Indian Journal of Science and Technology, Vol 9(48), DOI: 10.17485/ijst/2016/v9i48/107957, December 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Enhancing Embedding Capacity and Security using Reversible Texture Synthesis in Image Steganography

S. Kruthika* and V. Kalpana

School of Computing, SASTRA University, Thanjavur - 613401, Tamil Nadu, India;
kruthikaselva21@gmail.com, kalpana@cse.sastra.edu

Abstract

Objectives: Image steganography embeds a secret data of any form on an image. It hides data into a digital media like image, audio and video. The message existence is made unknown by embedding it in a digital host before transmitting it. Secret communication can be achieved through cryptography and steganography. But steganography has few advantages over cryptography one such major advantage is that the encrypted text is hidden and cannot easily be disclosed. **Methods:** Steganogrphy technique involves cover object and stego object where Cover-object is the object in which message is embedded and Stego-object is the object that carries the hidden message. Texture synthesis is used in steganography where smaller texture image is resampled into new texture image with similar visual properties. Instead of using a cover image for hiding messages the proposed method involves concealing original texture of the image and embedding the secret messages. **Findings:** In Reversible texture synthesis the source texture can be recovered which is same as that of the original image therefore it can be reused further. In the proposed system Patch based texture synthesis is employed wherever the textures are synthesized by pasting the patches from original texture. Embedding capability and security will be increased without degrading image quality using Huffman cryptography. **Applications:** Steganography is mainly used for confidential and secret data sharing, protection against data alteration, control system access for digital distribution of contents, Steganography is also used for media database systems

Keywords: Huffman Coding, Patch Synthesis, Security, Steganography, Texture Synthesis

1. Introduction

Image steganography is a process of concealing data of any form onto an image which can be extracted later. It is simply an improvement over cryptography, where the data is directly manipulated to a form which cannot be understood by any unauthenticated user. Encrypted messages which are visible to human eye will be of more concentration. Hence images are preferred as cover medium since it will not catch the attention of an object of inspection. Cryptography intends to protect only the content of the secret data. But image steganography[1] intends to protect the content and as well as the truth that undisclosed data will be sent. When cryptograph is combined with image steganography, even more security can be attained. The intended secret data to be sent is first encrypted using a cryptographic algorithm. It is then embedded onto an image and sent. At receiver's end, the text is first extracted and later decrypted to get the original data. The main components of image steganography are a cover image, data to be transmitted, and an algorithm to embed data onto the image. Cover image is said to be the carrier which will hold the data. The quality of the cover image depends on the algorithm that is chosen. Watermarking is different from steganography. Image is nothing but a collection of pixels. The color depth of each pixel ranges from 1 to 48, where 1 bit forms black & white images, 2 bits pixels forms gray scale images and

*Author for correspondence

others form true color images. The embedding process in image steganography is done by manipulating the bits in the pixels, with the bits in the encoded data. The extraction process extracts the manipulated bits and combines them to generate original data. The Information- hiding process in a Steganographic system starts by simply identifying a protective cover medium's obsolete bits those can certainly be modified without wrecking that medium's integrity. The embedding process provides an impressive stego medium by exchanging these repetitive bits with data from the concealed message. In conventional days steganography's goal is to keep its mere occurrence undetectable, but Steganographic system because of their intrusive nature leave behind detectable footprints in the cover medium. Even if key content is not revealed, the existence of it is changing the cover medium changes its statistical properties, so eavesdroppers can find the distortions in the consequential stego medium's properties. Widely used algorithm for steganography involving images uses raw image as host medium. The distortion amount encountered by the image implies the cost for encasing secret messages and this result in following drawbacks. Initially the scale of any quilt image has been mounted when large amount of undisclosed messages is embedded the quality of image is degraded. Process that reveals the secret messages hidden within stego image is image steganalysis. Some distortion will be contained in stego image, and in spite of however minute it's, the natural choice of the quilt image will be interfered. This result in downside as a result of it's still potential that a picture steganalytic algorithmic program will overcome the steganography and therefore the hidden message can be easily uncovered from the encrypted image. A small size image can be resampled into a synthesized image by means of replacement texture image with an identical native look and random size, this method is the texture synthesis. Thus the texture synthesis method is employed here for concealing secret messages in to source texture. Instead of exploitation an existing cover image for hiding messages, this algorithmic rule hides original image and entrench secret messages using a method called texture synthesis, this allow the extraction of original image as well as the message which is embedded in it without any alteration. Advantage of the method is it provides reversibility by the use of texture synthesis with in steganography. This method has 3 benefits. Texture synthesis will produce a random size of texture pictures, the entrenching capability that this theme provides an appropriate size proportional to the dimensions in the image of the stego texture. Another is that Huffman coding[2,3] used in this method for compression further increases the embedding capacity and steganalytic algorithm; it is not possible to break the above mentioned technique since the resulting image contains original texture of image. Then, this process enables a reverse method which reproduces the original image texture. The extracted image of the source can be reused for second set of hiding process.

