ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

Enhancement of Embedding Capacity in Steganography

Reddy Yogita[1], Balajee Maram[2]

MTech II year, Department of CSE, GMR Institute of Technology, RAJAM, Andhra Pradesh, India

Sr. Assistant Professor, Department of CSE, GMR Institute of Technology, RAJAM, Andhra Pradesh, India

ABSTRACT: Reversible texture synthesis is a new stenographic method proposed in this paper.A reversibletexture synthesis, it is a process of resamples a smaller texture image, which synthesizes a new texture image with a similar local appearance and an arbitrary size. Reversible texture based technique, to protect the information against eaves droppers. In steganographywe weave the texture synthesis process to obscure secret messages**.** To hidemessages, using an existing cover image. The process of texture synthesis conceals the source texture imageandembeds secret messages.Texture synthesis to extract the secret messages and source texture from a stego image. This project exploits the high contrast regions of an image as embedding locations. The modificationin the edgeareas cannot discover by human eyes, since they can do in smooth areas is known. The integration of TWPCleadsto a better embedding capacity. Thus, this paper shows the strengths of edge adaptive and TWPC.

KEYWORDS: Steganography, RDH, Data embedding, Reversible data hiding, Texture synthesis

I. INTRODUCTION

In today's world the data security is main apprehension .So, the different data security techniques are cryptography, steganography etc. steganography techniques are used by most of the, organizations, governments, military, business, private citizens for security purpose. Steganography, it is the technique of concealing the data into some other data or image. By using steganography techniques, if we are transfer data, it would become difficult to know the go-between user that the secret data is hidden in the appearing image or data. Steganography techniques are used in music, movie for remarking early distribution of screenings. For communication the internet becomes prime factor and recently cybercrime increases exponentially so to avoid those computer scientific techniques are used [1].
In steganography most of the, algorithms takes original image as cover image, which it is expense of embedding secrete messages into cover image that indicates to the image distortion of produced stego image [2].].Hiding a message in one median and then again hide it another median increases the complexity and make more deceptive to third party and it improves the protection level of new data [3]. The enactment of steganographic technique is needed to enhance the level of security of data which leads us to develop new algorithms with tough security, capability and imperceptibility [4].In steganography the most popular objects are images, there are two groups of image steganography techniques, and are divided first spatial domain and second transform domain [5].Appropriate cover image is selected to hoard the secret message. The cover image should not exist on websites because stalkers can easily compare the created stego image and cover image [6]. The digital image is group of data about pixels. The images are huge as compared to messages which is hidden.So, we always prefer digital image as cover medium for secrete information sending [7]. The secrete message in the audio steganography are hidden inside an audio signal. Communication is hidden by a tad changing the binary sequence of sound file [8].. Long Term Transmission becomes perfect carrier for steganography [9]. In digital scenario the communication happened in secure manner, using common technique that is cryptography. Cryptography method used for secure information transmission is the steganography [10]. Texture synthesis [11] it is the procedure of algorithmically making a large digital image from a small digital sample image by taking lead of its structural content. Texture synthesis are of several methods are available like tilling, stochastic, pixel-based, patch-based. The remainder of this paper is organized as follows: in section II we review the texture synthesis techniques, including embedding and extracting procedures. In section III, experimental results and extracting procedures. Insection IV followed by conclusions in the final section.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

II. RELATED WORK

In computer vision and PC graphics Texture synthesis has gotten a excessive covenant of consideration. The newest work has concentrated on texture synthesis, in which a source texture image is re-examined using either pixel based or patch-based algorithms to deliver another synthesized texture image. Pixel-based algorithms produce the composed picture pixel by pixel and it uses spatial neighborhood correlations to preference the most comparable pixel, for an example composition as the yield pixel. Since every yield pixel is dictated by the as of now integrated pixels.

Otori and Kuriyama [6], [7] headed the work of combining data coding with pixel-based texture synthesis. Top-secret messages to be concealed are encoded into hued spotted examples and they are forthrightly painted on a blank image. A pixel-based algorithm coats whatever is left of the pixels using the pixel-based texture synthesis strategy, in this manner concealing the presence of spotted examples.

Patch-based algorithms [8], [9] adhesive patches from a source composition somewhat than a pixel to synthesize textures.ThisapproachofCohenetal.

Also, Xu et al. augments the picture environment of pixel-based engineered surfaces in light of the fact that configuration structures inside the patches are kept up. Then again, since patches are trapped with a little covered district amid the synthetic procedure, one provisions to try to guarantee that the patches concur with their neighbors.

