Steganography With Reversible Texture Synthesis Method for Embedding Data

Ms. Swapnali Bhujbal[1], Prof. P.B. Sahane[2]
Department of Computer Engineering
[1]Research Scholar, PK Technical Campus, Pune, India.
[2]Professor , PK Technical Campus, Pune, India.

Absract: *A steganography is an art of hiding confidential data into digital media such as image, audio, video, etc. Here we are going to combine the work of steganography long with image processing. To do this a texture synthesis process is used which resamples input texture image to create a new texture synthesis image. It provides a secure data embedding efficiency because the size of the cover image is vary depends upon the secret message .this will make to store large amount of information. The stegno analytic algorithm is used to extract the secret message from source texture. The distortion of image is very low in our proposed system. Reducing distortion is the crucial issue in existing method this will handled by our system. These system can embed the size of the image and provide high quality image which avoids the distortion of image quality which the existing system can not. The proposed system is much more robust against any kind of attack and provide high degree of security to the confidential data hidden inside the image patches. The proposed system can be combined with other steganographic systems to provide high degree of security. With this system the message can not be accessed by any person except the authorized person and who is having a secure key with him.*

Keywords-Steganography, Texture synthesis, Revercible, Cryptography.

I. INTRODUCTION

Previous days, for the security of the secret Messages cryptography was used. Cryptography converts the secret message into ciphertext. But sufficient security was not provided to the massages. So we use steganoghraphy. Steganography is an art of hiding existence of the data in another transmission medium to achive the secret communication. Steganography method is used in this paper is based on reversible texture synthesis process. There are various steganographic algorithms are available in literature which provides high amount of security with lower distortion. In this paper, texture synthesis process is widely used which takes source texture image as an input and create the new stego synthesized image as an output. The stego synthetic image is a composition of secret message as well as the source texture image. This approach have three main advantages: (1) Preliminary process of synthesizing the texture image of an arbitrary size can offer an optimal embedding capacity which is proportional to the size of stego structured image. (2) as the stego structural image is composed of source texture , our proposed system is not vulnerable to any kind of hazards generated in steganalatic algorithms. (3) Most importantly, a proposed system can inherit various functionalities to revert the source texture back. The steganography is an art of hiding existence of the data in another transmission medium to achieve the secret communication. It is not the replacement for the cryptography but rather it boosts the security. Steganography method used in this system is based on reversible texture synthesis process. In the typical steganography process two parties try to make secure communication and whose success depends on detecting the existence of the communication. Moreover a steganography is a mechanism which conceals the secret messages inside other compatible media so that any enemy could not be able to detect it. Here the objective is a typical steganographic application includes covert communications between two parties whose existence is unknown to a possible attacker and whose success depends on detecting the existence of this communication.

II.LITERATURE SURVEY

This section contains the evaluation of different methods prefered for steganography construction for security of data.

The working of steganography with reversible texture synthesis is discussed by Kuo-Chen Wu and chung-Ming Wang in “Steganography using Reversible Texture Synthesis” [1]. This uses the patch based approch in which secret message is made hidden.

The main working of steganography is discussed by the Provos and P. Honeyman in “Hide and Seek: An introduction to steganography, Security, Privacy”[2]. This elaborates working of steganography. Steganography is nothing but hiding the confidential data into digital media such as image, audio, video. It only emphasis on working on steganography.

A high capacity steganographic approaches are discussed by the Y.-M. Cheng and C.-M. Wang in "A High capacity steganographic approach for 3D polygonal meshes"[3]. In this fo high capacity approach a modified multilevel embed procedure that can embed at least three bits per vertex with little visual distortion.

The pixel based approach is discussed by the A.A. Efros and T.K. Leung in "Texture synthesis by non-parametric sampling" [4]. In this the working of pixel based approach is given. In pixel based approach the hiding of confidential message is done by encoding the message into pixels. Each output pixel is determined by the already synthesized pixels.

The LSB algorithm is discussed by the S.C. Liu and W.H. Tsai in "Line Based cubism- like image a new type of art image and its application to lossless data hiding"[5]. This paper elaborates steganography using LSB algorithm. In this Least Segnificant Bit of the image is replaced with the bit of the message. with this approach size : clearity ratio is maintained.

