Secure Transmission of Audio Video and Image Using Reversible Texture Synthesis Method

Asmita Kamble[1], Payal More[2], Rishabh Patil[3], Rohit Dhengle[4], Hrutuja Vakil[5]

[1]*Professor, Dept. of Computer Engineering, Sinhgad Institute of Technology and Science, Maharashtra, India*
[2,3,4,5]*Student, Dept. of Computer Engineering, Sinhgad Institute of Technology and Science, Maharashtra, India*

---***---

Abstract - *Today's demand of internet in applications in large amount requires data to be transmitted in a secure manner. In communication system transmission of data is not secure because interception & improper manipulation done by the eavesdropper. We can Write hidden messages in such a way that no one, except the sender and receiver can suspect the existing of the message form of security and the solution for this problem is Reversible Texture Synthesis. In this paper we propose a new approach for steganography using reversible texture synthesis.*

In this texture synthesis technique we re-form a smaller texture image which analysize a new texture image which has a similar figuration and size. We knit the texture synthesis process into steganography to hide secret messages.To protest using an available cover image to hide messages, our algorithm helps hiding the source texture image and secret messages is embeded using this process of texture synthesis. This helps us to extract secret messages and source texture from a stego synthetic .

Reversible texture synthesis uses the concept of steganography using reversible texture synthesis. The data which is secret is hidden at sender side into the texture image, we generate patches from source texture and index table and composite image is being generated, message is embedded and data which is corrected can be recovered from the cover image with no change at receiver end. Mostly all the part of system will include synthesis of texture, embedding of message and recovering source texture ,extraction of message and authentication of message. The system is to be developed which will be easily embed into the different application where security is main concern.

Key Words:**-Reversible Texture, Secret Data, embedding, De-embedd, Pixel, Patch.**

1. INTRODUCTION

In this paper, we are proposing a concept for steganography using reversible texture synthesis. A texture synthesis process re-sampling a small texture image in order to synthesize a new texture image which looks similar . We form the texture synthesis process into steganography which hide secret messages and source texture. In contrast to using an existing cover image to hide messages, our algorithm hides the source texture image and embeds secret messages through the process of texture synthesis. This process allows us to extract the secret messages and the source texture from a stego texture. According to our knowledge, steganography taking advantage of the reversibility has been presented within the literature of texture synthesis.

Information security is the process of avoiding information from unauthorized permission. It is a general term that can be used regardless of the form the data may take information security threats that occur in many different ways. Most of the common threats today are software attacks, denial of service attack,theft of intellectual property, identity theft, theft of equipment , and information extortion. Most people have faced software attacks in many cases. Viruses, worms, phishing attacks, and Trojan horses are a few common examples of software attacks that causes harm to our system. The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability that is all security levels.

To conceal data security, there are few methods introduced earlier, the list of methods are LSB Coding, Phase Shifting, Parity Coding and Spread Spectrum. We proposed this method to gain more security that is reversible texture. Reversible Texture Synthesis is an approach for data security. It uses the patch based algorithm which represents an image block of source texture where user specifies its size. A texture synthesis process re-samples a smaller texture file, which synthesizes a new texture file which looks similar and on randomly based. The texture synthesis process is formed into steganography to hide secret messages. In case of using an existing cover image to hide messages, this algorithm hides the source texture file and embeds secret messages using the process of texture synthesis. This allows extracting the secret key messages and original texture from a stego synthetic texture. The approach have some advantages. First, the scheme giving the embedding capacity that is proportional to the size of the stego texture image. Secondly, the reversible capability inherited from this scheme provides functionality, which allows recovering the source texture.

Reversible texture synthesis is practice of concealing an Audio, image or video within another audio, image, or video. The reversible texture synthesis application includes not only acknowledged or displayed communication between two parties whose existence is unknown to possible attacker and whose success depends on detecting the existence of this communication. Many of the image, Audio, Video pixel and patch algorithms which adopt an existing image as secrete medium. The embedding of secret messages into the cover image which lead to image distortion in the stego image.

In case of using an existing cover image to hide messages, the algorithm hides the source texture image and embeds secret messages using the process of texture synthesis. This allows extracting the secret messages and source texture from a stego synthetic texture.

The sender can securely send message to destination. This can be achieved by embedding a audio file to the message. So the third party does not know about the secret message. They think that a audio and video file is sending and they don't know about this secret sending of the message. In this a sender can encrypt a file by entering a key. The same key must be entered same key must entered at the time of decryption process. This process can be done by entering the key that previously entered during the Encryption process. If the entered key is wrong the message the we will not get correct message.

