International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 24 Issue 9 – JUNE 2017.

Providing Security to Online Shopping Using Credit Cards through Reversible Texture Synthesis in Steganography

Aswathy P S [#1]

[#] *M-Tech, ,Department of Information Technology,Toc H Institute of Science and Technology Kochi, Kerala, India*

***Abstract*— Due to the advancements made in the Information and Communication Technologies (ICT), security plays a major role in today's environment. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. Steganography is the art of hiding information and an effort to conceal the existence of the embedded information. In this paper, we have proposed a novel security model that suggests a way for steganography utilizing the process of texture synthesis. First, the process of synthesizing an arbitrary size of texture image can offer good embedding capacity that is proportional to the size of the stego texture image. Second, as the stego texture is composed of source texture, our proposed method is not vulnerable to any steganalytic algorithm. Third, the proposed method is able to provide the recovery of source texture back. With these advantages, the propose method will completely synthesize the source texture image and impose security over it by embedding the secret message over to it. Experimental analysis has shown the efficacy of our proposed security model.**

***Index Terms*—Steganogrpahy, hiding information, texture back**

I. INTRODUCTION

The widespread use of internet for communication has increased the attacks to users. The security of information is an important issue related to privacy and safety during storage and communication [1]. Cryptography and Steganography are two popular ways of sending vital information in a secret way. Cryptography is the method of converting plaintext into cipher text. The messages are converted into an encrypted format using a key and then this cipher text is hidden into an image, audio or video file according to the user's choice. The encryption is done using Advanced Encryption Algorithm and the key is hashed using Secure Hash Algorithm [2].

The Steganography, Cryptography and Digital Watermarking techniques can be used to obtain security and privacy of data. The steganography is the art of hiding data inside another data such as cover medium by applying different steganographictechniques. While cryptography results in making the data human unreadable form called as cipher thus cryptography is scrambling of messages [3]. Whereas the steganography results in exploitation of human awareness so it remains unobserved and undetected or intact. It is possible to use all file medium, digital data, or files as a cover medium in steganography. Generally, steganography technique is applied where the cryptography is ineffective [4].

The rest of the paper is organized as follows: Section II presents the prior work; Section III presents the proposed model; Section IV depicts the experimental analysis and finalizes in Section V.

II. PRIOR WORK

This section depicts the prior works processed by other researchers. In [5] YimoGuo proposed video texture synthesis with multi-frame LBP-TOP and diffeomorphic growth model. Two key factors, such as frame representation and blending artifacts that affects the synthesis performance. To improve the synthesis performance from two features: First, effective frame representation is used to capture both the longitudinal information in temporal domain and the image appearance information in spatial domain. Second, artifacts that reduce the synthesis quality are significantly suppressed on the basis of a diffeomorphic growth model. It aims to set up a diffeomorphic growth model to emulate local dynamics around stitched frames. In [6] L.-Y. Wei and M. Levoy present an efficient algorithm that can efficiently synthesize a wide variety of textures. The algorithm is easy to use and it generates textures with perceived quality equal to or better than those produced by previous techniques, but runs two orders of magnitude faster.

In [7] A. A. Efros proposed a non-parametric method for texture synthesis. The texture synthesis process grows a new image outward from an initial seed, consider one pixel at a time. First, chose a single pixel so that the model captures high frequency information as possible. All previously synthesized pixels in a square window around single pixel are used as the context. Using the probability tables for the distribution of single pixel, synthesis is preceded, given all possible contexts. In [8] C. Han develops a multiscale texture synthesis algorithm. A novel example-based representation, called an exemplar graph is proposed that simply requires a few low-resolution input exemplars at different scales. Exemplar graph is an input representation better suited for the multiscale setting. The nodes in the graph are exemplars, and they are connected by directed and weighted edges.

In [9] H. Otori and S. Kuriyama propose a new type of image coding method using texture image synthesis. A digital camera mounted on a mobile phone is utilized as a data input device to obtain embedded data by analysing the pattern of an image code such as a 2D bar code. Regularly arranged dotted-pattern is first painted with colors picked out from a texture sample, for having features corresponding to embedded data. This improved the quality of data-embedded textures. In [10] M. F. Cohen proposed a simple stochastic algorithm for non-periodically tile the plane with a small set of Wang Tiles for image and texture generation at runtime. Wang Tiles are squares in which each edge is assigned a color. The generation of large textures is very fast.

