International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 07 | July-2016 www.irjet.net p-ISSN: 2395-0072

"Steganography Using Reversible Texture Synthesis Method for Embedding Data."

Vikas D. Chavan, Prof. D. S. Uplaonkar

ME-II Student,Department of Computer Engineering,JSPM's Rajarshi Shahu School of Engineering &Research,Narhe,Pune, Maharashtra, India.
Assistant Professor,Department of Computer Engineering,JSPM's Rajarshi Shahu School of Engineering &Research,Narhe,Pune, Maharashtra, India.

Abstract - *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 project 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.Existing steganography process is much expensive and not so robust because if the size of the secret message increases it results into distortion of the image. A texture synthesis process provides embedding capacity so that to hide the large message. With the texture synthesis process the blank image is constructed from input image and the input image is divided into no. of different patches. These patches are given a patch ID and randomly pasted on the blank 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 opposed system. Reducing distortion is the crucial issue in existing method this will overcome 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— Data embedding, example-based approach, Changable, steganography, texture synthesis.

1.INTRODUCTION

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.

There are various steganographic algorithms available in the literature which provides high amount of security with lower distortion. But these algorithms are quite harsh to implement as they fail to provide robustness.

In this system texture synthesis process is widely used which takes source texture image as an input and creates 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 consistent size can offer an optimal embedding capacity which is proportional to the size of stego structured image.

2. As the stego structured image is composed of source texture, our proposed system is not vulnerable to any kind of hazards generated in steganalytic algorithm.

3. Most importantly, a proposed system can inherit various functionalities to revert the source texture back.

With above advantages, the proposed system will be full-fledged to synthesize source texture image and impose security over it by embedding the secret message over to it.

2.OBJECTIVE

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.

3.RELATED WORK

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

1.Kernal boundary

2.Region boundary

4. Generate the index table.

The index table stores the location information of source patch set SP in the synthetic texture. The index table allow 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.

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 piece ID and tells the position where the pieces 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 andcomposition image is also taken as input to this process.

3. EXISTING 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.

In contrast to using an existing cover image as to the hide messages, our algorithm cover the source texture image and embeds secret messages through the process of texture synthesis. A typical steganographic application includes to covert the communications between two parties whose existence is unknown to a possible attacker and the success depends on the detecting the existence of the communication

Most image steganographic algorithms adopt the existing image as a cover medium. The expense of embedding secret messages into this cover image is the image distortion meet in the stego image.

4. PROPOSED SYSTEM

The proposed system algorithm can provide various numbers of embedding capacities, produce a visually possible the texture images or recover the source texture. The proposed an image reversible data hiding algorithm which can recover the cover image without as any distortion from the stego image after the hidden data have been extracted. The basic unit used for our steganographic texture synthesis is referred to as the patch.

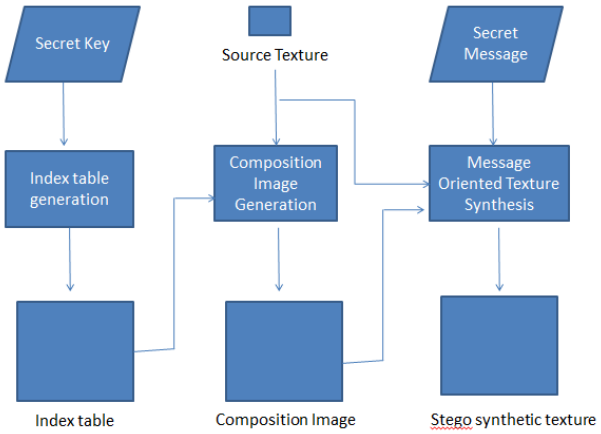


Fig.1. Architecture of proposed system

Our approach offers three distinct advantages. First, our scheme offers the embedding capacity that is corresponding to the size of the stego texture image. Second, a steganalytic algorithm is the not likely to the defeat our steganographic approach. Third, the reversible capability inherited from our scheme to provides the functionality which allows to the recovery of the source texture.