III.PROPOSED APPROACH FRAMEWORK AND DESIGN

Steganography is the art and the science of writing hidden messages in such a way that no one, apart from the sender and intended receiver, Assume the existence of the message, a form of security through obscurity. The word steganography is of the Greek word which means "covered writing" from the Greek words steganos meaning "covered or protected", and graphei meaning "writing".Search[7].

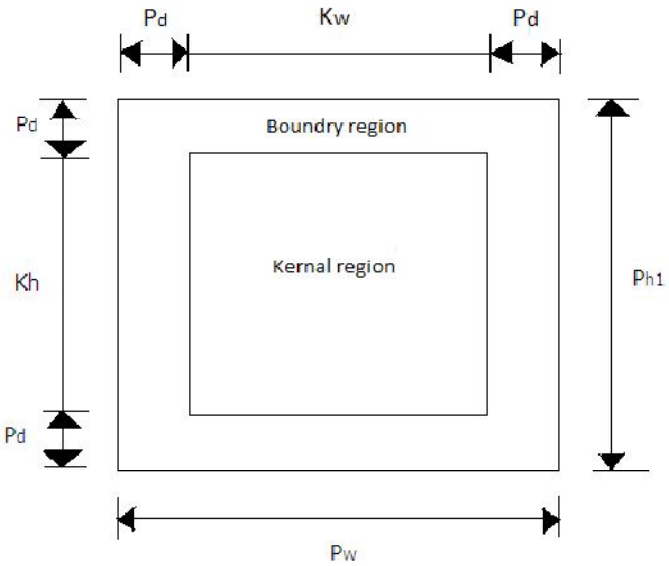
The computer based steganography, images, audio files, documents, and even three-dimensional (3D) models are all serve as innocent looking hosts for secret messages. With the development of various 3D applications and computer animation, many steganography and watermarking schemes have been presented for 3D models. This paper presents a high-capacity steganographic approach for 3D polygonal meshes. This method first uses a modified multi-level embed procedure that can embed at least three bits per vertex with short visual distortion. Furthermore, a new representation rearrangement procedure based on the representation domain to achieve the higher capacity with no visual distortion. Psychological studies show that context under which information accessed before can serve as a powerful cue for information recall, as it is always easier to remember than detailed information content itself[5].

In the pixel based texture synthesis process , we first construct blank image from the given input image. The blank image will act as a workbench where we hide the secret message. In this process the secret message to hide is first encoded by glowing some of the pixels of blank image, the rest of the pixels are coated on that blank image based on the input image.[9]

These system give emphasis on hiding the data using LSB algorithm. The LSB stands for Least Significant Bit algorithm. In this we divide the image into no of bits and store these bits into byte array. The secret message is also divided into bits. We take each bits of the secret message and replace that with least significant bit of the image. With this approach we can be able to hide secret information but if the size of the message is increased then it leads to image distortion.

The proposed steganography process uses the patch based algorithm.The patch based algorithm works as follows:

1. Take the input image:- We call the input image as source texture image. This image may be captured in a photograph or drawn by an artist to create synthesized texture image which is having similar appearance.
2. Create the blank image from the given input image:- The purpose of creating the blank image from the input image is that the blank image is going to act as workbench where the patches will be pasted at the end.
3. Divide the input image into no. of patches:- First the input image is divided into no. of patches. Each patch is having two areas
   - Kernal boundary
   - Region boundary



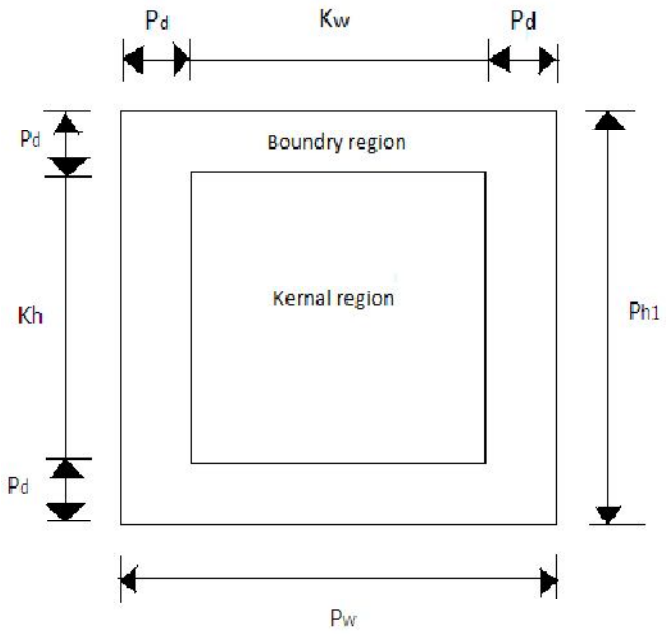


Fig.1 Block diagram of patch

As shown in the above figure Kw and Kh represents the size Pw represents the depth of patch.

