STEGANOGRAPHY USING TEXTURE SYNTHESIS

V.B.Jayasree[1], K.R.Lashya[2], S.Jayanthi[3]

Student,Dept. of Computer Science and Engineering, Agni college of Technology, India
Ass.Professort,Dept. of Computer Science and Engineering, Agni college of Technology, India
[1]Vbj1995@gmail.com[2]Lashu2721@gmail.com[3]Jayanthi.cse@act.edu.in

ABSTRACT

We propose a novel approach for steganography using a texture synthesis. 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. We weave the texture synthesis process into steganography to conceal secret messages. 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. This allows us to extract the secret messages 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 – Steganography , texture synthesis, Encryption, Decryption, DES algorithm

I . INTRODUCTION

We often would like to send messages in the form of smilies or images. For example while viewing for a facebook video or for a whatsapp video we Would like to comment the particular person instead of others knowing it.It is very difficult in facebook whereas in whatsapp we can make use of the individual chat.Since it uses steganography we can encrypt an image or a text in a video file and then can be posted it in the facebook or whatsapp , the person having this application and knowing the right algorithm can alone decrypt this message thus this provides a sense of security as well the comment can be shared without others noticing it.

2. BACKGROUND AND RELATED WORK

In this section, we provide background and related work on steganography , upon which our presented algorithms are applied.

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]–[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.

Otori and Kuriyama [12], [13] 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. A pixel-based algorithm coats the rest of the pixels using the pixel-based texture synthesis method, thus camouflaging the existence of dotted patterns. To extract messages the printout of the stego synthesized texture image is photographed before applying the data-detecting mechanism. The capacity provided by the method of Otori and Kuriyama depends on the number of the dotted patterns. However, their method had a small error rate of the message extraction.

Patch-based algorithms [14], [15] paste patches from a source texture instead of a pixel to synthesize textures. This approach of Cohen et al. and Xu et al. improves the image quality of pixel-based synthetic textures because texture struc- tures insidethe patches aremaintained.However,since patches are pasted with a small overlapped region during the synthetic process, one needs to make an effort to ensure that the patches agree with their neighbors.

Liang et al. [16] introduced the patch-based sampling strategy and used the feathering approach for the overlapped areas of adjacent patches.

Efros and Freeman [17] present a patch stitching approach called “image quilting.” For every new patch to be synthesized and stitched, the algorithm first searches the source texture and chooses one candidate patch that satisfies the pre-defined error tolerance with respect to neighbors along the overlapped region. Next, a dynamic programming technique is adopted to disclose the minimum error path through the overlapped region. This declares an optimal boundary between the chosen candidate patch and the synthesized patch, producing visually plausible patch stitching.

Ni et al. [18] proposed an image reversible data hiding algorithm which can recover the cover image without any distortion from the stego image after the hidden data have been extracted. Histogram shifting is a preferred technique among existing approaches of reversible image data hiding because it can control the modification to pixels, thus limiting the embedding distortion, and it only requires a small size

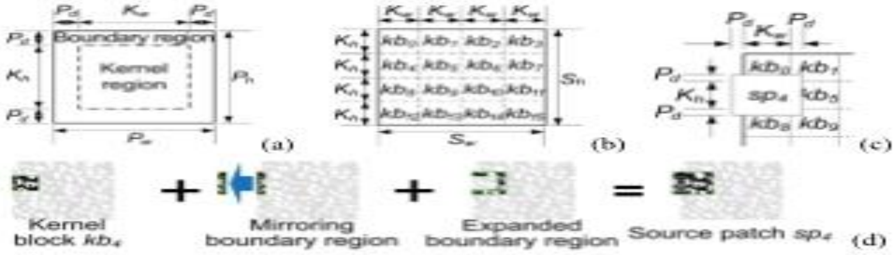

Fig. 1. Patch, kernel blocks, and source patch.

(a) The diagram of a patch. The central part of a patch is the kernel region; the other part around the kernel region is the boundary region.

(b) An illustration of non-overlapped kernel blocks subdivided from the source texture.

(c) The diagram of source patches derived by the expanding process using kernel blocks.

(d) The boundary mirroring and expanding for a source patch.

location map, thereby reducing the overhead encountered.

The current state-of-the-art for reversible image data hiding is the general framework presented by Li et al. [19]. 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, providing the functionality of reversibility. We detail our method in the next section.

3. SYSTEM OVERVIEW

This section formalizes our proposed method with modular description.

A. Proposed Method

In this section , we deal with modules we use in our system

1)Secret Message Formulation : Secret Message Formulation is out secret message which is an image. Pixel values of first 8x8 of 128x128 sized image is taken in. Each pixel intensity is then converted into equivalent binary values. As the size of the image is 128x128 we got 128x128x8=131072 bit (the secret message bits to be hidden).