In [11] K. Xu et al. explore the use of salient curves in synthesizing intuitive, shape-revealing textures on surfaces. The texture synthesis is guided by two principles: matching the direction of the texture patterns to those of the salient curves, and aligning the prominent feature lines in the texture to the salient curves exactly. In [12] Liang et al. introduced the patch-based sampling strategy. The algorithm synthesizes textures from an input sample. This patch-based 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 texture patches in the sampling scheme provide implicit constraints to avoid garbage found in some textures.

In [13] Efros and Freeman proposed a method that generates a new texture by stitching together small patches of existing textures. This process is known as image quilting. It is very fast and simple texture synthesis algorithm. The generalization of the method is used to perform texture transfer. This method is extended to perform texture transfer. In [14] Ni et al. proposed a novel reversible data hiding algorithm, which can recover the original image without any distortion from the marked image after the hidden data have been extracted for embedding the data into the image. The algorithm applicable to a wide range of images such as commonly used images, medical images, texture images, aerial images and all of the 1096 images in CorelDraw database.

III. PROPOSED MODEL

A. *Problem Statement*

This study proposes an implementation of steganography using reversible texture synthesis in an online shopping system using credit cards. The secret data which is the credit card details is hidden into the texture image at sender side. It is done by generating patches from source texture and index table and composite image is generated. Message is embedded and correct data can be recovered from the cover image with no change at receiver side. Major part of system will include Texture synthesis, message embedding and source texture recovery, message extraction and message authentication. Given an original source texture, first we have to produce a large stego synthetic texture hiding the secret messages. By using a conventional patch-based method the textures are synthesized. The studywill provide reversibility to retrieve the original source texture from the stego synthetic texture, making possible a second round of texture synthesis if needed. The system to be developed will be easily embedded into the different application where security is main concern.

B. *Enhanced reverse texture synthesis model*

The proposed approach steganography using reversible texture synthesis offers three advantages. First, since the texture synthesis can synthesize an arbitrary size of texture images, the embedding capacity is proportional to the size of the stego texture image. Secondly, a steganalytic algorithm is not likely to defeat this steganographic since the stego texture image is composed of a source texture rather than modifying the existing image contents. Third, the reversible capability inherited provides the functionality to recover the source texture. Since the recovered source texture is exactly the same as the original source texture, it can be employed to proceed onto the second round of secret messages for steganography if needed.Fig.1 presents the overall system architecture.

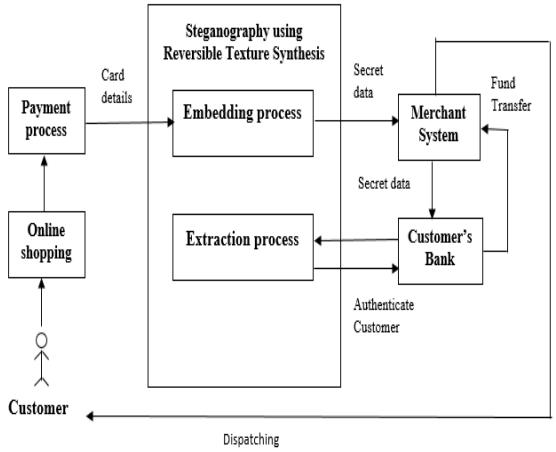

Fig.1. System Architecture

The proposed model is explained as follows:

1) Customer registration and login module:

In this module, a new customer can register in the web portal with their details such as name, address, email id, phone number, etc. The data entered by user is being passed through necessary validation checking. The customer details will be stored in the database. The users once registered can login to the system with their user id and password. Proper authentication and user verification is being done at the time of login process.

2) Shopping module:

The customer can view the items in the shopping portal. The details of the product such as product name, price, description, etc will be displayed. The user can add the items which they want to buy to their cart. The customer can add any number of items to their cart. Each item in the cart can have a product id, quantity, cost of the item, etc. Each user's cart will have a cart id and the total cost of the items in the cart.

3) Customer payment module:

Once the customer done with their shopping, they can proceed with the payment process. For this, the customer needs to provide their credit/ debit card details such as the card number, name on the card, etc. These details will be hidden from the merchant system with the process of Steganography using reversible texture synthesis.

4) Steganography using reversible texture synthesis module:

This module is divided into four sections: 1) Generating Patches 2) message embedding procedure 3) Capacity determination 4) Message extracting procedure.

