International Journal of Current Research and Modern Education (IJCRME)
ISSN (Online): 2455 – 5428 & Impact Factor: 3.165
Special Issue, NCFTCCPS - 2016

STEGANOGRAPHY USING REVERSIBLE TEXTURE SYNTHESIS

B. Abinaya*, R. Bhuvaneshwari*, S. Roja* & C. Muthukumaran**
* UG Scholar, Arasu Engineering College, Kumbakonam, Tamilnadu
** Assistant Professor, Department of Computer Science & Engineering, Arasu Engineering College, Kumbakonam, Tamilnadu

Abstract:

In areas where steganography and strong encryption are being outlawed. Steganography is the concept of hiding of a data or image within another image so that hidden information is invisible. The key concept behind steganography is that message to be transmitted is not detectable to casual eye, but hackers are tracked. The past method can deploying the phishing attack by the adversary. The proposed of system using steganography using reversible texture. Using weave the texture synthesis process into steganography to conceal secret messages.A texture synthesis process re-samples a smaller texture image which synthesizes a new texture image with a similar local appearance and arbitrary size.Reversible texture based technique, to protect the information against eaves droppers. The Steganography is an art or practice of concealing a file, message, image, or video within another file, message, image, or video. So using this technique, personal information is hide with in image and preventing misuse of their information.

Index Terms: Steganography, Data Embedding, Reversible & Texture Synthesis

Introduction:

Steganography 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 hidden message is being conveyed in a stegoimage.In this paper, we propose steganography and strong encryption are being outlawed. Steganography is the concept of hiding of a data or image within another image so that hidden information is invisible. The key concept behind steganography is that message to be transmitted is not detectable to casual eye, but hackers are tracked. The past method can deploy the phishing attack by the adversary. The proposed of system using steganography using reversible texture. Using weave the texture synthesis process into steganography to

conceal secret messages. A texture synthesis process re-samples a smaller texture image which synthesizes a new texture image with a similar local appearance and arbitrary size. Reversible texture based technique, to protect the information against eaves droppers. The Steganography is an art or practice of concealing a file, message, image, or video within another file, message, image, or video. So using this technique, personal information is hiding with in image and preventing misuse of their information. The remainder of this paper is organized as follows: in Section II, we review the texture synthesis techniques. In Section III, we detail our algorithm including embedding and extracting procedures. We describe experimental results and theoretical analysis in Section IV, followed by our conclusions and future work presented in the final section.

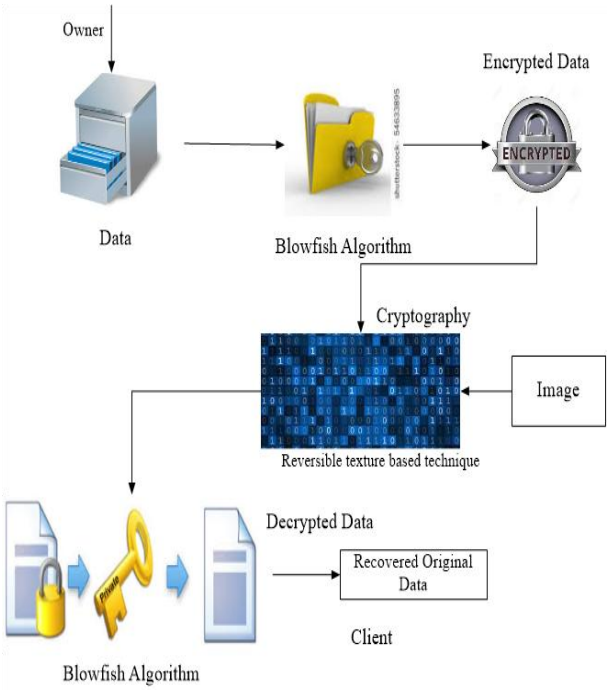
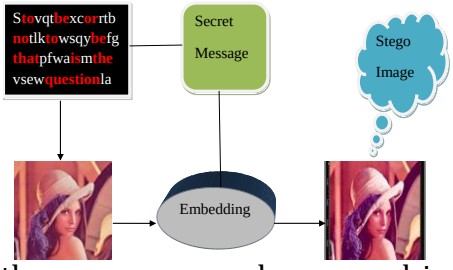


Figure 1: Architecture diagram for Steganography

Related Work:

Texture synthesis has received a lot of attention recently in computer vision and computer graphics [8]. The most recent work has focused on texture synthesis by example, in which a source texture image is re-sampled using either pixel-based or patch-based algorithms to produce a new synthesized texture image with similar local appearance and arbitrary size. Pixel-based algorithms [9], [10], [11] generate the .pixel in a sample texture as the output pixel. Since each output pixel is determined by the already synthesized pixels, any wrongly synthesized pixels during the process influence the rest of the result causing propagation of errors. However, since patches are pasted with a small overlapped region during the synthetic process, one needs to make an effort to ensure that the patches agree with their neighbors. 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. Histogram shifting is a preferred technique among existing approaches of reversible image data hiding because it can control the modification to pixels, thus limiting the embedding distortion, and it only requires a small size location map, thereby reducing the overhead encountered. To the best of our knowledge, we were unable to disclose any literature that related patch-based texture synthesis with steganography. In this paper, we present our work which

takes advantage of the patch-based methods to embed a secret message during the synthesizing procedure. This allows the source texture to be recovered in a message extracting procedure, providing the functionality of reversibility. We detail our method in the next section.



