharp regions compared to smooth regions, edge adaptive methods has been proposed to find the edge regions and hence improve the quality of the stego image as well as improve the embedding capacity and TBPC to hide the secret data into the cover image. Secondly, a steganalytic algorithm is not to defeat the steganographic approach since the texture image is composed of a source texture rather than by changing the existing image contents. Third, the reversible capability used in the project results in the recovery of the source texture so that the same texture can be used for the second round of message redirect.

First, it limits the capacity of embedding message because it gives result as image distortion. So the embedding capacity and quality of cover image is reduced. Second, it is possible to reveal the hidden message in a stego image by using any image stegnalitic algorithm. This paper contain a texture synthesis process to re-samples a small texture image which may be captured or drawn to generate a new texture image with an arbitrary size and similar appearance .To hide source texture and secret messages it introduce a new technique in steganography called as texture synthesis process. In process of texture synthesis instead of using cover image to hide secrete message, this algorithm use texture synthesis to embed message and hide source texture. First, it creates a stego image from source texture which gives the advantage of reversibility. This approach has three advantages. First, though the texture synthesis provides the ability to synthesize texture images of arbitrary size, the embedding capacity is become proportional to the stego texture image size. Secondly, steganography approach

unable to defeat by the steganalytic algorithm because instead of modifying the contents of existing image this approach compose the stego texture image from source texture. Third, to recover the original source texture this scheme offers the capability called reversibility. The reversibility technique generates the exactly similar and visually plausible source texture image to the original texture give opportunity to apply second round of steganography for more secrecy of the message. Steganography is the practice of concealing a file, message, image or a video within another file, message, image or a video. It is a science of hiding in formations, necessary for secure communication over an insecure network or channel ,namely privacy, confidentiality, key exchange, authentication and non repudiation. The goal of cryptography is to make data unreadable by a third party. There are many ways for hiding information such as using a covert medium, hiding texts within web pages, using ciphers etc..,One of the most widely used method is Digital Watermarking. In our paper we use retrieving the secret information from a source image. Communications between two parties whose existence is unknown to a possible attacker and whose success depends on detecting the existence of this communication. In general, the host medium used in steganography includes meaningful digital media such as digital image, text, audio, video, 3Dmodel etc. A texture synthesis process re-samples a smaller texture image which synthesizes a new texture image with a similar local appearance. In contrast to using an existing cover image to hide messages, our algorithm conceals the source texture image and embeds secret messages through the process of texture synthesis. It involves hiding the information within infinite number of patches. 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. No significant visual difference exists between the two stego synthetic textures and the pure synthetic texture.

Steganalysis [1] is the reverse process of steganography. The aim of steganalysis process is to break steganography systems. The steganography process starts with a set of suspected information streams. Then the set is reduced with the help of advanced statistical methods. The three main types of steganalysis are

(i) visual detection steganlysis:- a set of stego images are compared with original cover images and note the visible difference.

(ii) Statistical detection steganalysis:- are powerful and successful because they reveal the smallest alterations in an images. This attack is further classified as passive and active attacks. Passive attack deal with identifying the presence or absence of a covert message or the embedding algorithm used etc. whereas the active attacks is to estimate the embedded message length or the locations of the hidden message or the secret key used in embedding.

(iii) structural attacks are based on fact that format of the data files often changes as data to be hidden are embedded, on identifying these characteristic structure changes can detect the existence of image.

Applications of steganography are confidential communication and secret data storing, copyright protection of electronic products, Bank Transactions, Healthcare information, Internet security, Authentication and Information assurance etc. Motivation: Due to increasing demand for privacy and security, a need of various data hiding techniques which lead to the development of several techniques for embedding and extraction. Steganography is powerful method of embedding secret information for covert communication. Contribution: In this paper non embedding steganography using average technique in transform domain is proposed. The new concept of average value of matrix obtained using division of PA by CD is used to generate stego image. The quality of stego image is improved by using different values of NETV. Organization: This paper is organized into following sections. Section 2 is an overview of related work. The steganography definitions, proposed embedding model and extraction model are described in section 3. Section 4 discusses the algorithm used for embedding and extraction. In section 5 Performance analysis is discussed and conclusion future work is discussed in section 6.