C. Generation of patches

The basic unit used for the steganographic texture synthesis is referred to as a patch. A patch represents an image block of a source texture where its size is user-specified. We can denote the size of a patch by its width (Pw) and height (Ph). A patch contains the central part and an outer part where the central part is referred to as the kernel region with size of Kw×Kh, and the part surrounding the kernel region are referred to as the boundary region with the depth (Pd). Fig.2 represents the generation of patches.

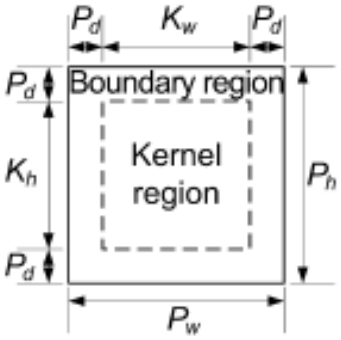

Fig.2. Generation of patches

A source texture with size of $S_w \times S_h$ can be subdivided into a number of non-overlapped kernel blocks, each of which has the size of $K_w \times K_h$, as in Figure 4.4. Let KB represent the collection of all kernel blocks thus generated, and ‖KB‖represent the number of elements in this set. The indexing for each source patch $k_{bi}$is employed as KB = { k_{bi} | i = 0 to ‖KB‖- 1} . We can expand a kernel block with the depth $P_d$at each side to produce a source patch. Figure 3 indicates the source patch sp_4obtained when kernel block kb_4 is expanded.

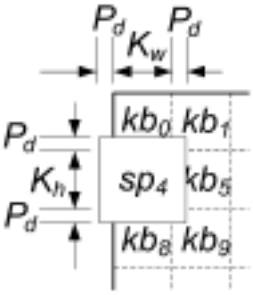

Fig.3. Source patch

1) Message embedding procedure

Message embedding procedure contains the following modules 1) Index Table Generation, 2) Composition Image Generation, 3) Data Encryption 4) Pixel Oriented embedding with Texture Synthesis. Fig.4 shows the flowchart of the message embedding procedure.

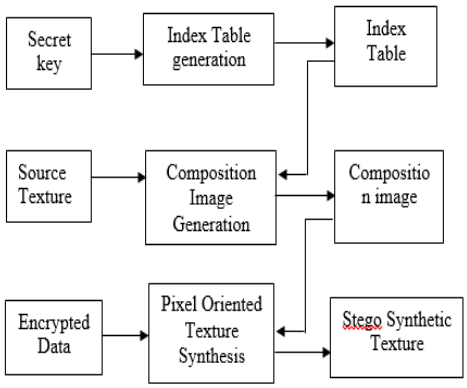

Fig.4 Flowchart of Message Embedding Procedure

This index table allows us to access the synthetic texture and retrieve the source texture completely. This reversible embedding style is the major advantage of the proposed system. The dimension of the index table (Tpw × Tph) is first determined. Given the parameters Tw and Th, which are the width and the height of the synthetic texture we intend to synthesize, the number of entries in this index table can be determined using equation (1) where TPn denotes the number of patches in the stego synthetic texture.

$$TP_n = T_{pw} \times T_{ph} = \left\lfloor \frac{(T_w - P_w)}{(P_w - P_d)} + 1 \right\rfloor \times \left\lfloor \frac{(T_h - P_h)}{(P_h - P_d)} + 1 \right\rfloor \quad (1)$$

Second step of message embedding procedure is to paste the source patches into a workbench to produce a composition image. For that a blank image has to establish as the workbench where its size is equal to the synthetic texture. Then paste the source patches into the workbench based on the source patch ID stored in the index table to produce a composition image. If no overlapping of the source patches is found, then patches can be attached directly into the workbench. If pasting locations cause the source patches to overlap each other, then an image quilting technique is employed to reduce the visual artefact on the overlapped area. Next step is to encrypt the secret message. Advanced Encryption Standard (AES) is used for encrypting the secret message. AES is based on substitution and combination and it is fast in both software and hardware. After the encryption of the message, the message can embedded pixel by pixel during the texture synthesis process to produce synthetic texture.

