International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 13
September 2016

Efficient and Secure Online Transaction Using Steganography

***P.HARINI** ****B.SARITHA**

*M.TECH student ,Dept of CSE, VAAGDEVI ENGINEERING COLLEGE

**Assistant Professor, Dept of CSE , VAAGDEVI ENGINEERING COLLEGE

ABSTRACT:

The online transactions can be made secured by using stegnography. 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. In general, the host medium used in stegnography includes meaningful digital media such as digital image, text, audio, video, 3D model. A large number of image stegnographic algorithms have been investigated with the increasing popularity and use of digital images. We weave the texture synthesis process into Steganography to conceal secret messages. In contrast to using an existing cover image to hide messages, our algorithm conceals the source texture image and embeds secret messages through the process of texture synthesis. This allows us to extract secret messages and the source texture from a stegno synthetic texture. Embedding capacity that is proportional to the size of the stegno texture image, a steganalytic algorithm is not likely to defeat our steganographic approach and the reversible capability inherited and provides functionality which allows recovery of the source texture. verified that it can provide various numbers, produce a visually plausible texture images, and recover the sourcetexture.

INTRODUCTION

In the last decade many advances have been made in the area of digital media, and much concern has arisen regarding steganography for digital media. Stegnography a singular method of information hiding techniques. It embeds messages into a host medium in order to conceal secret messages so as not to arouse suspicion by an eavesdropper 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. In general, the host medium

used in steganography includes meaningful digital media such as digital image, text, audio, video, 3D model etc. A large number of image steganographic algorithms have been investigated with the increasing popularity and use of digital images.

Most image steganographic algorithms adopt an existing image as a cover medium. The expense of embedding secret messages into this cover image is the image distortion encountered in the stego image. This leads to two drawbacks. First, since the size of the cover image is fixed, the more secret messages which are embedded allow for more image distortion. Consequently, a compromise must be reached between the embedding capacity and the image quality which results in the limited capacity provided in any specific cover image. Recall that image steganalysis is an approach used to detect secret messages hidden in the stego image. A stego image contains some distortion, and regardless of how minute it is, this will interfere with the natural features of the cover image. This leads to the second drawback because it is still possible that an image steganalytic algorithm can defeat the image steganography and thus reveal that a hidden message is being conveyed in a stego image.

In this paper, we propose a novel approach for steganography using reversible texture synthesis. A texture synthesis process re-samples a small texture image drawn by an artist or captured in a photograph in order to synthesize a new texture image with a similar local appearance and arbitrary size. We weave the texture synthesis process into steganography concealing secret messages as well as the source texture. In particular, in contrast to using an existing cover image to hide messages, our algorithm conceals the source texture image and embeds secret messages through the process of texture synthesis. This allows us to extract the secret messages and the source texture from a stegno synthetic texture. To the best of our knowledge, steganography taking advantage of the reversibility has ever been presented within the literature of texture synthesis.

Our approach offers three advantages. First, since the texture synthesis can synthesize an arbitrary size of texture images, the embedding capacity which our scheme offers is proportional to the size of the stegno texture image. Secondly, a steganalytic algorithm is not likely to defeat this steganographic approach since the stegno texture image is composed of a source texture rather than by modifying the existing image contents. Third, the

reversible capability inherited from our scheme provides 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. Experimental results have verified that our proposed algorithm can provide various numbers of embedding capacities, produce visually plausible texture images, and recover the source texture. Theoretical analysis indicates that there is an insignificant probability of breaking down our steganographic approach, and the scheme can resist an RS stegna analysis attack.

EXISTING SYSTEM

In contrast to using an existing cover image to hide messages, our algorithm conceals the source texture image and embeds secret messages through the process of texture synthesis.

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

Most image steganographic algorithms adopt an existing image as a cover medium. The expense of embedding secret messages into this cover image is the image distortion encountered in the stego image.No significant visual difference exists between the two stego synthetic textures and the pure synthetic texture.

PROPOSED SYSTEM:

Experimental results have verified that our proposed algorithm can provide various numbers of embedding capacities, produce a visually plausible texture images, and recover the source texture.
proposed an image reversible data hiding algorithm which can recover the cover image without any distortion from the stego image after the hidden data have been extracted.

We illustrate our proposed method in this section. First, we will define some basic terminology to be used in our algorithm. The basic unit used for our steganographic texture synthesis is referred to as a "patch."The three fundamental differences between our proposed message-oriented texture synthesis and the conventional patch-based texture synthesis are described in Table I. The first difference is the shape of the overlapped area.proposed scheme

offers substantial benefits and provides an opportunity to extend steganographic applications.

ADVANTAGES:

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

Conclsion: we can weave the steganography into a conventional patch-based texture synthesis. Our method provides reversibility to retrieve the original source texture from the stegno synthetic textures, making possible a second round of texture synthesis if needed. With the two techniques we have introduced, our algorithm can produce visually plausible stegno synthetic textures even if the secret messages consisting of bit "0" or "1" have an un even 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.

References:

1. S. Kamara, and K. Lauter, "Cryptographic cloud storage,"
2. S. Grzonkowski, and P. M. Corcoran, "Sharing cloud services: user authentication for social enhancement of home networking,"
3. P.A. Cabarcos, F.A. Mendoza, R.S. Guerrero, A.M. Lopez, and D. Diaz-Sanchez, "SuSSo: seamless and ubiquitous single sign-on for cloud service continuity across devices,"
4. D. Diaz-Sanchez, F. Almenarez, A. Marin, D. Proserpio, and P.A. Cabarcos, "Media cloud: an open cloud computing middleware for content management,"
5. J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy keyword search over encrypted data in cloud computing," encrypted cloud data,"
6. C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure ranked keyword search over
7. N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving

multi-keyword ranked search over encrypted cloud data,"

8. Q. Chai, and G. Gong, "Verifiable symmetric searchable encryption for semi-honest-but-curious cloud servers,"

Web Sites Referred:

www.cloudxl.com

www.cloud-computing.com

www.talkincloud.com

www.cloudcomputing.sys-con.com

www.virtualizationreview.com/Home.aspx

www.thecloudtutorial.com

AUTHOR 1:-

* P.HARINI completed her B tech in RAMAPPA ENGINEERING COLLEGE in 2013 and completed M-Tech in VAAGDEVI ENGINEERING COLLGE

AUTHOR 2:-

**B.SARITHA is working as Assistant Professor in Dept of CSE ,VAAGDEVI ENGINEERING COLLGE