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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

Stegnography Using Reversible Texture Analysis

N.Padmavathi[1], R.Radha[2]

Research Scholar, Dept. of Computer Science, Bharathiyar College for Woman, Attur, Tamilnadu, India [1]

Asst.Professor, Dept. of Computer Science, Bharathiyar College for Woman, Attur, Tamilnadu, India [2]

ABSTRACT: Steganography refers to embedding information or secret message into media. It presents a simple and secure high-capacity Steganography algorithm for information hiding. The thesis synthesize a cover-image texture which is increased in size according to user desire. The input texture is smaller in size and the texture is increased in size and resulting high resolution image is obtained. The secret information is placed in the high resolution image patches based on the look up table created. The created lookup table denotes the location of the secret information. The secret message is embedded in the images based on LSB replacement of the DCT coefficients of the cover image. The same process is reversed in the receiver side in order to obtain the secret message and the original source patch. The performance of the process is measured based on the embedding capacity and other parameters. On the other hand, each byte of the secret information (secret Message, image, etc.) is first encrypted based on an exponential modular arithmetic which is then partitioned into two4-bit words. Each 4-bit word represented as an integer value in is inserted into a pixel in the selected cover- image to form a stego image. The embedding capacity for an m by n cover-image could be as high as (m × n)/2, an experiment is illustrated for the proposed methodology. This prevents a visible seam while ensuring that the color style of significant parts of the selected region is preserved when pasting. Matting techniques are used to construct the weight map. Diffusion is performed using a framework of mean-value coordinates rather than solving the original .The benefits of this hybrid approach, compared to previous image composite method, are twofold. Firstly, since a gradient-based approach is used, it is unnecessary to extract an accurate matte, which allows user interaction to be much less precise.

KEYWORDS: DCT coefficients, Steganography, SLDS, dynamic texture analysis.

I. INTRODUCTION

Steganography is a method for hiding secret informations in images. The advantage of steganography over cryptography is that the hided secret message does not attract attention. Steganography has numerous applications in the transmission of messages, digital water marking,etc. Texture synthesis helps in concealing the secret information in the image. There are commonly two types of texture synthesis Pixel based.Patch based.Patch based texture synthesis pattern preserves the image quality.

Steganography is a popular topic for scholarssince Internet becomes the most common way of communication. It forces people to establish a passive attitude of protecting data with high security to avoidbeing victims. The most important requirement of steganography is undetectability; the concealed messages should be perfectly disguised under all statistical and visual analysis. This system addresses generating any user-requested size of texture image, based on Markov random field synthesis, as a cover image to meet the size of secret message. Furthermore, if there are some pixels unused in the later rows of a stego-image, we can cut them without changing the visualization of stego-images. Second, each texture synthesized with the same parameters looks visually the same but different in their contents. Third, the same 2-bit words need not be embedded into the same pixel values. With out knowing α locations, it's hard to extract the binary encrypted secret message sequence. There fore if acover image is also part of secret information, then our approach of using MRF-synthesized texturesprovides a solution.

This reversible data hiding technique is mainly used for natural images. The most differences between pairs of adjacent pixels are equal or close to zero because of the similarity of neighbor pixels values. Based on these difference

DOI: 10.15680/IJIRCCE.2016. 0412243

statistics, the histogram is constructed. Multilevel histogram modification mechanism is used in the data embedding stage. Based on one or two level histogram modification, the hiding capacity is enhanced as more peak points are used for secret bits modulation. The distortions on the host image made by secret content embeddingis reduced as the differences of having common center around zero is improved. Instead of the peak points and zero points, the embedding level is used in the data extraction and image recovery stage.

The both using mixtures of linear models, unlike SLDS, our model ensures continuous motionand does not require constraints for local model transitions. We have demonstrated our approach in two classes of motions: holistic textured motions and articulated human motions. In particular, compared to the existing works in dynamic texture analysis, our method enhances the visual quality in synthesis of temporally stationary dynamic textures, and is able to model and synthesize non-stationary dynamic textures with fast and large shape variations which have not been accomplished in the literature.

A significant benefit of using mean-value coordinates is that the output value at each interior point can be interpolated totally independently of all other interior points, thus allowing a very efficient GPU implementation. Furthermore, the mean-value coordinates λ I (x) of a pointx are only dependent on the boundary. Thus, once the user has specifiedthe cutting boundary, all MVCs are determined, independently of where the patch is to be pasted: it is unnecessaryto recalculate MVCs as the patch is dragged over the target image. This allows fast enough updates for the user to immediately see what the results of pasting will look like.