System Modules:

1. Encryption
2. Embedding Process
3. Reversible Techniques
4. Decryption

Encryption:

In this module it allows user to enter the user name and password in order to restrict the user to access the system. Then it validates the entered user name and password, if it is correct it will allow the user to access the application. Authentication process is always occurred prior to mobility management process included location registrations and service delivery. Ensures network resources are accessed by authorized clients and prevents resources from any illegal client or damage.

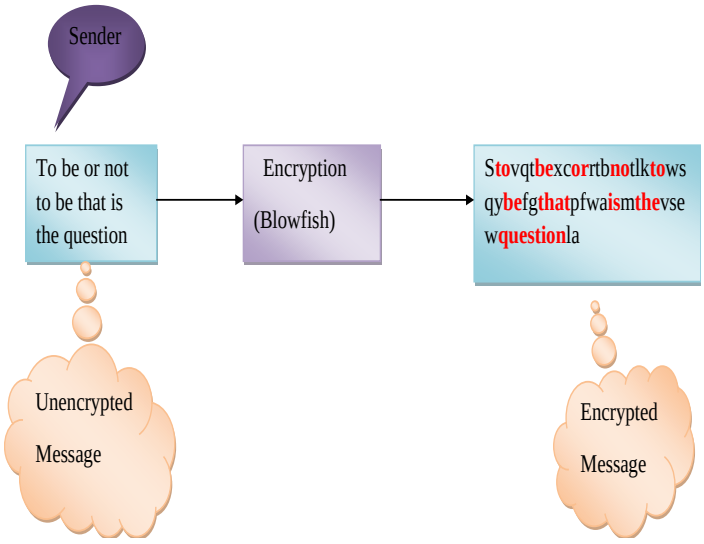


Figure 2: Encryption Process

Embedding Process:

In this module it allows to pick the image from the gallery and then to enter the password key for encryption after that has to enter the message. The keyless algorithm is a symmetric key block cipher that can be effectively used for encryption and safeguarding of data. Keyless Algorithm is a Feistel Network, iterating a simple encryption function 3 times. The block size is 64 bits, and the key can be any length up to 448 bits. Although there is a complex initialization phase required before any encryption can take place, the actual encryption of data is very efficient for secure data encryptions. It is suitable for applications where the key does not change often, like a communications link or an automatic file encryption.

Reversible Techniques:

Cryptography is that branch of science which is concerned with the mathematical techniques for keeping message secure and free from attacks. Cryptography is the art of achieving security by encoding the data into unreadable form. Data that can be read and understood without any difficulty is called plain text or clear text. The method of encoding Plain text in such a way as to hide its content is called

encryption. Technique is used to shuffling room in image pixels process before encryption. The data are hidden in the every Shuffling pixels of the image.

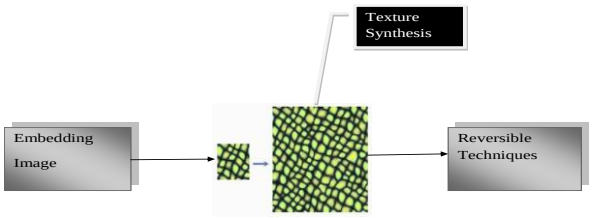


Figure 3: Reversible Techniques Process

Decryption:

In this module it allows to pick the encrypted image received from the owner Side Encrypting Data and then to enter the password key to decrypt. If the image and the key are correct then the corresponding message will be displayed. To decrypt any file one has to know exactly what is the key matrix and to find the random matrix theoretically one has to decrypt the cryptography image data. The keyless method can be applied for data encryption and decryption in any type of application for sending confidential data

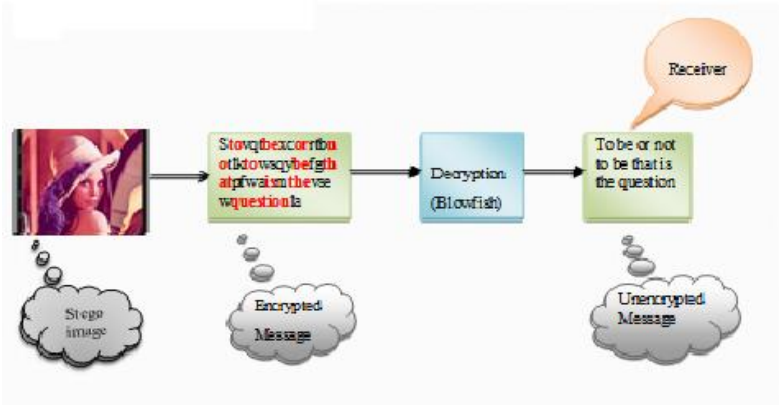


Figure 4: Decryption Process

Conclusion:

This paper proposes a reversible steganographic algorithm using texture synthesis. Given an original source texture, our scheme 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 novel and provides reversibility to retrieve the original source texture from the stego 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 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.

References:

1. 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.
2. I.-C. Dragoi and D. Coltuc, “Local-prediction-based difference expansion reversible watermarking,” IEEE Trans. Image Process., vol. 23, no. 4, pp.1779-1790, 2014.

3. J. Fridrich, M. Goljan, and R. Du, "Detecting LSB steganography in color,and gray-scale images," MultiMedia, IEEE, vol. 8, no. 4, pp. 22-28, 2001.
4. 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, 2013.
5. H. Otori and S. Kuriyama, "Texture synthesis for mobile data communications," IEEE Comput. Graph. Appl., vol. 29, no. 6, pp. 74-81, 2009.
6. 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.