ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 7, Issue 7, July 2018

Security Enhanced Steganography in DCT Domain using Reversible Texture synthesis and AES Encryption

Rinsa[1], Ayshamol V H[2]

Asst. Professor, Department of ECE, Ilahia College of Engineering and Technology, Ernakulam, Kerala, India[1]

PG Student, Department of ECE, Ilahia College of Engineering and Technology, Ernakulam, Kerala, India[2]

ABSTRACT: In steganography most important requirement is to increase the security and embedding capacity. In the proposed method it is able to accomplish both the requirements . A distinctive method of steganography in DCT domain using reversible texture synthesis is presented in this paper. A texture synthesis process re-samples a smaller texture image, which synthesizes a new texture image with a similar local appearance and an arbitrary size. Here texture synthesis is integrated with steganography to hide the secrete message. Along with these cryptography is used so that attacker doesn't know about the existence message and message itself is encrypted to ensure more security. The secret message is encrypted using one of the most powerful technique called AES algorithm .To enhance the security steganography is performed in frequency domain rather than spatial domain, using DCT technique . The effectiveness of the proposed method has been estimated by Mean square Error (MSE) and Peak Signal to Noise Ratio(PSNR) .

KEYWORDS- steganography, reversible texture synthesis, AES, DCT

I. INTRODUCTION

An important aspect of the modern way of life is communication .The considerable progress of internet and the rapid growth of its use have forced the human to the digital world and communicating by the use of digital data . In some cases it is needed to hide the data while travelling through different channels. In such cases communication security is a critical need. Steganography [1] and cryptography [2] are two methods used for sending vital information in a secret way. Steganography is powerful method of embedding secrete information for covert communication . It hides the message so it cannot be understood. Cryptography scrambles a message so it cannot be understood.

In this paper steganography and cryptography are combined to get the advantage of both . Steganography is a method of hiding a message ,file ,image or video within another message ,file ,image or video .A typical steganographic application includes secrete communications between two parties whose existence is unknown to a possible attacker .
Most image steganographic algorithms adopt an existing image as a cover medium. Embedding secrete messages into this cover image leads to distortion in the stego image. This leads to two drawbacks. First, since the size of cover image is fixed, the more secrete messages which are embedded allow for more image distortion. This result in the limited capacity provided in any specific cover image. Image steganalysis is an approach used to detect secrete messages hidden in the stego image by comparing it with original cover image .The second drawback is that image steganography can be defeated by image steganalysis and thus reveal that a hidden message is being conveyed in a stego image.

This paper proposes an approach for steganography with DCT (Discrete cosine transform) technique using reversible texture synthesis and AES (Advanced Encryption Standard) encryption. This helps to enhance the capacity and security of the embedded message. A texture synthesis process re-samples a small texture image in order to synthesize a new texture image with similar local appearance and arbitrary size. In the proposed method , the texture synthesis is weaved into steganography. This algorithm conceals the source texture image and embeds secrete message through the process of texture synthesis.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 7, Issue 7, July 2018

The proposed method offers four advantages. First, since the texture synthesis can synthesize an arbitrary size of texture images , the embedding capacity is proportional to the size of stego texture image. Secondly, a steganalytic approach is not likely to defeat the steganographic approach,since the steganography is performed in DCT domain and stego texture image is composed of source texture rather than by modifying the existing image contents . Third, the reversible capability provides the recovery of the source texture. Forth, encryption of secrete message adds one more level of security.

This paper is organized into following sections. Section II is an overview of related works. Section III presents the proposed system. Section IV discusses the experimental results and extraction, followed by conclusion in section V..

II. RELATED WORKS

In recent times texture synthesis have received a lot of attention in computer graphics and computer vision. Texture is an image which has locality and stochastic property. We often require large texture images. So we need to create large texture images from small texture images. The most recent work based on texture synthesis is one 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 subjective size.

Pixel based algorithm [3]-[5] generates synthesized image pixel by pixel and use spatial neighborhood comparison to choose the most similar pixel in a sample texture as the output pixel.

Otori and Kuriyama [6] pioneered the work of combining data coding with pixel-based texture synthesis.Secret messages to be concealed are encoded into colored dotted patterns and they are directly painted on a blank image.To extract messages the printout of the stego synthesized texture image is photographed before applying the data detecting mechanism.