II. EXISTING SYSTEM

Pixel-based algorithms generate the synthesizedimage pixel by pixel and use spatial neighborhood comparisons to choose the most similar pixel in a sample textureas the output pixel. Since each output pixel is determinedby the already synthesized pixels, any wrongly synthesizedpixels during the process influence the rest of the result causingpropagation of errors.Otori and Kuriyama pioneered the work ofcombining data coding with pixel-based texture synthesis.Secret messages to be concealed are encoded into coloreddotted patterns and they are directly painted on a blank image.A pixel-based algorithm coats the rest of the pixels using thepixel-based texture synthesis method, thus camouflaging theexistence of dotted patterns. To extract messages the printoutof the stego synthesized texture image is photographed beforeapplying the data-detecting m echanism. The capacity providedby the method of Otori and Kuriyama depends on the numberof the dotted patterns. However, their method had a small errorrate of the message extraction.

To the best of our knowledge, we were unable to discloseany literature that related patch-based texture synthesis withsteganography. In this paper, we present our work whichtakes advantage of the patch-based methods to embed asecret message during the synthesizing procedure. This allowsthe source texture to be recovered in a message extractingprocedure, providing the functionality of reversibility.We detail our method in the next section.

The pure synthetic texture which does not convey any secret message.

III. PROPOSED SYSTEM

The basic unit used for our steganographic texturesynthesis is referred to as a “patch.” A patch represents animage block of a source texture where its size is user-specified.We can denote thesize of a patch by its width (Pw) and height (Ph) .Apatchcontains the central part and an outer part where the centralpart is referred to as the kernel region with size of K w × K hand the part surrounding the kernel region is referred to as theboundary region with the depth.The first process isthe index table generation where we produce an index tableto record the location of the source patch set SP in thesynthetic texture. The index table allows us to access thesynthetic texture and retrieve the source texture completelySuch a reversible embedding style reveals one of the majorbenefits our proposed algorithm offers.

The embedding capacity is one concern of the data embed-ding scheme. Table II summarizes the equations we describedto analyze the embedding capacity our algorithm can offer.The embedding capacity our algorithm can offer is relatedto the capacity in b its that can be concealed at each patch(BPP, bit per patch), and to the number of embeddable patchesin the stego synthetic texture (EPn) . Each patch can concealat least one bit of the secret message; thus, the lower bound ofBPP will be 1, and the the maximal capacity in bits that can beconcealed at each patch is the upper bound of BPP, as denotedbyBPP max . In contrast, if we can select any rank from thecandidate list, the upper bound of

BPP will belog2(CPn) The total capacity (TC) our algorithm can offer is shown in (5) which is the multiplciation of BPP andEPn.

The system introduces RS steganalytic scheme since this algorithmis well-known, having been adopted for most steganalysis attacks. .

Advantages of Proposed System

- The secret messages and source texture from a stego synthetic texture. Our approach offers three distinct advantages.
- The steganography taking advantage of the reversibility has ever been presented within the literature oftexture synthesis.
- This have advantage of the patch-based methods to embed asecret message during the synthesizing procedure.

System Architecture

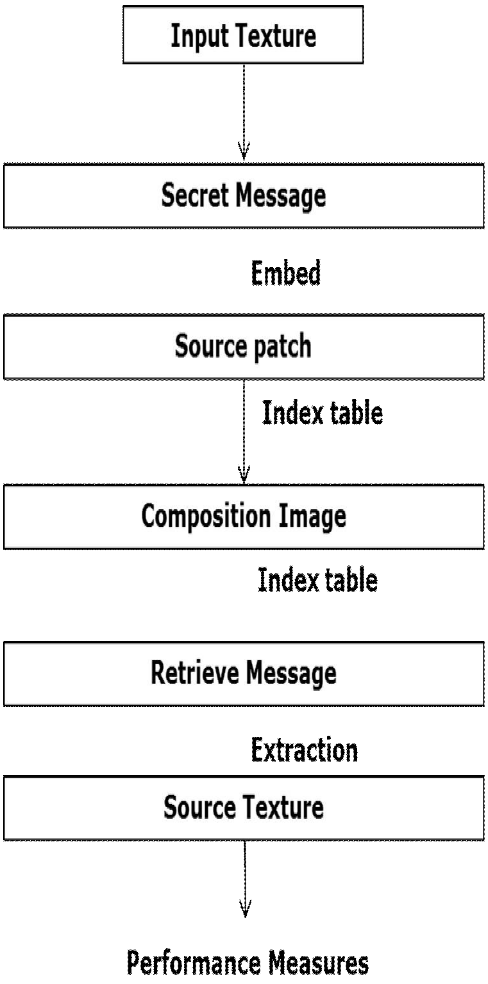

Fig 3.1: Architecture Diagram

IV. IMPLEMENTATION

Embedding

In this module the secret message is placed inside the input patch by using DCT. The input texture is decomposed using DCT. The secret information is placed in the low coefficient of the image.
To embed the message in the image the discrete cosine transformation is applied to the image.

$$X_k = \sum_{n=0}^{N-1} x_n \cos\left[\frac{\pi}{N}\left(n+\frac{1}{2}\right)k\right]$$

where
x- Image pixels
N- Size of the image
K-The image pixel position
The obtained DCT coefficients were then combined with the message inorder to produce the source patch.
〖Cipher〗_p=((〖DCT〗_p+〖msg〗_p))2
where 〖Cipher]_p is the resulting source patch.
〖DCT_p is the DCT coefficient of image.
〖msg_p is the input message to be hided.