A.Mathematical model using Set Theory

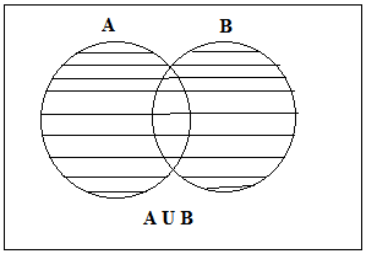
Set theory:-

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}

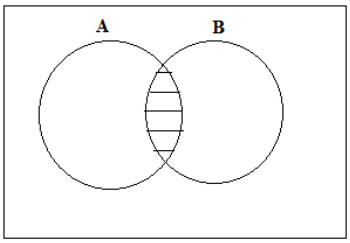
Union of sets:-

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



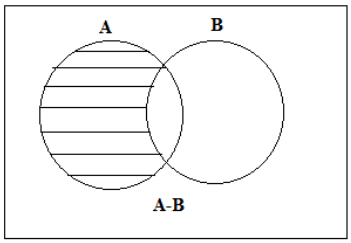
Intersection of sets:-

Intersection of two sets A & B is defined to be the set of all those elements which belongs to set A and set 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}

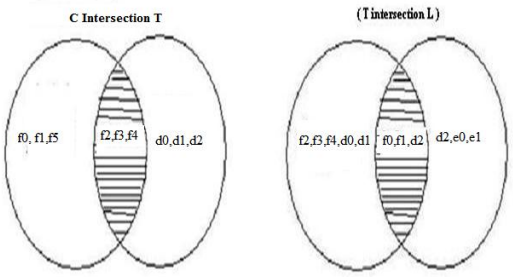
Set (L) = { f0,f1,d2,e0,e1}

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.

5.ALGORITHM

The large number of image steganographic algorithms have been investigate with the increasing popularity and use of digital images.

- **Algorithm:**
- Source Patch Generation
- Index Table Generation

1. Source Patch Generation:

I. Size (Patch) = (Pw) *(Ph).

Where (Pw) is width of patch and (Ph) is height.

II. Size (Kernel) = Kw×Kh,

Where Kw and Kh is width and height of kernel region.

III. Source Texture T= Sw×Sh

IV. Divide T into non overlapping kernel block of size Kw×Kh

||KB||= {kb0, kb1, …, kb1n}.

V. SP={spi| i = 0 to ||SP||-1}.

Where SP -source patches.

Vi. Source Patches required is,

SPn= Sw/ Kw* Sh/ Kh.

2. Index Table Generation Process:

1. Dimension Of Index Table is given as (Tpw×Tph)
2. Total Number Of patches can be calculated as follow:

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

3. Select Patch priority L1 with high priority and L2 with low priority.

4. Patch Priority can be Decided Using following formula:

$$\begin{cases} \|L_1\| = \left\lceil \frac{T_{pw}-2}{2} \right\rceil \times \left\lceil \frac{T_{ph}-2}{2} \right\rceil \\ \|L_2\| = \left\lceil \frac{T_{pw}-2}{2} \right\rceil \times \left\lceil \frac{T_{ph}-2}{2} \right\rceil \end{cases}$$

Typical image steganography process reduces the image quality as if the size of secret message is large enough .So in the previous 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.

6.EXPECTED RESULT

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.

7.CONCLUSION

With the proposed system we 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.

Acknowledgment

I express true sense of gratitude towards my project guide Prof. Deepak S.U., of computer department for his in valuable co-operation and guidance that he gave me throughout my research, for inspiring me and providing me all the lab facilities, which made this research work very convenient and easy. I would also like to express my appreciation and thanks to our HOD Prof. R.H.Kulkarni and Director Dr. D.M.Yadav and all my friends who knowingly or unknowingly have assisted me throughout my hard 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 image—A 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 Comput. 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.