2) Capacity Determination

The embedding capacity is important for data embedding scheme. Embedding capacity of the algorithm depend on the capacity of bits that can be concealed in each patch (BPP, bit per patch), and the number of patches which is embedded in the stego_synthetic texture (EP_n). Every patch can hide at least 1 bit of the secret data; thus, the lower bound of BPP will be one, and the maximal capacity in bits that can be concealed at each patch is the upper bound of BPP, as denoted by BPP_{max}. The total capacity that the proposed scheme can offer is shown in equation (2) which is the multiplication of BPP and EP_n. The number of the embeddable patches is the difference between the number of patches in the synthetic texture (TP_n) and the number of source patches subdivided in the source texture (SP_n).

$$TC = BPP \times EP_n = BPP \times (TP_n - SP_n) \quad (2)$$

1) Message extraction Process:

The message extracting for the receiver side involves

generating the index table, retrieving the source texture, performing the texture synthesis, and extracting and authenticating the secret message concealed in the stego synthetic texture. Fig.5. shows the flowchart of the message embedding procedure.

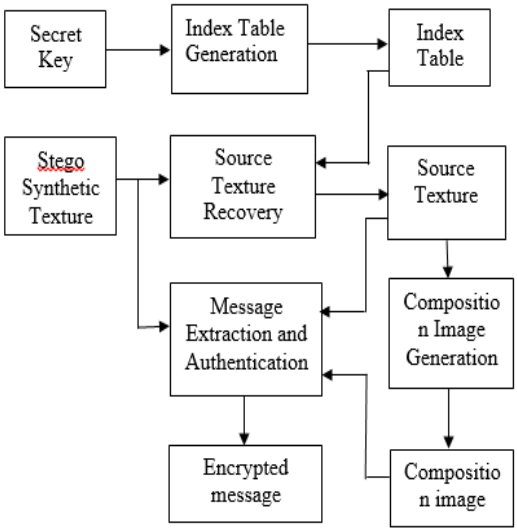

Fig.5. Flowchart of message extraction procedure

To extract the original message, appropriate patch is extracted from the composition image. The patch contains encrypted data. The extraction of patch is done byreferring the index table. The index table tells where the patch in the image is pasted and based on this information the patch is extracted from the composed image. Once the patch is extracted, the next task is to decrypt the encrypted message. The main reason behind encrypting the message is to provide high security to the confidential data. So with the encrypted message, the third person is not able to detect the contents inside the message body unless and until they have the corresponding decryption key with them.

3) Transaction and dispatch module

The details provided by the customer are being forwarded to their bank. The bank server uses the message extracting procedure of steganography using reversible texture synthesis to extract the details provided the customer. Using these details, the bank checks whether the card holder is authorized or not. If the credit/debit card holder is authorized, the bank checks whether there is enough fund in the customer's account to buy the selected items in the shopping cart. If so, the amount required to buy the items selected by the customer is being transferred to the merchant's account from the customer's bank account. Upon receiving the payment, the merchant system dispatches the items selected by the customer.

IV. EXPERIMENTAL ANALYSIS AND RESULTS

The proposed method steganography using reversible texture synthesis is demonstrated by a texture image using MATLAB tool. The example demonstrates the message embedding and message extraction.