Firstly the Discrete Cosine Transform (DCT) of thecover image is obtained. Then the stego image is constructed byhiding the given secrete message image in Least Significant Bitof the cover image in random locations based on threshold. DCTcoefficients determine the randomized pixel locations for hidingto resist blind steganalysis methods such as self calibrationprocess by cropping some pixels to estimate the cover imagefeatures. Blind steganalysis schemes can be guessedeasily hencethe proposed technique is more practically applicable.

Intex table creation

The obtained source texture is then placed in the image matrix with the help of the index table which acts a key for image composition The patch which contains the first part of the message is placed in a location and in the index matrix the corresponding location is denoted as 1 and so on.The locations where the secret message is not present were denoted in the index table as -1.

Pasting the Image patches

The index table obtained acts as the key for the extraction of the secret information.The indexing regions that are having value -1 is replaced with the help of the original image patches.The other regions were replaced with the embedded image that contains the secret information corresponding to the number in that place.The resulting image is the composited image with secret information hided

Energy Source patch Identification

The source patch is identified by the reversing the same image composition process.The values in the index table values acts as key for the identification of source patch.The patches in the regions that are having index table value as -1 were identified as the source patch.

The source patch generatorwill transform thevulnerable source code by generating a vulnerability-speciØcsource code patch, hence preventing the same vulnerabilityfrom being exploited. The patch is then integrated backto thedetectorso that the same vulnerability will not bereported again.

Extracting secret message.

The image patches that are having the values other than -1 contains the secret message.
The secret message is retrieved by reversing the embedding process

$$msg_p = [\Big(Cipher]_p \ast 2 \Big) - DCT_p$$

where $Cipher_p$ is the resulting source patch.

DCT_p is the DCT coefficient of the image.

msg_p is the input secret message to be hided.

The identified secret information is then arranged so that the hided message is retrieved.The arrangement is done by placing the extracted secret information in the order corresponding to the order denoted in the index table.

Performance Analysis.

The performance of the process is measured by calculating BPP and Total embedding capacity.

$$BPP_{max} = \left[\log_2 \left[\left(S_w - P_w + 1\right) * \left(S_h - P_h + 1\right)\right]\right]$$

$$SP_n = \left[\frac{S_w}{P_w - (2 * P_d)} + 1\right] * \left[\frac{S_h}{P_h - (2 * P_d)} + 1\right]$$

$$TP_n = \left[\frac{(T_w - P_w)}{P_w - P_d} + 1\right] * \left[\frac{(T_h - P_h)}{P_h - P_d} + 1\right]$$

$$EP_n = TP_n - SP_n$$

$$TC = BPP * EP_n$$

BPP_{max} □ - Bits per pixel

SP_n - Number of source patches obtained

TP_n - Number of synthetic patches obtained

EP_n - Number of embedded patches

TC – Total Embedding capacity

The BPP value and TC value should be high which indicates that the embedding capacity of our proposed methodology is high.

V. CONCLUSION

A secret hiding method that makes the secret informations more secure is proposed. Inorder to make the informations more secure the secret message is hided in the image patch and the patch is reconstructed to produce a better embedded image.The hiding of the information is done by using the Index table.The same process used for the encryption is reversed inorder to obtain the hided information and source texture. The performance of the process is measured by calculating the Bits per pixel and the total embedding rate of the image.This is indispensable, if the classification algorithmassumes normal distribution of the training samples. Traditionalimage classification methods tend to suffer shortcomings due tonon-normality of distribution of the training samples. The first running of BP takestheK1cluster centers as the label candidates. Suppose thatafter the first BP, the result forx I is the center of thekthcluster. Then in the second BP, the label candidates forx I are the elements in thekth cluster (if the number of theelements is larger thanK2, thenK2candidates are randomlyselected from the elements).

REFERENCES

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

[2] N. Provos and P. Honeyman, “Hide and seek: An introduction tosteganography,” IEEESecurity Privacy , vol. 1, no. 3, pp. 32–44,May/Jun. 2003.

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

[4] Y.-M. Cheng and C.-M. Wang, “A high-capacity steganographic approach for 3D polygonal meshes,” Vis. Comput., vol. 22, nos. 9–11,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.

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

[7] J. Fridrich, M. Goljan, and R. D u, “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, an d 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.
[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-parametric sampling,” in Proc. 7th IEEE Int. Conf. Comput. Vis., Sep. 1999,pp. 1033–1038.