Liang et al. [10] offered the patch-based sampling methodology and used the feathering methodology for the covered ranges of nearby patches. Efros and Freeman [11] extant a patch sewing approach called "image quilting". For each new patch to be blended and sewed, the calculation first inquiries the source composition and picks one claimant fix that fulfills the pre-characterized blunder resistance regarding neighbors along the enclosed district. Next, a dynamic programming strategy is adopted to uncover the minimum error path way through the covered region. This announces an ideal limit between the picked applicant patch and the blended patch.

Ni et al. [12] proposeda image reversible data hiding algorithm which can improve the cover image with no expression from the stego picture after the hidden information have been extracted. Histogram shifting is preffered system among prevailing methodologies of reversible picture information hiding on the grounds that it can control the variation to pixels, along these lines restricting the inserting distortion, and it just requires a little size area guide, subsequently decreasing the overhead practiced. The current best in class for reversible image information covering up is the general system displayed by Li et al. [13].

To the best of our understanding, we were not able to reveal any writing that related patch-based configuration amalgamation with steganography. In this paper, we show our work which takes auspiciouslocation of the patch-based techniques to embed a secret message amid the incorporating methodology. This allows the source texture to be recovered in a message extricating system, giving the utility of reversibility. We point of interest our strategy in the following segment.

III. TEXTURE SYNTHESIS

Steganography refers to embedding data orsecret message into image. This approach works whichearns advantage of patch-based methods to insert a secretmessage during the synthesizing procedure. This permits thesource texture to be improved in a message extractingprocedure, providing the functionality of reversibility.This is a simple and safe high capacitysteganographic algorithm for information hiding.Synthesize a cover-image texture which is increased in sizeaccording to user need. The input texture is lesser in sizewhich is gradually produces, if the size is original into doubleand the texture is enlarged in size and resulting highresolution image is gained. The secret information ishired in the high resolution image patches based on thelookup table created. The created lookup table signifies theplace of the information.The secret message isembedded in the images based on LSB replacement of theDCT quantities of the cover-image.The same procedures reversed in the received sidein order to obtain the secret message.

Before inserting the secret message, it is securing it by embedding, using the DCT of the input image. So we can recognize whether the secret information is concealed in which location since secret information hidden in the DCT co-efficient of the new patches. The image, surreptitious information is well secure since it is located in high resolution image which is of the sizes and differ.

The input texture is gained and in that texture the embedding of the process is hired. By using DCT, the secret information is placed in source patch. The input texture is disintegrated using DCT and the secret information is hired in the coefficients of the images in the LSB of the new table. Finally, to the obtained images, the inverse cosine

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

transform is applied and it is used for the following method and after hiding the secret message in the image and index table is created. In the image matrix the attained source code is placed with help of the index table, it performances as the key for image composition.

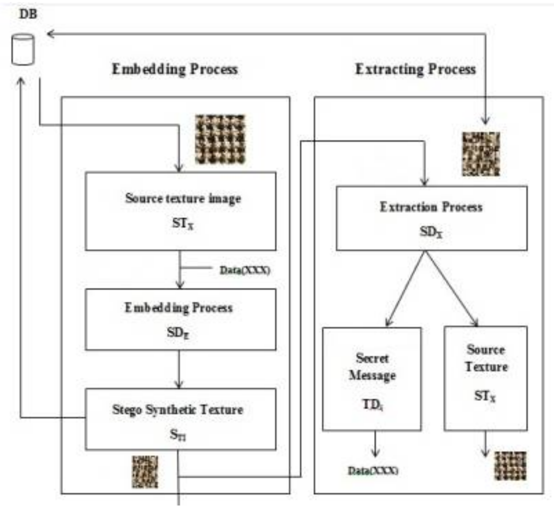


Fig.1 System Architecture

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 andsteganography. It contains mainly two procedures [1].

- Message embedding procedure
- Message extracting procedure

A. Message Embedding Process: The message embedding technique follows thethree process. This processcontains three sub steps. They are Index table generationprocess, Patch composition process and Message-orientedtexture synthesis process.
Index table generation,process is used to recordthe location of the source patch in synthetic texture. Patch composition process glue the source patches into aworkbench to produce a composition image and thenfinally we embed a secret message via the message orientedtexture synthesis to produce the final stego synthetictexture.
To distribute the patch we use algorithm.For that first plot the surf location point and then embeddingprocess is done. Then, we detach the blocks by using pixelstrong points. After that covert data is pasted in to theblocks to get embedding map. If the length of the data ispasted in to the blocks to get embedding map then the textis embedded into image. Then the patch compositionprocess and message oriented process is done.