H.Otori and S.Kuriyama [6] have presented a data hiding technique tools for protecting copyright or sending secrete messages. This paper proposed a method for embedding arbitrary data by synthesizing texture images using the smart technique of generating repetitive texture patterns through feature learning of a sample image.

L.Liang , C.Liu [7] presented a patch based algorithm for synthesizing texture from an input sample. This sampling algorithm is very fast and it creates high-quality texture image. This algorithm works well for a wide variety textures like regular to stochastic textures.

The building blocks of the patch-based sampling algorithm are patches of the input sample texture to construct the synthesized texture.We carefully select these patches of the input sampe texture and paste it into the synthesized texture to avoid mismatching features across patch boundaries.

Z.Ni,Y.-Q. Shi [8] presented a reversible data hiding algorithm for recover the orginal image without any distortion from the marked image after the hidden data have been extracted.The algorithm is applicable to a wide range of images such as commonly used images,medical images,texture images, aerial images.

The common image steganography technique are (i)Least Significant Bit(LSB) insertion.The LSB of cover images replaced with the confidential information.(ii)Masking and filtering method.The specific masking algorithm is used to select pixels to embed the secret information(iii)Transform techniques: The cover image converted intotransform domain by applying transformation such as Discrete cosine transform (DCT) ,Discrete Wavelet Transform (DWT)Discrete Fourier Transform etc and confidential information.

Hardik Patel and Preeti Dave [11] proposed a technique based on least significant bit replacement considering DCT coefficient value of pixels. The DCT of carrier image is obtained then based on proper threshold random locations are selected. LSBs of these potential locations in carrier image are replaced with MSB of the secrete image.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 7, Issue 7, July 2018

Data security is primary concern for every communication system. There are many ways to provide security to data that is being communicated. The more popular and widely used symmetric encryption algorithm is Advanced Encryption standard (AES).This is a standardised version of Rijndael algorithm ,which can process data block of 128,192, and 256 bits. AES can be programmed in software or build with pure hardware.AES is resistant against all cryptanalytic attacks. All other cryptographic algorithms have some problem.Most of the existing image steganographic algorithms have many drawbacks.First, the size of the cover image is fixed , so embedding more secret messages will leads to image distortion.So it needs a compromise between embedding capacity and the image quality,which result in the limited capacity provided in any specific cover image.Second, the image steganalytic algorithm can be used to detect secret messages hidden in the stego image .To overcome this limitations,Kuo-Chen Wu and Chung-Ming Wang [12] have proposed an approach for steganography using a reversible texture synthesis.A texture synthesis process synthesizes a new texture image from a smaller texture image which has a similar local appearance and an arbitrary size.This process combines texture synthesis with steganography to conceal secret messages.This scheme offers many advantages. First the embedding capacity is proportional to the size of the stego texture image. Second, steganalytic algorithm not defeat this steganographic approach. Third this allows recovery of the source texture.
This paper present a steganographic method in DCT domain which takes the advantage of the patch based method to embed encrypted secret message during the synthesizing procedure. This provide increased security and allows the source texture to be recovered in a message extracting procedure. This method is explained in the next section.

III. PROPOSED METHOD

The proposed method is highly secure and it provide improvement on the PSNR of the embedded image. The proposed method is described as follows. The basic unit of the steganographic texture synthesis is introduced as a “patch”. A patch represents an image block of a source texture where its size is user specified. The patch size is denoted by the width (P_h) and height (P_h).A patch contain the central part and an outer part. The central part is referred to as the kernel region with size of K_w x K_h ,and the part surrounding the kernel region is referred to as the boundary region with depth P_d .

Initially a source texture is selected and the source texture is divided into number of patches. Fig 3. shows the source texture.These patches has been pasted as part of the contents in the large synthetic texture image of arbitrary size and the secret message is embedded in this synthesized image. This method combines the texture synthesis process and steganography for concealing secret message as well as the source texture.

The procedure in sender side are:1)Texture synthesis 2)Message Encryption using AES 3)Performing steganography in DCT domain. Fig 2. shows flowchart of sender side.
The receiver section include following steps.1)Source texture Recovery 2) Extraction of secret message 3)Decrypting the message. Fig 7. shows flowchart of sender side.