II. RELATED WORKS

Texture analysis: how to capture the essence of texture? Need to model the whole spectrum: from repeated to stochastic texture. This problem is at intersection of vision, graphics, statistics, and image compression .Some Previous Work–multi-scale filter response histogram matching[11] [Heeger and Bergen,'95]–sampling from conditional distribution over multiple scales [DeBonet,'97]–filter histograms with Gibbs sampling [Zhu et al,'98]– matching 1st and 2nd order properties of wavelet coefficients [Simoncelli and Portilla,'98]–N-gram language model [Shannon,'48]–clustering pixel neighborhood densities [Popat and Picard,'93].Our Approach.[1]Our goals:–preserve local structure–model wide range of real textures–ability to do constrained synthesis. Our method:-Texture is ―grown‖ one pixel at a time–conditional pdf of pixel given its neighbors synthesized thus far is computed directly from the sample image A Novel method of Steganography to

achieve Reversible Data Hiding (RDH)[10] is proposed using Histogram Modification (HM). In paper the HM technique is revisited and a general framework to construct HM-based RDH is presented by simply designing the shifting and embedding functions on the cover image. The Secret Image is embedded inside the cover image using several steps of specific shifting of pixels with an order. The secret image or logo is retrieved without any loss in data on the cover and as well as in the secrete image. The Experimental results show the better Peak Signal to Noise Ratio (PSNR) with the existing methods. This paper investigates the effectiveness of prediction-error expansion reversible watermarking on textured images[6].Five well performing reversible watermarking schemes are considered, namely the schemes based on the rhombus average, the adaptive rhombus predictor, the full context predictor as a weighted average between the rhombus and the four diagonal neighbors, the global least-squares predictor and its recently proposed local counterpart. The textured images are analyzed and the optimal prediction scheme for each texture type is determined. The local least-squares prediction based scheme provides the best overall results.

Narasimmalou and joseph [19] proposed image data hiding technique based on discrete wavelet transform. Two different hiding techniques are implemented namely (i) three level wavelet decomposition taking a single plane of the cover image for embedding and processing the image as 4x4 blocks with swapping. (ii) Single level wavelet decomposition. Prabhakar and Bhavani [20] proposed a modified secure and high capacity based steganography method of hiding a large size secret image into a small size cover image. Arnold transformation is performed to scramble the secret image. DWT is applied followed by alpha blending operation. Banoci et al., [21] presented a steganographic method for embedding of secret data in still gray scale JPEG image. The embedding is performed in DCT domain in JPEG file. The method uses modulo operator to achieve characteristics of blind steganography system. The secret message is encrypted by advanced encryption standard Ciphering. Nadeem Akhtar et al., [22] implemented a LSB based image steganography. The bit inversion is applied on stegoimage which is obtaining by LSB technique. The steganography quality is improved using bit inversion technique, particular pattern of some bits of the cover image pixels are inverted to reduce the number of cover image pixel modification. The bit patterns for which LSB's has inverted is stored within the stego image. Nadeem Akhtar et al., [23] presented a data hiding based on a module – based substitution method. Modulus and shifting operations with compression logic is used for hiding secret data. Secret data may be text, image or audio file. IndradiP Banerjee et al., [24] proposed a frequency domain image steganography in 4 bit pixel factor mapping method using DCT coefficients. DCT coefficient value for embedding the secret data is selected using pixel selection algorithm. Gabriel Bugar et al., [25] designed a steganography method that uses the properties of Harr transformer coefficients. The secret message is compressed before embedding into cover image to improve capacity. The blind steganography methods do not require an original image in the process of extraction. Bin Li et al., [26] proposed the process of cost assignment in spatial image steganography. The two phases are (i) determining a priority profile and (ii) specifying a cost value distribution. The cost value distribution determines the change rate of cover elements, when the cost values are specified to follow a uniform distribution, the change rate has a linear relation with the payload, which is a rate property for content – adaptive steganography. Kodovsky and Fridrich [27] presented a paper on how the detectability of embedding changes is affected when the cover image is down samled prior to embedding. The down scaled images are used for steganography, since down sampling changes the strength and character aof dependencies among adjacent image pixels. It also affects steganalysis. The lower image resolution decreases the strength of pixel dependencies due to more rapid changes in the image content. Depending on the image down sampling algorithm the strength of pixel dependencies may increase due to interpolation (averaging). Kuo Chen Wu and Chung – Ming Wang [28] proposed a steganography method using a reversible texture synthesis. The source texture image embds secret messages into cover image through the process of texture synthesis. A texture synthesis process resamples a smaller texture image, whoch synthesizes a new texture image with a similar loca; appearance and an arbitrary size.

III. PROPOSED WORK

We propose a novel approach for steganography using reversible texture synthesis A texture synthesis process resamples a small texture image and provides an image of arbitrary size and shape, which holds the hidden message. It involves generation of an index table with a desirable number of rows and columns. The index table is split into given number of rows and columns and the secret message is hidden in any of the column or row according to the sender's choice. Then the image is merged into its original form with a merging file name. The image will only be sent to the list of available users, that is the users with valid username and registered users. At the receiver end, the receiver, for whom the message is intended will receive it in their inbox. As the splitting procedure is only revealed to the registered user, they split the merged image using secret key and read the message. First, we will define some basic terminology to be used in our algorithm. The basic unit used for our steganographic texture synthesis is referred to as a

—patch.‖ We illustrate our proposed method in this section. First, we will define some basic terminology to be used in our algorithm.