B. Message Extracting Process

The message extracting for the receiver sideinvolves producing the index table, retrieving the sourcetexture, performing the texture synthesis, and extractingand authenticating the secret message concealed in thestego synthetic texture.
In the receiver side, the same index table as theembedding procedure can be generated. The next stage is thesource texture recovery. The recovered source texturewhich will be accurately the same as the source texture. In thenext step, the composition image generation to paste thesource patches into a workbench to produce a compositionimage by referring to the index table. This generates acomposition image that is identical to the one produced inthe embedding procedure. The final step is the messageextraction. We can extract all of the secret messages that are concealed in the stego synthetic texture patch by patch.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

C. Capacity Determination

The embedding capacity is one concern of the data embedding scheme, so to increase embedding capacity we used Adaptive embedding technique which is having following steps:

The embedding algorithm is summarized as follows:

• Step 1. Calculate the seven predictable values, prediction-errors and textured valuesfor every pixels.
• Step 2. Sort thetexture values ascendingly to obtain the running order of pixels. Use this order for Step 3 to Step 8.

• Step 3. Reserve the final pixels and accumulate their LSB values.
• Step 4. Check the tender and rough predictors making use of the optimization procedure as illustrated in Algorithm
. Step 5. Determine the first operating threshold utilizing the method as illustrated in Algorithm.
• Step 6. Embed the payload, final LSBs and region map. Create the location map making use of. This step applies pixel by way of pixel.
• Step 7. Create the footer and change it into the final LSBs after which calculate the PSNR.
• Step 8. Broaden the threshold t and repeat step 6 by means of 8. Stop the procedure when the PSNR decreases.

For the decoding algorithm, the layers are recovered in reverse order from the final to the first. The decoding algorithm is summarized as follows:

• Step 1. Calculate textured values
• Step 2. Sort the texture values ascendingly to acquire the operating order of pixels. Use this order for Step 3 to Step 7.
• Step 3. Extract the footer from the last LSBs: the gentle and hard predictors, running and textured thresholds and last role of embedding.
• Step 4. Separate smooth-rough areas through the textured threshold, calculate the anticipated values of the smooth-rough areas by way of the gentle and tough predictors after which calculate the modified prediction-error.
• Step 5. Extract the payload, region map and original LSBs.

• Step 6. Recover Original pixel values.

• Step 7. Substitute the LSBs with the original one.

D. Tree Based Parity CheckData Hiding

Lots of the current methods cover data throughout the randomly selected pixels without due to the fact that the regional pixel values. Accordingly probabilities for hiding data within the soft areas of the image are excessive. In this part, we explain how data is hidden within the side boundaries of an image with the aid of an edge adaptive scheme to make stronger the symmetry between cover picture and stego image. Tree based Parity check (TBPC).

Step 1: Location discovering approach: Hiding Secret data in area regions of animage is extra secured as a result edge areas are preferred. The edge region(ER) contains a pair of pixels as an embedding unit is (x_i, x_{i+1}), in which difference between these two pixels can be higher than or equal to threshold (T) value known through the sender and receiver.

The non-overlapping consecutive pixel pair in every embedding unit is located by means of traversing every row within the matrix illustration of the coverimage from left to correct. Relying on quantity of nodes within the grasp tree, quantity of pixel pairs is decided.

Step 2: Tree based Parity investigates (TBPC) process: The TBPC method is a least huge bit steganography approach. This procedure is used for generating stego code utilizing the LSB of selected pixels which encompass following three steps.

Step 3: Construction of master tree and create master string and toggle string: The system constructs an entire binary tree known as the master tree. The quantity of leaf nodes of the tree is equivalent to the message size (l).

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

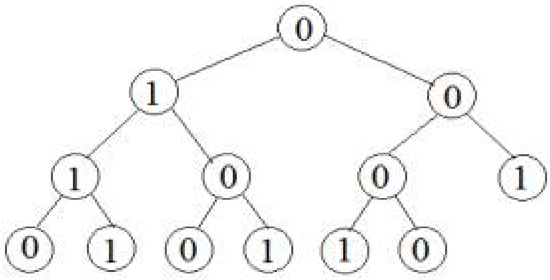
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

The nodes within the master tree is filled with the LSBs of the chosen pixels level by using degree, from high to bottom and left to right. The master string is created by performing even parity investigate on the master tree from the basis to leaves. Distinct-OR bit sensible (XOR) operation is carried out between message and master string to get a toggle string.