A. SENDER SECTION

A.1.Steps involved in Texture synthesis

A.1.1. Index table generation process

The first process in texture synthesis is an index table generation. Index table is created to preserve the location of the source patch set in the synthetic texture. It allows us to access the final synthetic texture and retrieve the source texture completely. Synthesized texture of any size can be generated using this index table.

Initially all the values in the index table is set as -1, which shows that the table is blank. It is required to re-assign the values when source patch ID is distributed in the synthetic texture. A secret key is used to mark the locations in index table for placing source patches in workbench. It provide security and authentication.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 7, Issue 7, July 2018

In this index table ,the entries with non-negative values indicate the corresponding source patch ID subdivided in the source texture, while these entries with the value of -1 represent the patch position that will be synthesized by using any one of the original source patch.

A.1.2. Patch composition process

The second process in the texture synthesis is to paste the source patches into a workbench, which is a blank image, to obtain a composition image(Fig 4.). The source patches are pasted in the locations identified by the index table. The size of workbench is equal to synthetic texture. Fig. 3 shows the source patches pasted in workbench.

After pasting the original source patches, one of the source patch is used to synthesize the texture image. Embedding capacity is the most important requirements for steganography methods. Here the secret message is embedded in the synthesized patches. The number of source patches is very small compared to the number of synthesized patches. Therefore here it is possible to increase the embedding capacity.

BLOCK DIAGRAM

SENDER SECTION SOURCE

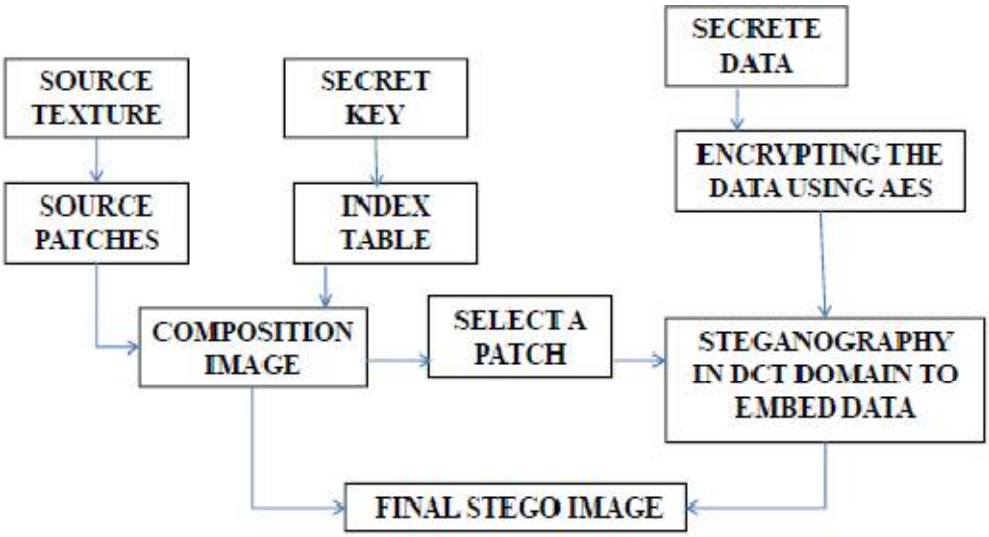

Fig 2.Flowchart of sender side

Fig 3 .Source Texture(Peanuts)

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 7, Issue 7, July 2018

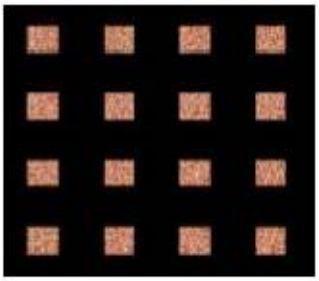

Fig 4 .Composition Image

Fig 5.Final stego synthetic texture

A2. Message encryption using AES

The security of the secret message being communicated can be enhanced by encrypting the message before embedding it in the patches. Here the textual data entered by the user is encrypted using AES algorithm(Fig 6).AES is very secure, simple and flexible. It allow data length of 128 bits.AES works with byte quantities, so first convert 128 bits into 16 bytes.128 bits of data is divided into four blocks. The blocks are organized in 4x4 matrices which is called states. Operations in AES are performed on a two-dimensional byte array of four rows and four columns. Encryption of data include four transformation steps and encryption is completed when 10 rounds of these transformations are performed. The transformations are Bytesubstitution , Shiftrows ,Mixcolumns, and Addroundkey

Bytesub transformation is a non linear byte substitution method .This transformation is done using s-box or substation block. S-box is constructed by multiplicative inverse and affine transformation, Second transformation is Shiftrows. This is a simple byte transformation. The last three rows of state are taken and the bytes in the last three rows are shifted cyclically.