In[3] Reversible data hiding method which is a histogram shifting process. It works by creating feature components of histogram and embedding the data by shifting histogram bins. Even though this technique good, it has a downside such as low embedding capability and lack of ability. To adjust the capability by concealing the secret text bits into fault values. In[4] Multi resolution sampling process to analyze and synthesize the texture images in two phases. In first texture is analyzed by quantify the joint happening in the texture inequality options. In the next phase a new texture is created which samples consecutive frequency in spatial brands and the input texture in the identical joint happening of options at inferior level frequency. Successive capture of input texture will do the previous techniques. The newly synthesized textures are different from the first and appear to be created by steady underlying image. In[5] Multi resolution filter process the algorithm program which takes the input sample and randomize the texture. In the way that protects the interscale dependencies. The downside of this technique is texture pictures are bigger than the input. In[6] Primary and second order property prediction of joint way coefficients. On the other hand, it fails to replicate high frequency information. In[7] Non parametric process produces texture element by element, apparent from the primary seed. Single element is chosen as entity or synthesis. So this model captures the maximum amount of frequency information as achievable. So the non-parametric process is enormously powerful. In[8] Information hiding system needs capability, security, and strength. Here capability refers to the quantity of the text concealed within the cover medium. Security refers to the protection against eves droppers that is inability to look for concealed information and strength refers quantity of information that a medium can withstand before and after extracting the hidden text. In[9] Multiscale synthesize of texture is a process that generate image from an input exemplary image. The algorithmic problem produces a larger coherent non episodic texture produces tiny low samples of texture.

Constrained band of spatial scales produce the texture data for the exemplar images, therefore the texture bigger than the exemplar pixels lost the square measures together. This is the downside in real world textures so it is beneficial if we select a multiscale texture with variable spatial scales. In[10] Hiding the text inside the image are Huffman coding based text embedding. In[11] Pixel based texture synthesizes generates image element by element and uses spatial vicinity comparisons to choose the foremost similar element as a output pixel. The output elements are produced by previously synthesized pixels if any one of them is wrongly synthesized. It will reflect throughout the result. It produces propagation of errors.

2. Proposed Model

In the proposed methodology, patch based texture methodology and Huffman technique is used to enhance the capacity and security of steganography.

2.1 System Architecture

Figure 1 shows the size of texture source is denoted as S.wi*S.ht. where S.wi is original source width, S.ht is the original source height is given as input for synthesizing textures**.** The proposed Patch-based model is to insert undisclosed text message with in the desired image where Patch refers necessary Unit of Steganographic textures. A patch is an image block of source texture with the option that user can specifies its size. Pa.w, Pa.h, Pa.d are patch's width, height and depth. The core part is referred as kernel block its size is denoted as K.w*K.h. where K.w is kernel block width and K.h is kernel block height. The size of texture source is denoted as S.wi*S.ht where S.wi is original source width, S.ht is the original source height. Source texture is divided into non overlapped kernel blocks where Kb referred as collection of all kernel blocks, represents amount of elements. Source patch is referred as sp in which sr.n refers amount of elements in the sp. This methodology generated candidate patches. It must be a unique one. Modules involved in hiding the information inside the image are Huffman coding based text embedding, Texture recovery, and source text extraction.

2.2 Huffman Code based Text Embedding

Steps involved in text embedding are Index table generation, Composition of patches, Text embedding and capacity calculation.

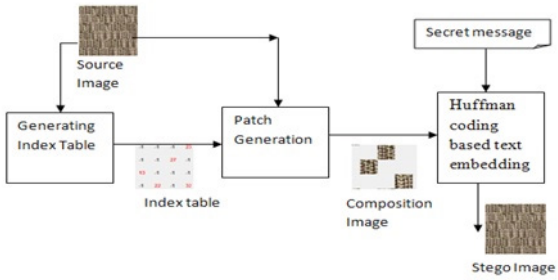

Figure 1. Block diagram for Embedding secret text.

2.2.1 Index Table Generation

The first method is the generation of index table where it generated a table of index which preserved the identity of the original texture source within the texture formed. With the help of this table, original source texture is extracted. The texture of user defined size is used for the creation of the index table.

2.2.2 Composition of Patches

The second step is attached the patches of original texture in a work table which provided composed picture. Initially this method considered an empty image as the work table wherever the scale of the work table is proportional to the original image. Concerning the original patch identity, stored the respective patch within this work table. If the imbrications of the original patch are not found, then it attached the source patches directly into the work table.

2.2.3 Text Embedding and Capacity Determination

In this step, Huffman methodology compression is carried out. It converted the text into binaries (0's & 1's). Then finally the compressed text is embedded in to the synthesized patches. Thus stego image is created which is sent to the intend receiver.

2.3 Texture Recovery

In the receiver side the text is extracted which involves the generation table of index, pullout the original texture source, and revealed the hidden text and then validated the secret text hidden in stego source. Once the table of index is created, kernel size of region K.wi*K.ht, S.wi*S.ht is used to retrieve the original source. Thus the source texture recovered is exactly similar to the original image.