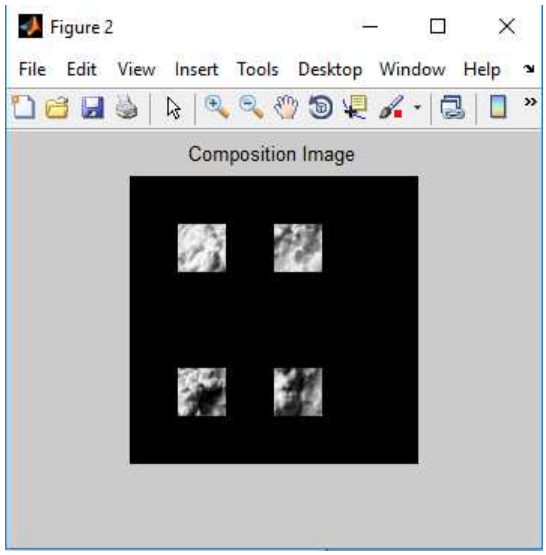

Fig.6. Composition of generated images

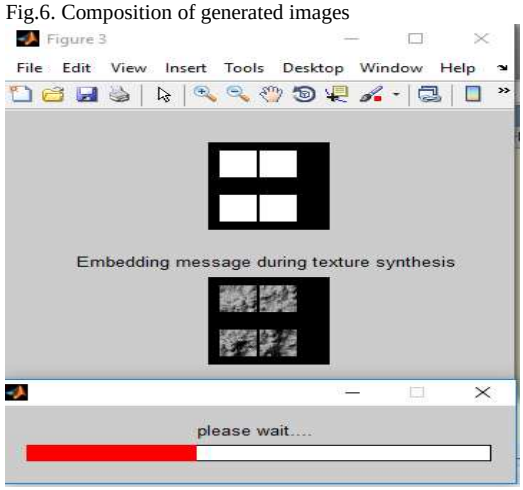

Fig.7. Message Embedding process

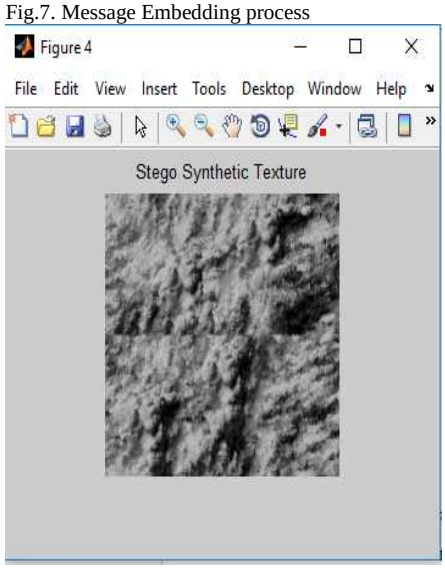

Fig.8. Stego Synthetic Texture

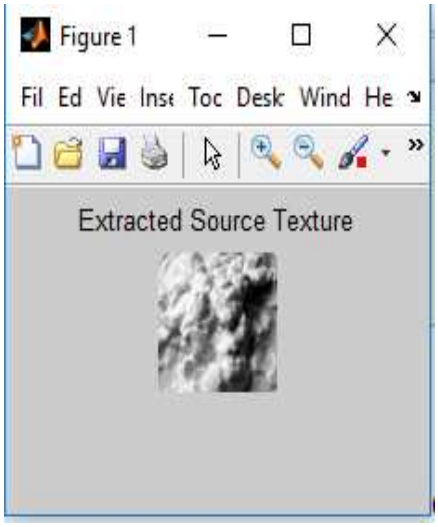

Fig. 9 Extracted Source Texture

Synthetic Texture Size : 1008 ×1008; Patch Size: 48 ×48		
$S_w \times S_h$	**No of source patches SP_n**	**Embedding Capacity in bits**
96 × 96	I. 4	II. 1006848
128 × 128	III. 9	IV. 995328
192 × 192	V. 16	VI. 979200
Synthetic Texture Size : 1024 ×1024 ; Patch Size: 24 ×24		
96 × 96	VII. 16	VIII. 1039360
128 × 128	IX. 25	X. 1034176
192 × 192	XI. 64	XII. 1011712

TABLE 1. ANALYSIS OVER EMBEDDING CAPACITY

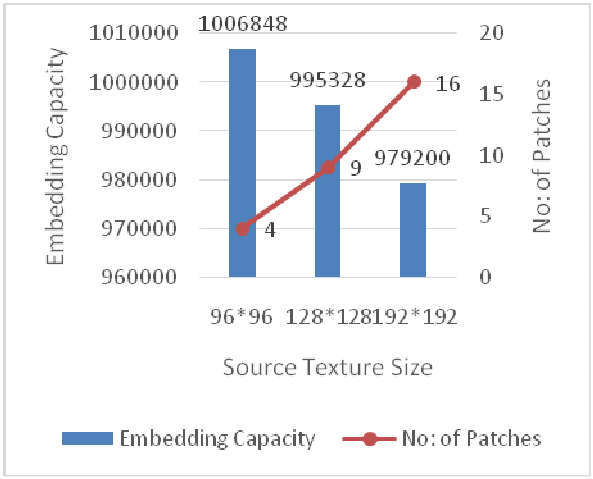

Fig. 10. Chart showing Embedding capacity and no. of patches when source texture size is 1008 × 1008