4. Generate the index table:- The index table stores the location information of source patch set SP in the synthetic texture. The index table allows us to access the synthetic texture and retrieve the source texture completely. While generating index table we need to provide the secret key for the authentication purpose.

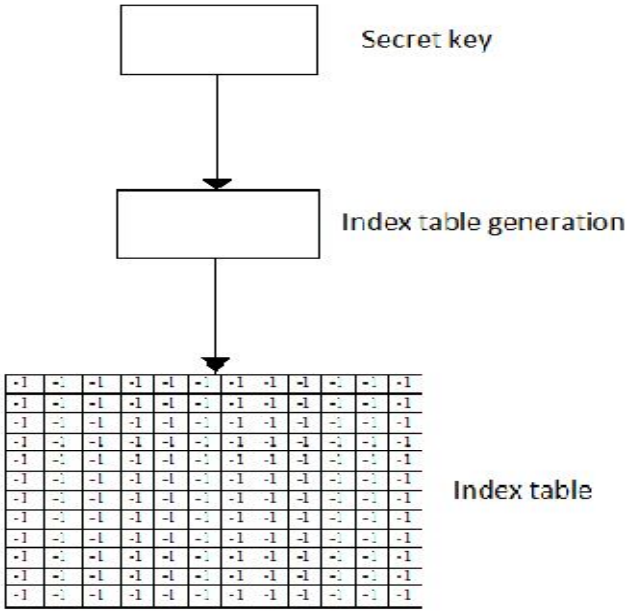


Fig.2 Index Table Generation

As shown in the figure above, initially the entry in the index table is -1 which represents that it is empty. We provide the patch ID to each of the patch and then change the entry in the index table by the patch ID and randomly paste the patches onto the blank imagecalled as workbench.

5. Composition image generation:- In this module we construct synthesized image which is a combination of different patches. To construct the synthesized image , appropriate candidate patches must be selected from the patch list. To select the patch the index table is referred which tells where to paste the in the blank image. The entries represented by green color in index table indicates the patch ID and tells the position where the patches are pasted onto blank image.

6. Message oriented texture synthesis:- In this module we create stego synthetic texture image which conceals a secret message. To construct stego synthetic image , first the message is converted into bytes and taken as input to message oriented texture synthesis process. Along with this source texture image and composition image is also taken as input to this process.