For illustration message to hide is h (1 1 0 1 0 0 0). The next are the chosen pixels 156,159,154, 165,160,162,105,166,161,162,165,171,166.Use the LSB of each and every pixel for developing the master tree.



Master Tree

Performing the parity determine from root to leaf node is referred to as the master String. Master String: 0 1 1 0 1 0 1 Message String: 1 1 0 1 0 0 0. Toggle string (1 0 1 1 1 0 1) is received via performing EX-OR operation between the Message and the master String. The Toggle string is depicted in fig. 2.

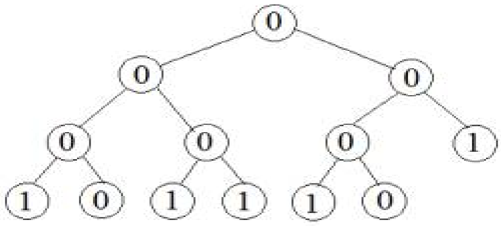


fig. 2.Toggle String

Step 4:Creation of toggle tree:Toggle tree is created by means of filling the leaf nodes with the toggle string and all of the different non-leaf nodes with zero. Then, traverse by means of each and every level, from the bottom to the basis, the non-leaf node and their corresponding leaf nodes are flipped if both of its children have bits as one. The Toggle tree is shown in fig.3.

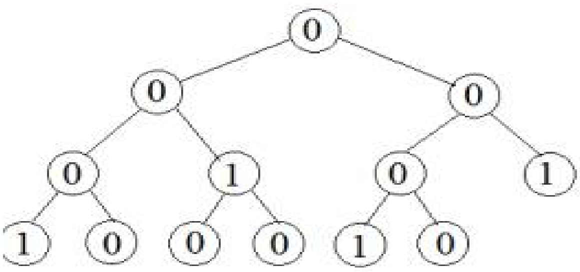


fig.3.Toggle Tree

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

Step.5: Construction of stego tree: The embedding algorithm obtains the stego tree through performing XOR between the master tree and the toggle tree. The stego code is obtained from the stego tree. The construction of the stego tree is proven in fig.4.The stego code (0 1 0 1 1 0 0 1 1 0 1 0 0) is embedded inside of an image using algorithm. The resultant stego image hides secret bits in an enormously at ease method.

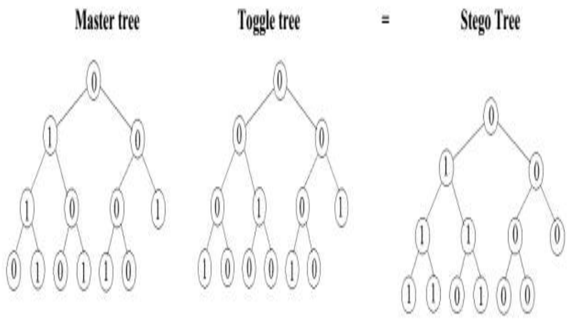


Fig.4Construction of stego tree

IV. EXPERIMENT RESULTS

In the first step is to read the input image and thenin that image we have to find out the surf location to embedthe secret messages. After that we need to createembedding map to hide the data. The information is hiddenbased on the strong points.

Input image

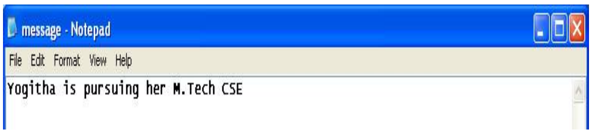
Composite image

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

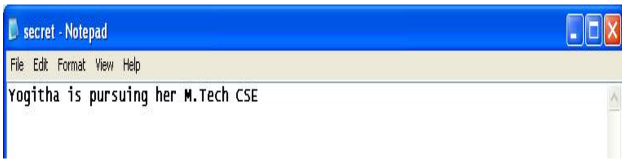
(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016