2)Frame Extraction And Embedding Secret Message: Here we have taken a avi video file as a cover or host video and all frames are extracted (28 frames). The resolution of the original AVI is 120x160 pixels. The R-channel is used for encoding secret message after performing block DCT on those frames. As the size of original babra.bmp image is 128x128, hence we have to encode total 128x128x8 bits in the video frames. Here we embed 16 bits per 8x8 DCT higher order coefficient and in a particular frame we can embed frames can accommodate our secret message bits. After extracting the frames, each R-channel frame is block processed by 8x8 DCT and 16-bit secret message bits are embedded into the higher order DC co efficient of each block. After encoding the R-channels of frames we combine those to get the video AVI file with secret message embedded. Figure 8 shows the video stream frames after secret message embedded. We did not find much more distortion in the video.

3)Decoding and Reconstruction of Secret Message: Decoding is done in reverse way of encoding.
First video frames are extracted and R-channel frames are processed by 8x8 block DCT then the 8x8 block processed R-Channel original frame values are subtracted to get secret message. From extracted secret message the image is reconstructed.

4. ALGORITHMS

In this section, we detail how our image can be encrypted in a video file using data encryption standard algorithm ,Triple data encryption standard algorithm ,Rivest Shamir Adelman algorithm.

A.Outline

Algorithm 1:Data encryption standard
Algorithm 2:Triple data encryption standard
Algorithm 3:Rivest Shamir Adelman

Algorithm 1 outline the encryption process were a block of 64 bits is permuted by an initial permutation called IP.Resulting 64 bits are divided in two halves of 32 bits, left and right.Right half goes through a function F(Feistel function)Left half is XOR-ed with output from F function above.Left and right are swapped(except last round).If last round, apply an inverse permutation IP-1 on both halves and that’s the output else, repete process.A round. DES has 16 identical rounds.Triple DES uses a "key bundle" that comprises three DES keys, K_1, K_2 and K_3, each of 56 bits (excluding parity bits). The encryption algorithm is:ciphertext = $E_{K3}(D_{K2}(E_{K1}(\text{plaintext})))$I.e., DES encrypt with K_1, DES decrypt with K_2, then DES encrypt with K_3.Decryption is the reverse: plaintext = $D_{K1}(E_{K2}(D_{K3}(\text{ciphertext})))$I.e., decrypt with K_3, encrypt with K_2, then decrypt with K_1.Each triple encryption encrypts one block of 64 bits of data.In each case the middle operation is the reverse of the first and last. This improves the strength of the algorithm when using keying option 2, and provides backward compatibility with DES with keying option 3.Keying options:The standards define three keying options:Keying

option 1:All three keys are independent.Keying option 2:K_1 and K_2 are independent, and K_3 = K_1.Keying option 3:All three keys are identical, i.e. K_1 = K_2 = K_3.RSA involves a public key and private key. The public key can be known to everyone, it is used to encrypt messages. Messages encrypted using the public key can only be decrypted with the private key.The keys for the RSA algorithm are generated the following way:Choose two different large random prime numbers p and qCalculate $n = pq$.n is the modulus for the public key and the private keysCalculate the quotient: $\phi(n) = (p-1)(q-1)$Choose integer e such that 1< $e < \phi(n)$, and e is coprime to $\phi(n)$ ie: e and $\phi(n)$ share no factors other than 1; gcd(e,$\phi(n)$) = 1.e is releasedasthepublickeyexponent. Computed d to satisfy the congruence relation $de \equiv 1 \pmod{\phi(n)}$ ie : $de = 1 + k\phi(n)$ for some integer k.
is kept as the private key exponent

B.System Study

1)Existing System : The existing system of most of the Steganography is LSB Algorithm. This means Least Significant Algorithm. In LSB algorithm, the message bit is taken from the message byte and then that particular bitwill be embedded inside the least significant bit of an image or video or audio file. This is done because..

1.The message embedded in the least significant bit of an image file will not draw the suspicion of the hacker as thethe image file will not be perceived by the normal naked human eye.

2.The message that will be embedded in the LSB of an audio file will not create suspicion to the hacker as that change would not be perceived by the human ear.

3.The same concept works out evenwith video file.

However, there are few weaknesses of using LSB. It is very sensitive to any kind of filtering or manipulation of the stego-image .Scaling, rotation, cropping, addition of noise, or lossy compression to the stego-image will destroy the message. On the other hand, for the hiding capacity, the size of information to be hidden relatively depends to the size of the cover- image. The message size must be smaller than the image. A large capacity allows the use of the smaller cover-image for the message of fixed size, and thus decreases the bandwidth required to transmit the stego-image.Another weakness is an attacker can easily destruct the message by removing or zeroing the entire LSB plane with very little change in the perceptual quality of the modified stego-image .Therefore, if this method causes someone to suspect something hidden in the stego-image , then the method is not success.