IV. METHODOLOGY

The proposed method is described as follows. The basic unit of the steganographic texture synthesis is introduced to as a "patch." A patch represents an image block of a source texture where its size is user-specified. The patches are combined together to form the composition image in which we are embedding our secret message. The project includes mainly three major steps.

1) Message Embedding Procedure
2) Source Texture Recovery, Message Extraction and Message Authentication Procedure
3) Capacity Determination

1. Concepts involved in Message Embedding Procedure

The message embedding procedure involves mainly four steps. They are

A) Index Table Generation
B. Patch Composition Process
C. Combined TBPC and Edge Adaptive Process
D. Message Oriented Texture Synthesis Generation.

A. Index Table Generation

The first process of this project is the index table generation where here will create an index table to preserve the location of the source patch set inside the synthetic texture. The index table will allow us to access the synthetic texture and extract the source texture wholly. The texture of any size according to our wish can be generated using this index table.

B. Patch Based Composition

The second step that has to be used in this project is to attach the source patches into a workbench to create a composition image. First here will set up an empty image as the workbench where the size of the workbench is proportional to the synthetic texture. By referring to the source patch IDs stored in the index table, we then attach the source patches into the workbench. During the attaching process, if no imbrications of the source patches are found, we can attach the source patches directly into the workbench.

C. Combined TBPC and Edge Adaptive Process

Embedding capacity is one of the most important requirements for steganography methods, and it is important for steganography process not to leave any noticeable traceable to the human eyes after hiding the secret data. Here will give a hybrid image steganography method that combines edge adaptive and TBPC methods together. The proposed method exploits the high contrast regions of an image as embedding locations. It is known that human eyes cannot discover modifications in the edge areas since they can do in smooth areas. Therefore, the number of hidden bits is on the basis of the variation value between the two pixels of each block. The integration of TBPC leads to a better embedding capacity. Thus, the proposed method mixes up the strengths of edge adaptive and TBPC.

D. Message Oriented Texture Synthesis Generation.

After the creation of the composition image we have to embed the secret message through the message oriented texture synthesis to generate the final steno synthetic texture.

2. Concept Involved In Source

Texture Recovery, Message Extraction, and Message Authentication Procedure The message extracted for the receiver side consist of creating the index table, attaining the source texture, performing the texture synthesis, and extracting and authenticating the secret message hidden inside the stego synthetic texture.

3. Capacity Determination.

The next step is to look for how much data can be embedded in the stego texture image. The embedding capacity can be related to the capacity in bits that can be hidden at each patch(BPP, bit per patch), and to the number of embeddable patches in the stego synthetic texture (EPn). Each patch can hide at least one bit of the secret message.

$TC = BPP \times EPn = BPP \times (TPn - SPn)$

V. STEGANOGRAPHY USING REVERSIBLE TEXTURE SYNTHESIS

The method of steganography using reversible texture synthesis is mainly used for hide the secret messages. A new texture image is synthesizes from several tiny texture images by using the texture synthesis process. The method consists of combination of both texture synthesis process and stegonography. It contains mainly two procedures [1]. 1: Message embedding procedure 2: Message extracting procedure In message embedding procedure, the first procedure is dividing the source texture image into different image block. This image block is called as patches. To record the corresponding source patch's location the index table is used. The workbench is blank image whose size is same as that of synthetic texture. With the help of source patch ID which is placed in the index table, the corresponding source patches are paste into the workbench to generate a composite image. After pasting the source patch the next step is to find mean square error (MSE) of overlapped region. This overlapped area is found in between the patch which we want to insert in the workbench and the synthesis area. The resultant patches are ranked as per the ascending order of mean square error (MSE). And finally the patches are selected from given list in such way that the rank of patches is equals to decimal value. The decimal value is nothing but the n-bit value of our secret message.