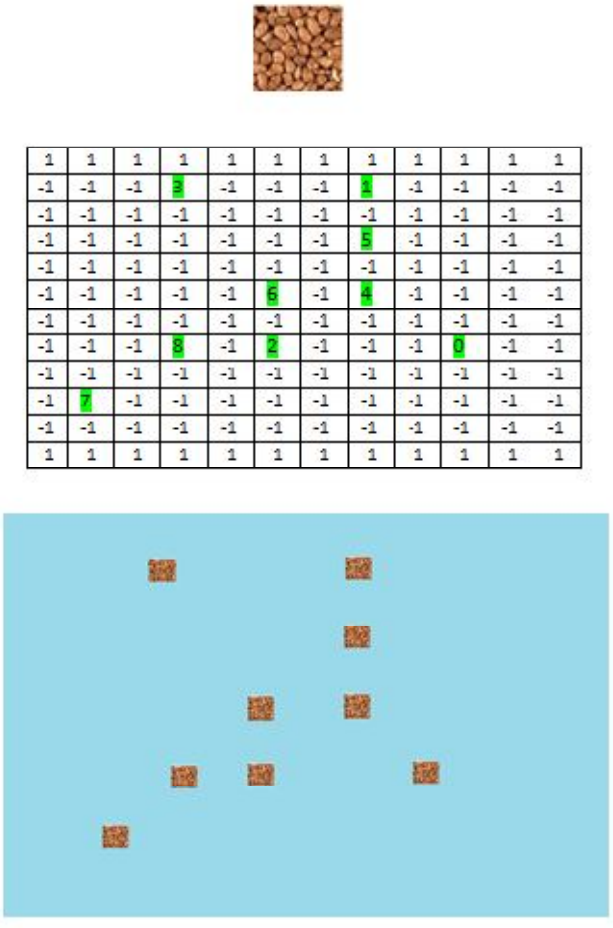


Fig.3 Illustration of composition image

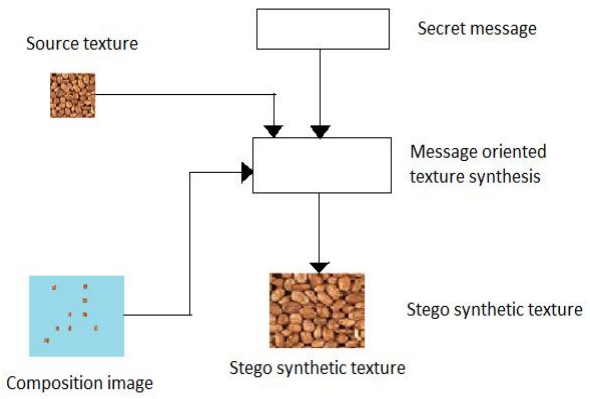


Fig.4Generation of stego synthetic image

V. IMPLEMENTATION

System Architechture:

Algorithm:

- Image steganalytic algorithm
- pixel-based algorithm

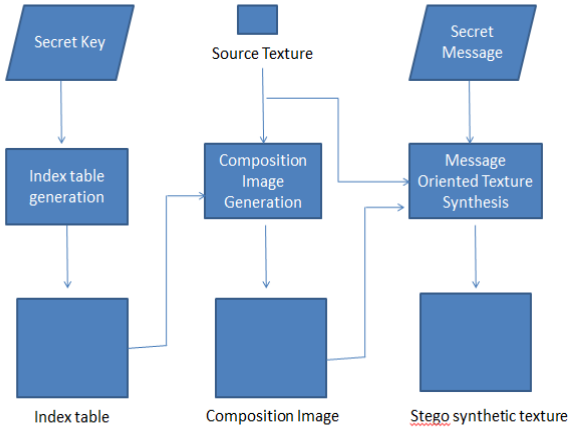


Fig.5 Architechture of Proposed System

Typical image steganography process reduces the image quality as if the size of secret message is large enough .So in the existing steganography technique it is expected that the size of the data must match the size of the image. If the size exceeds, it leads to image distortion. Our proposed approach provides high quality image even if the size of the secret message is much large and reduces the image distortion.

In this section, we see the actual implementation of our work.We divided our work in different 5 parts,

(1)Embedding,
(2)Image Composition,
(3)Source Patch Identification,
(4)Extracting Secrete Message,
(5)Performance Analysis.

1) Embedding

In the embedding, secret message is set in the one patch of the image by using the DCT (Discrete Cosine Transform). By using DCT, the input texture is decomposed. The main thing is that the secret message is always stored in the low coefficient of the image. The discrete cosine transform is applied on the image to embed the message in the image.

2) Image Composition

Image composition contains another 2 parts, (1) Index Table Generation, (2) Pasting the Image Patches.

A) Index Table Generation

The source texture of the message is placed on the image matrix with the help of index table. The index table acts as a key for image composition. The patch which contains the starting point of the message is placed in the first location and in index table and so on. Also the locations which do not have the secret message denoted by -1 in the index table.

B) Pasting the Image Patches

The index table is acts as a key for the extraction of the secret message. The index location which contains -1 value are replaced with the help of original image patches. And the another locations which contains value 1 are replaced with embedded image that contains secret message. Now the resulting image is composited image with secret message hided.

3) Source patch Identification

When we reverse the same image composition process, the source patch is get identified. The values present in the index table acts as a key for the identification of source patch. The patches in the image region which are having index table value as -1 are identified as the source patch. The source patch generator will transform the vulnerable source code by generating a vulnerability source code patch. It prevents the secret message from the external problems.

4) Extracting Secret message

The image patches that are having the values 1 contains the secret message. The secret message is retrived by reversing the embedding process.Here, we use Resulting source patch, DCT Coefficient of the image, Input secret

message, By using that the secret message is arranged so the hided message is retrived. The arrangement is done by placing extracted secret message in the order corrosponding to the order denoted in the index table.