Mixcolumns transformation is method in which columns of the state matrix is taken and matrix multiplication of columns is done. Here bytes are taken as polynomials , numbers are taken. A fixed matrix is multiplied with each column vector.Addroundkey is the final transformation . It is a simple XOR operation between the roundkey and the working state matrix.This transformation is an inverse of its own.

The initial step in the encryption is an Addroundkey. Next step consist of a block of four transformations(Bytesub,Shiftrows,Mixcolumns, Addroundkey).To this block a round function is applied .This step is performed iteratively up to 10 times.The last round leaves out the mixcolumn operation.The number of iterations will depend on the key length.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 7, Issue 7, July 2018

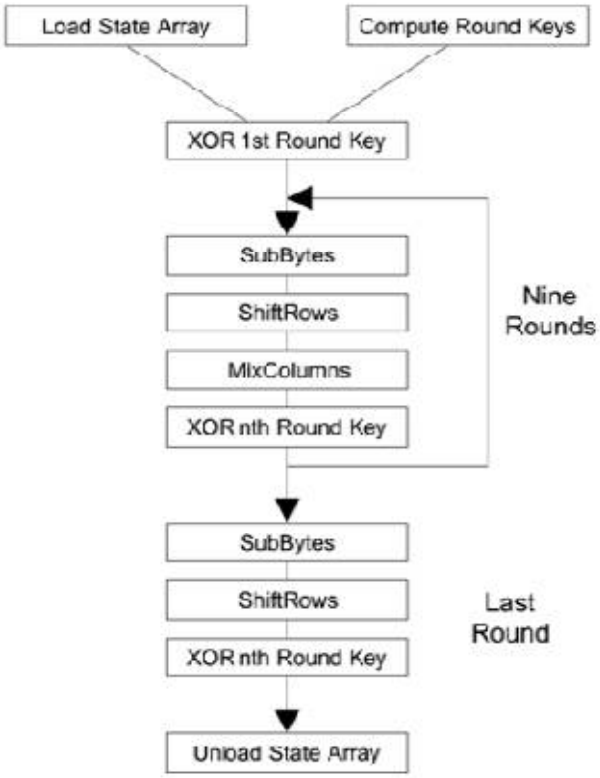

Fig 6 .Summary of AES encryption

A3. Performing steganography in DCT domain

In the proposed method the encrypted secret message is inserted into the Discrete Cosine Transform domain of the source patch used for synthesizing texture image.It means that the image is transformed from spatial domain to frequency domain.Advantge of using frequency domain steganography is that it is very secure and hard to detect.The image is divided into 8x8 block of pixels. Working from left to right,top to bottom subtract 128 in each block pixels.Then DCT is applied to each block and each block is compressed through quantization matrix. Then LSB is performed on DCT coeffients.After data hiding inverse DCT is taken.So that image is changed from transform domain to spatial domain.

Here Texture synthesis and steganography is performed correspondingly.

B. RECIEVER SECTION

B1. Source Texture Recovery

After the stego synthetic texture has been received in the receiver section ,an index table is created as did in the sender section. The key used to generate index table is same as that of the sender section. The next step is the source texture recovery. The source patches in the stego synthetic texture are retrieved by referring to the index table. The source patches can be arranged based on their ID to obtain the source texture.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 7, Issue 7, July 2018