2.4 Source Text Extraction and Authentication

It is the reverse of embedding process it has following steps. The primary step is text extraction and verification, the embedded text is extracted and decrypted. Then through Huffman coding the text is decompressed and retrieved. At the end, the extracted text is verified using match verification step Figure 2 shows the concealing of the data and index table generation for the given image. The figure describes the reverse process of concealing the data, where the index table is generated from the composed image. From which the source texture is extracted. Through decompression and decryption, the source text is retrieved. Thus the secret message is obtained.

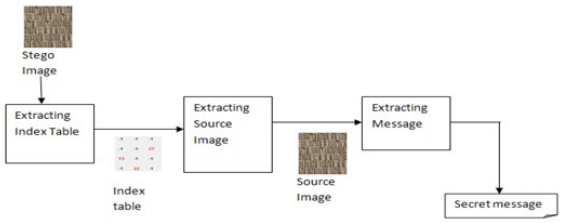

Figure 2. Extracting secret text.

3. Results and Discussions

Specified image given by the user is the input to the model. Next, index table is generated for the given input using the key given by the sender, which is a dynamic one. The location of the sources from the selected image gets stored in the table. Based on the height, width and depth of the image the values are calculated. At the receiver side the original image is extracted and the encoded text is retrieved using the same table. Patch pasted in a work table is provided the composed picture. Initially this method considered an empty image as the work table where the scale of the work table is proportional to the original texture. Concerning the original patch identity stored within this index table, attached the patch of original into the work table. The text provided by the user is encased into the image by applying Huffman coding which is the stego image. This stego image is sent to the receiver. Thus the text is transferred to receiver in a secured manner and at the receiver side the reverse process of the above mentioned steps takes place, which enabled the receiver to retrieve the source text from stego image. Additionally, the source image is also obtained without any damage. Quality of the image is evaluated using Mean Square Error of Overlapped Area which shows higher embedding capability with lesser distortions. MSEO is calculated using following formula. Where Pw is width of the patch and Ph is height of the patch,

$$\frac{1}{(P_n)P_w P_h}\sum_{i=1}^{P_n}\sum_{j\in O_i}(P_j^c - P_j^s)^2$$

MSEO =

Table 1 shows the Mean Square Overlapped Area for different types of textures, which denotes the image quality variations with embedding capacity. MSEO for pure texture, 5 bits per patch and 10 bits per patch shows that the MSEO varies with embedding capacity.

Table 1. Relation between MSEO and embedding capacity

	Peanuts	Rope net	Ganache	Metal
Pure	447.7	551.2	84.5	495.5
5 BPP	676.8	799.3	119.3	695.4
10 BPP	953.0	1227.5	218.3	996.3

4. Conclusion

In this work patch texture methodology is used for embedding process which outputs a stego image whose changes are almost impossible to perceive through naked human eye. Extracting the source texture from the stego image and extracting the hidden text from the stego image that was embedded. From experimental analysis, it is evident that the proposed methodology enhances the [12] embedding capacity which reconstructs the image with much better quality than the existing methods. It can also be concluded that patch method serves the purpose better than the other texture synthesis method in concealing the data, and providing reversibility to retrieve the source from the results and provides security. In future any other texture synthesis and steganography method can be combined together to enhance capability further.

5. References

1. Cheng YM, Wang CM. A high-capacity steganographic approach for 3D polygonal meshes. The Visual Computer. 2006 Sep; 22(9):845–55.
2. Dragoi IC, Coltuc D. Local-prediction-based difference expansion reversible watermarking. IEEE Transactions on Image Processing. 2014 Apr; 23(4):1779–90.

3. Hong W, Chen T-S, Shiu C-W. Reversible data hiding for high quality images using modification of prediction errors. Journal of Systems and Software. 2009 Nov; 82(11):1833–42
4. Witkin KM. Reaction–diffusion textures. ACM SIGGRAPH Computer Graphics.1991 Jul; 25(4):299–308
5. Image restoration using multire solution texture synthesis and image in painting [Internet]. [cited 2003 Jul 09]. Available from: http://ieeexplore.ieee.org/document/1214456/.
6. Simoncelli EP, Portilla J. Texture characterization via joint statistics of wavelet coefficient magnitudes. Proceedings of Fifth International Conference on Image Processing; 1998 Oct. p. 1–5.
7. Efros A, Leung TK. Texture synthesis by non-parametric sampling. Proceedings of International Conference on Computer Vision; 1999 Sep. p. 1–6.
8. Moulin P, Joseph A. Information-theoretic analysis of information hiding. IEEE Transactions on Information Theory. 2003 Mar; 49(3):563–93.
9. Han C, Risser E, Ramamoorthi R, Grinspun E. Multiscale texture synthesis. ACM Transactions on Graphics. 2008 Aug; 27(3).
10. Raja JN, Jaganathan P, Domnic S. A new variable-length integer code for integer representation and its application to text compression. Indian Journal of Science and Technology. 2015 Sep; 8(24):1–6.
11. Hong W, Chen T-S, Shiu C-W. Reversible data hiding for high quality images using modification of prediction errors. Journal of Systems and Software. 2009 Nov; 82(11):1833–42.
12. Ananth SV, Sudhakar P. Performance analysis of a combined cryptographic and steganographic method over thermal images using barcode encoder. Indian Journal of Science and Technology. 2016 Feb; 9(7):1–5.