2) Proposed System : In proposed, we use DES(Data Encryption Standard), Triple DES(Triple Data Encryption Standard),RSA (Rivest-Shamir-Adleman) Algorithms to embed the data. These algorithms are better than LSB Algorithms. An AVI (Audio Video Interleave) fie is nothing but a sequence of high resolution image called frames. It is possible to collect all the

frames in bitmap format. Each frame consisting of three channel of RGB. After collecting the frame we perform DCT (8x8 block) on any channel (say Rchannel) of the frames and embed the secret information bits in selected higher order coefficients. Each frame is processed by 8x8 Inverse DCT block processing and the combined to get AVI with hided message.
Decoding is done in reverse process of encoding. First each frame is extracted from just created AVI. Perform 8x8 DCT block processing on the channel where secret information was embedded earlier (R-channel here) and secret bit information's are extracted by subtracting from original DCT block processed values. The advantage of proposed over cryptography alone, is that messages do not attract attention to themselves. Plainly visible encrypted messages-no matter how unbreakable-will arouse suspicion, and may in themselves be incriminating in countries where encryption is illegal.Therefore, whereas cryptography protects the contents of a message, steganography can be said to protect both messages and communicating parties.

V.System Architecture

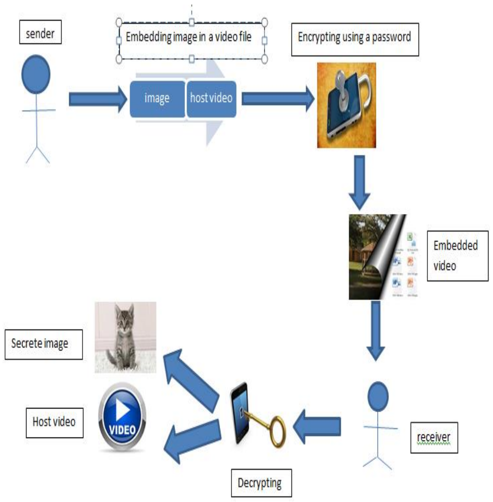

Fig 2 represents the system architecture

VI. System Analysis

This deals with the limitation of existing system and features of proposed system.

A.Limitations of existing system

- Very sensitive to any kind of filtering or manipulation of the stegno-image.
- Scaling, rotation, cropping, addition of noise, or lossy compression to the stegno-image will destroy the message.
- Attackers can easily destruct the message by removing or zeroing the entire LSB plane with very little change in the perceptual quality of the modified stegno-imagae.

- A large capacity allows the use of the smaller cover-image for the message of fixed size, and thus decreases the bandwidth required to transmit the stego-image.
- Low robustness to malicious attacks
- Vulnerable to accidental or environmental noise
- Low steganographyic capacity
- High payloads
- Low temper resistance

B.Features

- Our scheme offers the embedding capacity that is proportional to the size of the stego texture image.
- The reversible capability inherited from our scheme provides functionality, which allows recovery of the source texture
- Messages do not attract attention to themselves.
- Cryptography protects the contents of a message, steganography can be said to protect both messages and communicating parties.
- Source image can be conceled.
- Resistance to bruteforce attacks.
- Eliminate Security Issues and user friendly.

7. CONCLUSION

This paper proposes a steganographic algorithm using texture synthesis. Given an original source texture, our scheme can produce a large stego synthetic texture concealing secret messages. It is first method to exquisitely weave the steganography into convectional texture synthesis. This method is novel and provides reversibility to retrieve the original source texture from the stego synthetic textures, making possible a second roundof texture synthesis if needed.With the two techniques ,our algorithm can produce visually plausible stego synthetic textures even if the secret messages consisting of bit “0” or “1” have an uneven appearance of probabilities. The presented algorithm is secure and robust against an steganalysis attack. It is believed that the proposed scheme offers substantial benefits and provides an opportunity to extend steganographic applications. By implementation of this application secrete images and text can be shared without being hacked or being misused. It is less time consuming and more secured when compared to other techniques used.

REFERENCES

[1] Kuo-Chen Wu and Chung-Ming Wang “Steganography Using Reversible Texture Synthesis”, Member, IEEE. IEEE *transactions on image processing*, VOL. 24, NO. 1, JANUARY 2015

[2] R.Bonde, M.Mahendra and Vidya Dahake, “A General framework for reversible data hiding : a review,” International journal for research in emerging science and technology.,vol.2, issue-6, jun-2015

[3] Sreedevi S and Shinto Sebastian, “Fast Image Retrieval with Feature Levels,” International Conference on Microelectronics, Communication and Renewable Energy, 2013

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

[5] C-C Lai and Y-C Chen, “A user-oriented image retrieval system based on interactive genetic algorithm,” IEEE Trans. Instru. Measur, vol. 60, no. 10, pp. 3318-3325, Oct.2011.

[6] S.-B. Cho and J.Y. Lee, “A human-oriented image retrieval system using interactive genetic algorithm,” IEEE Trans. Syst., Man, Cybern. A, Syst.,Humans, vol. 32, no. 3, pp. 452–458, May 2002.

[7] V.Srikanth,C.Srujana,P.Nataraju,S.Nagarajuand,Ch.Vijayalakshmi, “Image gathering using both color and texture features,”IJECT, vol. 2, SP-1, pp. 55-57, Dec. 2011.

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

[9] H. Otori and S. Kuriyama, “Texture synthesis for mobile data com- munications,” IEEE Comput. Graph. Appl., vol. 29, no. 6, Nov./Dec. 2009.

[10] S.-S., Sebastian-S., “Content based image retrieval based on database revision,” International Conferenceon machine vision and image processing,Dec 2012.