2.. RELATED WORK

In this paper[1],To hide messages using an existing cover image audio and video to conceals the source texture and secret messages are embeded through this process of texture synthesis using our algorithm .This gives us access to extract secret messages and the source texture from a stego synthetic texture.

In paper[2] , It is a safe mechanism of data transmission to tackle the security problem of information which is transmitted in Internet. We propose a new technique on matrix scrambling which is based on random function, shifting and reversing techniques of circular queue.

In paper[3] , data transmission in public communication system is not secure because of interception and improper manipulation by eavesdropper. So the attractive solution for this problem is Steganography, which is the art and science of writing hidden messages in such a way that no one, apart from the sender and intend recipient, suspects the existence of the message, a form of security through obscurity.
This paper [4], focuses on the data security approach when communicated by hiding it inside the multimedia files. It provides the security to data before transmitting over internet.

3. EXISTING SYSTEM ARCHITECTURE

This texture synthesis mechanism performs a huge role in a graphics and visioning video texture this mechanism takes the video stream as an input and produces the output video stream by texture synthesis only on the particular temporal domain. Two types of algorithm used one is pixel based algorithm another one is patch based algorithm.in pixel based algorithm most similar pixel is produced as an output and rest of the pixels are retrieved by data detection mechanism. In patch bade algorithm first choose the source texture and then choose the candidate texture .after choosing the candidate texture identify the boundary gap between source texture and candidate texture by using dynamic programming. In this stenography technique the size of the stego image is compared with original file. the image after embedding the secret message is called "stego image". From this stego image the source texture had been retrieved.

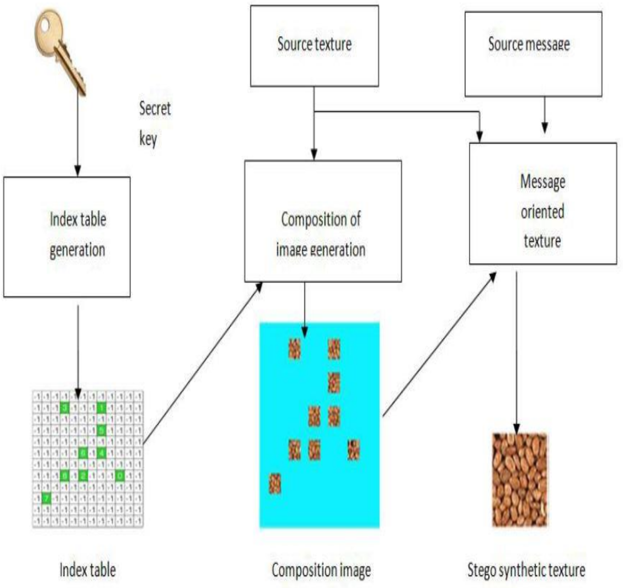


Fig.1 Existing System Mechanism

4. ALGORITHMIC DETAILS

1. Black module replacement:-

The codeword$C_{priv}$is inserted in standard QR code by replacing the black modules with textured patterns $P_1, . . . , P_q$respecting the codewordC_{priv}, starting from the bottom-right corner. Then, in the case of private message sharing scenario, the textured patterns are placed in the position tags with respect to the chosen permutation σ,. In the case of authentication scenario, the standard position tags keep unchanged black modules,

2. Patch Extraction:-

We can denote SP as the collection of all source patches and SPn=||SP|| as the number of elements in the set SP. We can employ the indexing for each source patch spi, i.e., SP= {spi| i = 0 to ||SP||-1}. Given a source texture with the size of

$Sw \times Sh$, we can derive the number of source patches SPnusing

If a kernel block has the size of $Kw \times Kh$. we assume the size of the source texture is a factor of the size of the kernel block to ease the complexity.