5) Performance Analysis

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

BPPmax=[log2[Sw-Pw+1)*(SH-PH+1)]]
Where,
BPPmax - Bits Per Pixel

In this eq, we take the height and width of the source patch and height and width of the patch. The BPP value and the Total capacity value should be high which indicates that the embedding capacity of our work is high.

A. Mathematical model using Set Theory

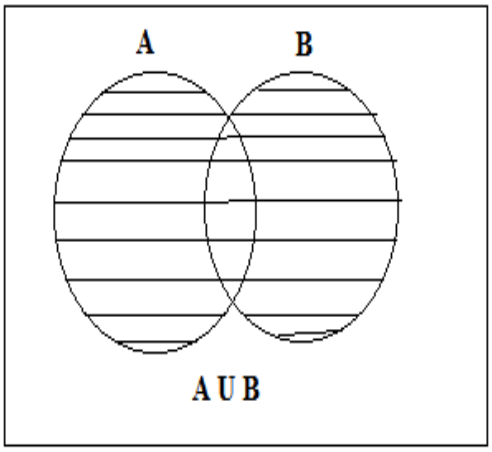
Set theory:-

A set is defined as a collection of distinct objects of same type on class of objects. The object of a set are called elements or members of the set. Object can be number, alphabet, names etc.

E.g.:-A= {1, 2, 3, 4, 5}

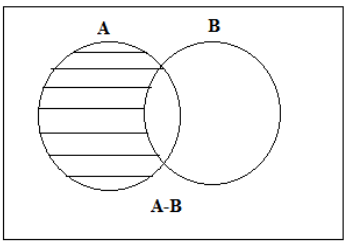
Union of sets:-

Union of two sets A & B is defined to be the set of all those elements which belongs to set A or set B or both and is denoted by A U B



Difference of sets:-

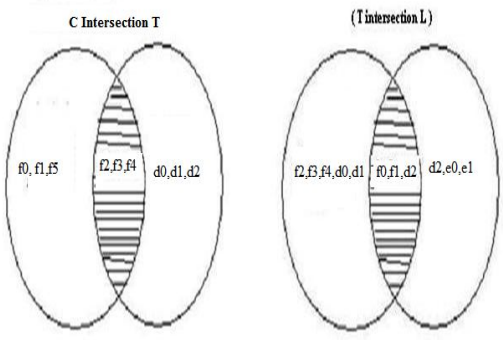
Union of two sets A & B is defined to be the set of all those elements which belongs to set A but do not belong to set B and is denoted by A-B



Set theory applied to the project:-
Sender Module:-
Set (C) = {f0, f1, f2,f3,f4,f5}
f0= Enter User name.
f1=Enter password.
F2= Enter secrete key
F3=Insert source texture
F4= Enter secrete message
F5= send the texture to receiver.
Stego Texture Generation:-
Set (T) = {f2,f3,f4,d0,d1,d2}
d0= Generate index table.
d1= Generate composite image.
D2= Embed secrete message to image.
Data retrieval Module:-
Set (L) = {f0,f1,d2,e0,e1}
e0= Retrive source texture.
e1= Extract secrete message.
Union and Intersection of project:-
Set (C) = { f0, f1, f2,f3,f4,f5}
Set (T) = { f2,f3,f4,d0,d1,d2}
Set (L) = { f0,f1,d2,e0,e1}

Venn Diagram:-

(CU TUL)={ f0, f1, f2,f3,f4,f5, d0,d1,d2, e0,e1}
(C intersection T)= { f2,f3,f4}
(T intersection L) = { f0,f1,d2}



B. Module Description:

1. Stegnography Process:

In this module, Steganography uses characteristics of English language such as inflection, fixed word order and use of peri phrase for hiding data rather than using properties of a sentence. The flexibility and freedom from the point view of the sentence construction but it increases computational complexity.

2.Encoding:

Representation of the each letter in secret message by its equivalent ASCII code. Conversion of the ASCII code to the equivalent 8 bit binary number. Division of the 8 bit binary number into two 4 bit parts. Choosing of suitable letters from the table 1 corresponding to the 4 bit parts. Meaningful sentence construction by using letters obtained as the first letters of the suitable words. Encoding is not case sensitive.

3.Decoding Steps:

First letter in each word of the cover message is taken and represented by the corresponding 4 bit number. 4 bit binary numbers of combined to obtain the 8 bit number. ASCII codes are obtained from the 8 bit numbers. Finally the secret message is recovered from the ASCII codes.