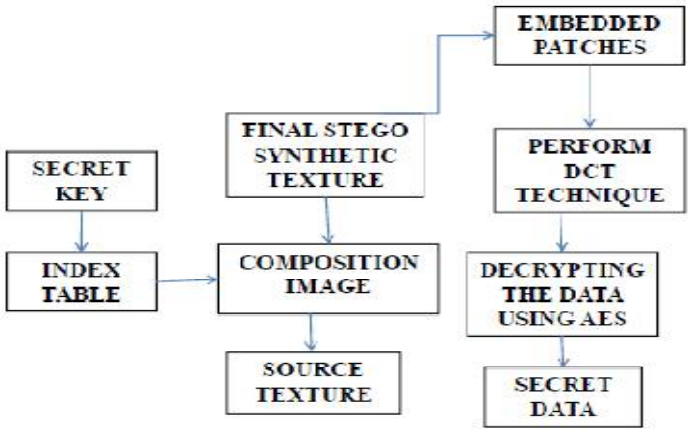

Fig 7.Flowchart of receiver section

B2. Extraction of Secret Message

By referring to the index table composition image is produced , that is identical to one produced in the embedding procedure. Firstly, source patch used for synthesizing texture image is selected, which contain no message. Then it is compared with each of the other patches used for synthesis. If they are unequal , then the other patch contain data. Thus patches containing data are found.
To extract the secrete message the image is converted from spatial domain to frequency or transform domain using Discrete Cosine Transform. Otherwise it is not possible to extract the message directly from the patch. This is one of the prominent advantage of the proposed system.

B3. Decryption of Secret Message

The extracted message is in encrypted form. Therefore to recover the original message from the sender , it is required to perform AES decryption. The decryption structure is similar to the encryption transformations. In decryption , the transformations are Inverse-Bytesub , the Inverse -Shiftrows , the Inverse-Mixcolumns, and the Addroundkey . Key schedules are identical for encryption and decryption.

IV.EXPERIMENTAL RESULTS

The experimental results are obtained in MATLAB R.2015a.The Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR) are the two error matrices used to compare image compression quality. The proposed model is able to produce highest Peak Signal to Noise Ratio (PSNR) and reduced Mean Square Error (MSE).

IV.1 MSE

It represents the cumulative squared error between the compressed and the original image. The lower value of MSE the lower the error.MSE is calculated using following equation.

$$MSE = \frac{\sum_{i=1}^{n} \sum_{j=1}^{n} (cov(i,j) \quad steg(i,j))^{2}}{M*N}$$

In this method,it is possible to reduce Mean square error to zero.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 7, Issue 7, July 2018

IV.2 PSNR

It is the ratio of the maximum signal to noise in the stego image. This ratio is often used as a quality measurement between original image and compressed image. Here peak signal to noise ratio between stego synthetic texture image and synthetic texture image is measured .It is computed using following equation.

$$PSNR=10 \log_{10} [R^2/MSE] \quad (2)$$

In the equation R is the maximum fluctuation in the input image data type. The proposed method is able achieve an infinite PSNR ,which means best quality of the stego image.

V.CONCLUSION

This paper proposes a steganography method in Discrete cosine transform domain incorporated with reversible patch based texture synthesis and AES encryption technique. Compared to the existing system it is able to give better PSNR and MSE value. The presented algorithm have advantages of increased security and increased capacity. It also provides reversibility to retrieve the original source texture from stego image. This method is resistant to steganalysis.

REFERENCES

[1] N. F. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen," *Computer*, vol. 31, no. 2, pp. 26–34, 1998.
[2] Domenico Daniele Bloisi , Luca Iocchi: Image based Steganography and cryptography, Computer Vision theory and applications volume 1 , pp. 127-134 .
[3] 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.
[4] 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.
[5] C. Han, E. Risser, R. Ramamoorthi, and E. Grinspun, "Multiscale texture synthesis," *ACM Trans. Graph.*, vol. 27, no. 3, 2008, Art. ID 51.
[6] 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.
[7]L. Liang, C. Liu, Y.-Q. Xu, B. Guo, and H.-Y. Shum, ―Real-time texture synthesis by patch-based sampling,‖ *ACM Trans. Graph.*, vol. 20, no. 3, pp. 127–150, 2001.
[8] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, ―Reversible data hiding,‖ *IEEE Trans. Circuits Syst. Video Technol.*, vol. 16, no. 3, pp. 354–362, Mar. 2006.
[9] Ken Cabeen and Peter Gent, ―Image Compression and Discrete Cosine Transform‖, College of Redwoods.
[10] J.R. Krenn, "Steganography and Steganalysis", January 2004.
[11] Hardik Patel, Preeti Dave- Steganography Technique Based on DCT Coefficients / International Journal of Engineering Research and Applications ., Vol. 2, Issue 1,Jan-Feb 2012, pp.713-717
[12]Kuo-Chen Wu and Chung-Ming Wang―Steganography Using Reversible Texture Synthesis‖*IEEE Trans.on* Image Processing, VOL. 24, NO. 1, Jan 2015