$$SP_n= (Sw/Kw)*(Sh/Kh)$$

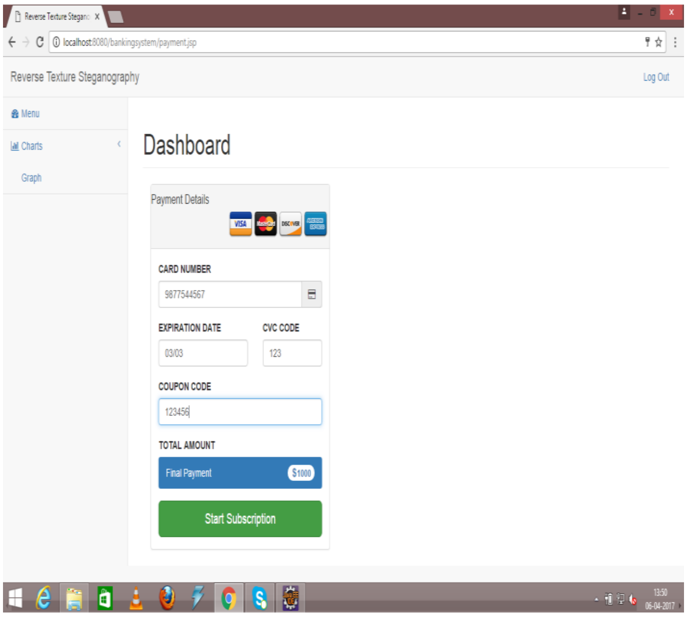
Our steganographic texture synthesis algorithm needs to generate candidate patches when synthesizing synthetic texture. The concept of a candidate patch is trivial: we employ a window $Pw \times Ph$and then travel the source texture ($Sw \times Sh$) by shifting a pixel each time following the scan line order. Let $CP=\{cpi|i=0,1, \ldots, CPn-1\}$ represent the set of the candidate patches where $CPn=||CP||$ denotes the number of elements in CP. We can derive CPn using (2).

$$CPn= ||CP||=(S_w-P_w+1)*(S_h-P_h+1)$$

When generating a candidate patch, we need to ensure that each candidate patch is unique; otherwise, we may extract an incorrect secret message. In our implementation, we employ a flag mechanism. We first check whether the original source texture has any duplicate candidate patches. For a duplicate candidate patch, we set the flag on for the first one. For the rest of the duplicate candidate patches we set the flag off to ensure the uniqueness of the candidate patch in the candidate list.

3.RESULT

Images


localhost:8080/bankingsystem/payment.jsp

Reverse Texture Steganography

Dashboard

Payment Details

CARD NUMBER: 9877544567

EXPIRATION DATE: 03/03

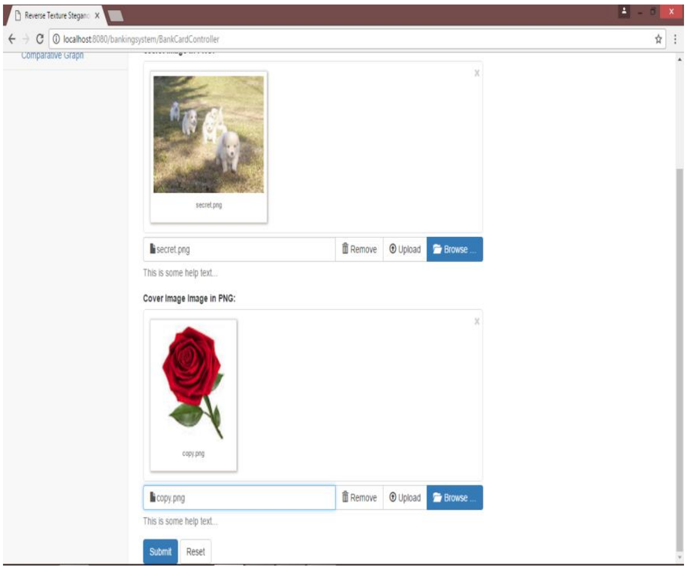
CVC CODE: 123

COUPON CODE: 123456

TOTAL AMOUNT

Final Payment $1000

As we have taken examples of online card system. Next step after the login is to go for payment details. Before starting subscription, fill card number, expiration date, cvc code, coupon code. Start subscription.