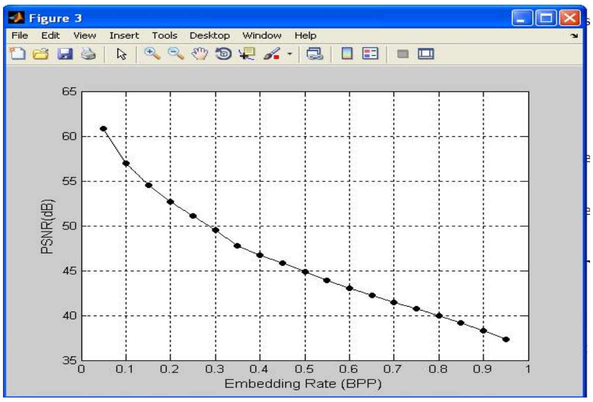
Embedded Text

Stego synthetic texture

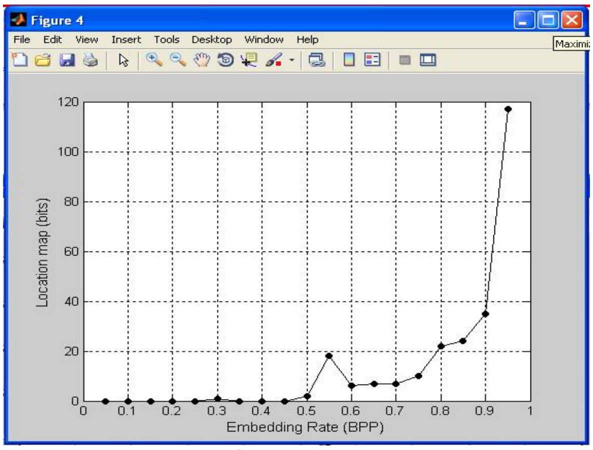


Extracted Text

Recovered image after extraction



PSNR vs. embedding rate



Size of the location map

Better performance in any data hiding scheme based on reducing the size of the location map. As the size of the location map decreases, fewer embedding bits are needed, resulting in smaller threshold values.
Therefore, theresulting distortion is reduced.

The gain in PSNR improves as the embedding rate increases, e.g. around 1.5 dB at 0.4 BPP to almost 3 dB at 0.8 BPP.Embeds two bits into smooth areas and one bit into rough areas. This strategy is called adaptive embedding. Embedding one bit into an already embedded pixel is better than embedding one bit into an expandable pixel of rough areas.

V. CONCLUSION

Steganography use different approaches to secure the communication. Many developers combine different algorithms ormodify the original algorithm to generate a new algorithm. The newly generated algorithms come up with more benefits.One of possible future study is to expand thisscheme to support other kinds of texture synthesisapproaches to improve the image quality of the synthetictextures. Another possible study would be to combine othersteganography approaches to increase the embeddingcapacities.

REFERENCES

1. Qingzhong Liu, Andrew H. Sung, Mengue Qiao, “Secure Data Hiding in Audio-Video Data Steganalysis by Anti-Forensics Technique”, IEEE Transactions On Information Forensics and Security, Vol.4 No.3 July 2015.
2. Kuo-Chen Wu and Chung-Ming Wang, Member, IEEE , “Steganography Using Reversible Texture Synthesis”, IEEE Transactions On Image Processing Vol: 24 No: 1 Year 2015
3. Odai M. Al-Shatanawi1 and Nameer N. El. Emam2 “A New Image Steganography Algorithm Based On Mlsb Method with Random Pixels Selection”, International Journal of Network Security & Its Applications (IJNSA) Vol.7, No.2, March 2015
4. Hamdan Lateef Jaheel and Zou Beiji, “A Novel Approach of Combining Steganography Algorithms”, International Journal on Smart Sensing and Intelligent Systems Vol. 8, No. 1, March 2015
5. Tahir Ali, Amit Doegar, “A Novel Approach of Lsb Based Steganography Using Parity Checker”, International Journal of Advanced Research In Computer Science And Software Engineering, Volume 5, Issue 1, January 2015.
6. Abdul Monems.Rahma, Matheel E.Abdulmunim, Rana J.S. Al-Janabi, “New Spatial Domain Steganography Method Based On Similarity Technique”, International Journal of Engineering and Technology, Volume 5 No. 1, January, 2015
7. R. Rejani1, D. Murugan2 and Deepu V. Krishnan3., “Pixel Pattern Based Steganography on Images”, ICTACT Journal on Image and Video Processing, February 2015, Volume: 05, Issue: 03
8. Kamalpreet Kaur, Deepankarverma, “Multi-Level Steganographic Algorithm for Audio Steganography Using LSB, Parity Coding and Phase Coding Technique”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume4, Issue 1, January 2014
9. Iwona Grabska, Krzysztof Szczypiorski, “Steganography in Long Term Evolution Systems”, 2014 IEEE Security and Privacy Workshops
10. Namitatiwari, Dr. Madhu Sandilya, Dr. Meenu Chawla, “Spatial Domain Image Steganography Based On Security and Randomization”, International Journal of Advanced Computer Science and Applications, Vol. 5, No. 1, 2014.08.