4.Transaction Online Shopping:

In this module traditional online shopping consumer selects the items from online shopping portal and then is directed to the payment page. Online merchant may have its own payment system or can take advantage of the third party payment systems such as the PayPal, pay online system, Web money and others. In the payment portal consumer submit his or her credit or debit card details such as the credit or debit card number, name given on the card, expiry date of the card.

5. Customer Authentication:

Customer unique authentication is the password for connection to the bank is hidden inside a cover text using the text based Steganography method. Customer authentication information (account no) in the connection with merchant is placed above the cover text in its original form. Now a snap shot of the two texts is taken. From the snapshot image, two shares are generated using visual cryptography. Now one of share is kept by the customer and the other share is kept in the database of the certified authority.

6. Certification Authority Access:

During the shopping online, after selection of the desired item and adding it to the cart, preferred payment system of the merchant directs the customer to the Certified Authority portal. In the portal, shopper submits to its own share and the merchant submits its to the own account details. Now the CA combines the its own share with the shopper's share and obtains the original image. From CA now, the merchant account details or cover text are sent to the bank where customer authentication password is recovered from the cover text.

7. Final Authenticated Information Results:

Customer authentication information is sent to the merchant by CA. The receiving customer authentication password, bank matches it to the its own database and after verifying legitimate customer, transfers fund from the customer account to the submitted merchant account. After receiving the fund, merchant's payment system validates receipt of payment using customer authentication information.

VI. WORK DONE

In this section, we see the actual work done. Here we provide the security to important information.

In proposed system provides high quality image even if the size of the secret message is much large and reduces the image distortion. One possible future study is to expand our scheme to support other kinds of texture synthesis approaches to improve the quality of the image for synthetic textures. Another possible study would be to combine other steganography approaches to increase the embedding capacities.

VII. CONCLUSION AND FUTURE WORK

This paper proposes a steganographic techniques by using the reversible texture synthesis. Here in steganography the secrete message is firstly encrypted and then this encrypted message is hided inside the image. For hiding the information in the image we use the patch based stegnography, in which the image is divided in the patches and every patch contains the secrete encrypted message. Our message is converted in the ASCII code so the information in the image is in the form of "0" and "1".Our proposed system also maintains the constant ratio between the message size and image quality.In the future work, we can send the secrete message by using the videos also. Means we can store the secrete message inside the videos. To provide more security to the secrete information we can use MD5, RSA algorithms.

ACKNOWLEDGEMENT

The satisfaction that a companies the successful completion of any task would be incomplete without mentioning the people who make it possible. We are greateful to the number of individuals, faculty members, whose professional guidance along their encouragement have made it very pleasant to undertake this work. We would like to express our special thanks of gratitude to Prof. P.B. Sahane for her enthusiastic assistance in improving the clarity of this work.

REFERENCES

[1] Kuo-Chen Wu and Chung-Ming Wang Steganography Using Reversible Texture Synthesis IEEE Transactions on image processing vol: 24 no: 1 year 2015
[2] S.-C. Liu and W.-H. Tsai, Line-based cubism-like imageA new type of art image and its application to lossless data hiding, IEEE Trans. Inf.Forensics Security, vol. 7, no. 5, pp. 1448-1458, 2012.
[3] H. Otori and S. Kuriyama, Texture synthesis for mobile data communications, IEEE Computer. Graph. Appl., vol. 29, no. 6, pp. 74-81,2009.
[4] H. Otori and S. Kuriyama, Data-embeddable texture synthesis, in Proc.of the 8th International Symposium on Smart Graphics, Kyoto, Japan,2007, pp. 146-157.
[5] Y.-M. Cheng and C.-M. Wang, A high-capacity steganographic approachfor 3D polygonal meshes, The Visual Computer, vol. 22, no. 9, pp.845-855, 2006.
[6] 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, 2006.
[7] N. Provos and P. Honeyman, Hide and seek: an introduction to steganography, Security Privacy, IEEE, vol. 1, no. 3, pp. 32-44, 2003.
[8] L.-Y.Wei and M. Levoy, Fast texture synthesis using tree-structured vector quantization, in Proc. of the 27th Annual Conference on Computer Graphics and Interactive Techniques, 2000, pp. 479-488.
[9] A. A. Efros and T. K. Leung, Texture synthesis by non-parametric sampling, in Proc. Of the Seventh IEEE International Conference on Computer Vision, 1999, pp. 1033-1038.25