localhost:8080/bankingsystem/BankCardController

secret.png

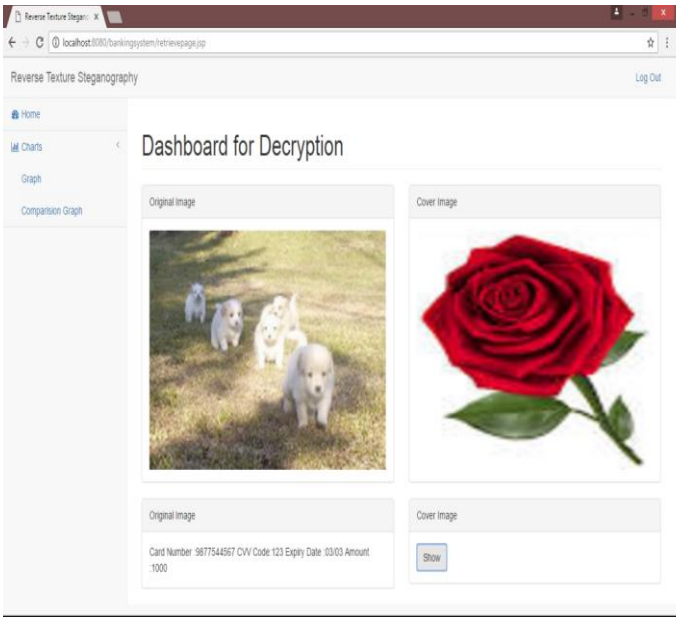
This is some help text...

Cover Image Image in PNG:

copy.png

This is some help text...

Upload one cover image and one original image. We can take any image as an cover and original image. For that we are providing browse option. We take RGB value of cover image as zero. We cannot see clear cover image. That's the motive of hidding our cover image. After selecting this two image, click on submit button.


localhost:8080/bankingsystem/retrievepage.jsp

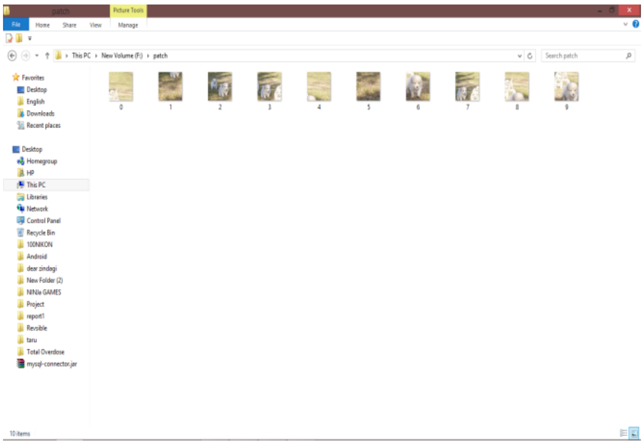
Reverse Texture Steganography

Dashboard for Decryption

Original Image

Card Number :9877544567 CVV Code:123 Expiry Date :03/03 Amount :1000

We can see decrypted payment details that we have given at the time of uploading two images. It means our data get decrypted.



We can see patches of our original images. Patches of cover image gets hide to increase security. If both the patches of original image as well as cover image get matched then only our data will decrypt.

4. CONCLUSIONS

This paper we design a reversible texture synthesis for image stegonography. Given an original source texture, can produce a large stego synthetic texture concealing secret messages. To the best of our knowledge, we are the first that can exquisitely weave the steganography into a conventional patch-based texture synthesis.Our method is good approch and provides reversibility so that we can retrieve the original source texture ,we can make possible a second round of texture synthesis if required. With the two techniques we have introduced, 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 RS steganalysis attack. We believe our proposed scheme offers substantial benefits and provides an opportunity to extend steganographic applications. One possible future study is to expand our scheme to support other kinds of texture synthesis approaches to improve the image quality of the synthetic textures. We can also study other steganography approaches and combine them to increase the embedding capacities.

REFERENCES

[1] Kuo-Chen Wu and Chung-Ming Wang, Member, IEEE, ”Steagnography Using Reversible Texture Synthesis”, year 2015.

[2] M.Kiran Kumar, S.Mukthyar Azam, ”Efficient Digital Encryption Algorithm Based on Matrix Scrambling Technique”, October 2010

[3] Jayram, Rangantha, Anupama, “Information Hiding Using Audio Stegnography- A Survey”, August 2011.

[4] Vipula Madhurkar Wajgade, Dr Suresh Kumar,”Enhancing Data Security Using Video Stegnography”,April 2013.

[5] 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.

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

[7] N. Provos and P. Honeyman, “Hide and seek: an introduction to steganography,” IEEE, vol. 1, no. 3, pp. 32-44, 2003.

[8] R. J. Anderson, and M. G. Kuhn, “Information hiding-a survey,” Proceedings of the IEEE, vol. 87, no. 7, pp. 1062-1078, 1999.

[9] Y.-M. Cheng and C.-M. Wang, “A high-capacity steganographic approach for 3D polygonal meshes,” The Visual Computer, vol. 22, no. 9, pp. 845-855, 2006.

[10] 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,” vol. 7, no. 5, pp. 1448-1458, 2012.