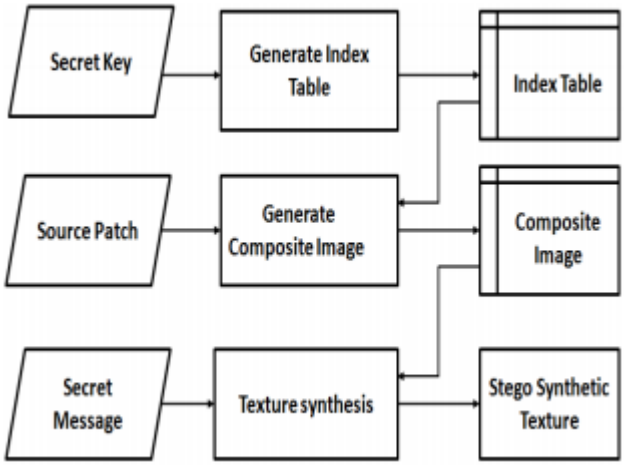

Fig 5: Message embedding procedure

At receiver side, the index table is generated by using secrete key which the receiver already have. To retrieve the size of the expected source texture we can refer each patch region and its related order which is present in the index table. After retrieving the size the blocks are arranged as per their corresponding order. Next step is authentication - We were going to suppose the present working location of workbench and similarly the working location of stego synthetic texture to predict the stego block region. The stego block region is used to search candidate list and to check whether there is any patch from candidate list having similar kernel region as the corresponding stego block region. If such similar patch is found, The rank is given to this matched patch. We can represent the value of secrete bits in patch which is in decimal format. This process is called as message extracting procedure.

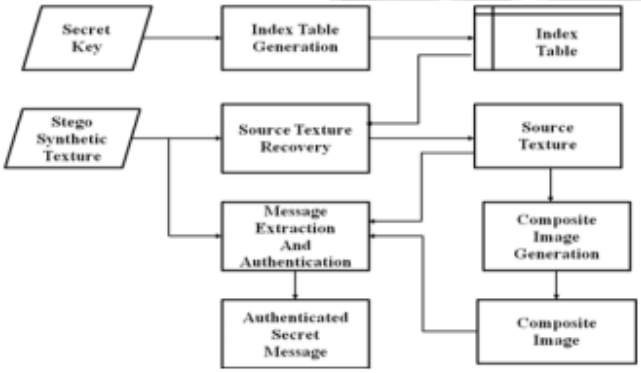

Fig 6: Message extracting procedure.

VI. CONCLUSION

In this way we contemplate few techniques which are meant for texture synthesis. Some of the technique use patches and synthesis information into that patches, another technique uses exemplar graph which contain infinite resolution which give benefits to the larger information synthesis into texture like spatial images. But there is also some drawback like chances of multiple time processing of same exemplar. Therefore approach proposed by Kuo-Chen Wu and Chung-Ming Wang have additional capabilities like reversibility to extract the original image from given stego texture. We can also apply another round of synthesis of source texture. The image recovery is possible by using this approach.

REFERENCES

[1] Kuo- Chen Wu and Chung-Ming Wang, “Steganography Using Reversible Texture Synthesis”, IEEE Transaction On Image Processing ,vol.24,no.1,pp.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] 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.

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

[5] M. F. Cohen, J. Shade, S. Hiller, and O. Deussen, “Wang Tiles for image and texture generation,” ACM Trans. Graph., vol 22, no. 3,pp 287-294,2003.

[6] K. Xu, D. Cohen-Or, T. Ju, L. Liu, H. Zhang, S. Zhou, and Y. Xiong, “Feature-aligned shape texturing,” ACM Trans. Graph., vol.28, no.5, pp.1-7-2009.

[7] J. Fridrich, M. Goljan, and R. Du, ―Detecting LSB steganography in color, and gray-scale images,‖ IEEE MultiMedia, vol. 8, no. 4,pp. 22–28, Oct./Dec. 2001.

[8] Y. Guo, G. Zhao, Z. Zhou, and M. Pietikäinen, ―Video texture synthesis with multi-frame LBP-TOP and diffeomorphic growth model,‖ IEEETrans. Image Process., vol. 22, no. 10, pp. 3879–3891, Oct. 2013.

[9] L.-Y. Wei and M. Levoy, ―Fast texture synthesis using tree-structured vector quantization,‖ in Proc. 27th Annu. Conf. Comput. Graph. Interact. Techn. 2000, pp. 479–488.

[10] A. A. Efros and T. K. Leung, ―Texture synthesis by non-parametricsampling,‖ in Proc. 7th IEEE Int. Conf. Comput. Vis., Sep. 1999,pp. 1033–1038.

[11] C. Han, E. Risser, R. Ramamoorthi, and E. Grinspun, ―Multiscaletexturesynthesis,‖ ACM Trans. Graph., vol. 27, no. 3, 2008, Art. ID 51.

[12] H. Otori and S. Kuriyama, ―Data-embeddable texture synthesis,‖ in Proc.8th Int. Symp. Smart Graph. Kyoto, Japan, 2007, pp. 146–157.

[13]Suhasni,M.O.Ramkumar,Image Re-Ranking for websearch al,International Journal of Computer Science and Mobile Computing, Vol.4 Issue.3, March-2015