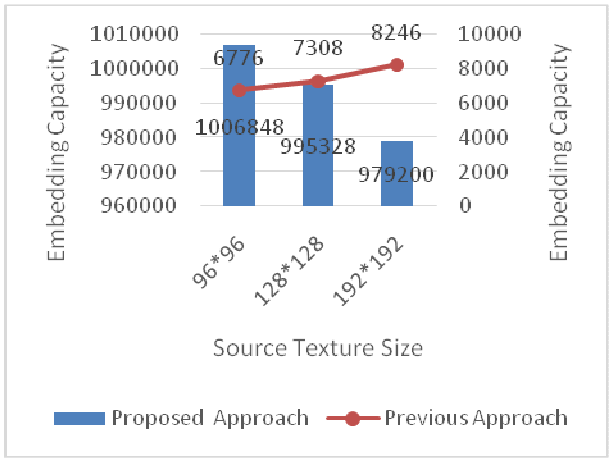

Fig.11. Chart showing comparison of Embedding Capacity

Then the image quality is analyzed by estimating PSNR values. The higher the PSNR, the better the quality of compressed or reconstructed image. Fig.12shows the result of the PSNR value calculated between the original texture and extracted texture. It shows that the PSNR value is infinity. It means that quality of the image is very high, i.e. the source texture has been recovered successfully.

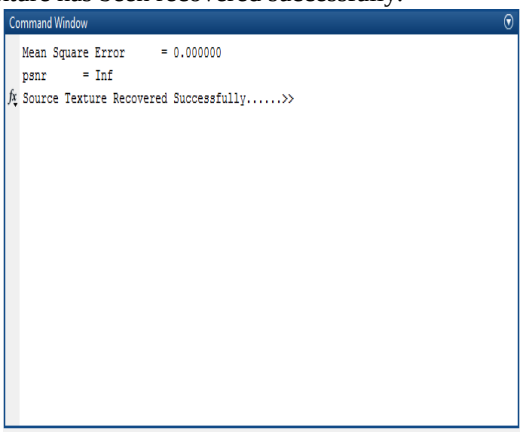

Fig.12. PSNR calculation

V. CONCLUSION

The approach Steganography using Reversible Texture Synthesis isweaved into an Online Shopping Application that uses credit cards as the mode of payment. It provides security to the confidential details of the customer. By encrypting the confidential data of the customer, double security can be provided to the system. This Steganography method minimizes the distortions during embedding process and produce visually plausible texture to reduce the probability of discovering the confidential data from unauthorized users. When comparing with the previous approach, this approach provides good embedding capacity. The proposed system is much more robust against any kind of attack and provides high degree of security to the confidential data hidden inside the texture. With this system, the confidential data cannot be accessed by any person except the authorized person and who is having a secret key with him/her. The proposed method Steganography using reversible texture synthesis is applied onto an online shopping system that uses credit cards as their mode of payment.Performance analysis is experimented in terms of efficiency of embedding capacity and image quality.

REFERENCES

[1] N. F. Johnson and S. Jajodia, “Exploring steganography: Seeing the unseen,” Computer, vol. 31, no. 2, pp. 26–34, 1998.
[2] N. Provos and P. Honeyman, “Hide and seek: An introduction to steganography,” IEEE Security Privacy,vol. 1, no. 3, pp. 32–44, May/Jun. 2003.
[3] Y. Guo, G. Zhao, Z. Zhou, and 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.
[4] 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.
[5] 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.
[6] C. Han, E. Risser, R. Ramamoorthi, and E. Grinspun, “Multiscale texture synthesis,” ACM Trans. Graph., vol. 27, no. 3, 2008, Art. ID 51.
[7] H. Otori and S. Kuriyama, “Texture synthesis for mobile data communications,”IEEEComput. Graph. Appl., vol. 29, no. 6, pp. 74–81, Nov./Dec. 2009.
[8] M. F. Cohen, J. Shade, S. Hiller, and O. Deussen, “Wang tiles for image and texture generation,” ACM Trans. Graph., vol. 22, no. 3, pp. 287–294, 2003.
[9] K. Xuet al., “Feature-aligned shape texturing,” ACM Trans. Graph., vol. 28, no. 5, 2009, Art. ID 108.
[10] 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.
[11] A. A. Efros and W. T. Freeman, “Image quilting for texture synthesis and transfer,” in Proc. 28th Annu. Conf. Comput. Graph. Interact. Techn., 2001, pp. 341–346.
[12] 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.
[13] R. Rejani,D. Murugan and Deepu V. Krishna―Pixel pattern based steganography on images‖ journal on image and video processing, feb 2015, volume: 05, issue: 03
[14] [14] Kuo- Chen Wu and Chung-Ming Wang, “Steganography Using Reversible Texture Synthesis”, IEEE Transaction On Image Processing ,vol.24,no.1, January.2015.