Volume 6, Issue 2, February 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

An Approach to Hide Message Using Steganography

Sneha Deokate, Purnima Selokar
Computer Science and Engineering, RTMNU, Nagpur,
Maharashtra, India

Abstract— Steganography is a technique of hiding important data behind any image. Such steganography is needed in day today life where important data is to be sent through a defined network. There are possibilities that the data may be attacked by the attackers or unwanted user and may use it illegally. Hence an approach to hide data using reversible texture synthesis is being used in steganography. Stego-synthetic texture can be decoded to get the original data using reverse texture synthesis. Patch based algorithm is being used to hide important data behind an image.

Keywords— Steganography, Stego-synthetic, Patch based algorithm, reversible texture synthesis,unwanted users.

I. INTRODUCTION

Texture synthesis process consists of re-sampling a small texture image captured in a photograph in order to synthesize a new texture image with a similar local appearance and arbitrary size. Such texture synthesis process is implemented in steganography in order to conceal the secret messages as well as the source texture. Steganography using reversibility has been used within the literature of texture synthesis. The advantages of using steganography in reversible texture synthesis are that the embedding capacity to hide message has been increased considerably. Also the level of security to hide message increases as stego synthetic texture is used and by using reversible method helps to recover the source texture. Since the decoded source texture is exactly the same as the original source texture that was sent and hence it can be used to check the authenticity of the message.

II. PROPOSED METHOD

Steganography is implemented in watermarking for hiding secret message. In watermarking the secret message to be hidden is covered into a cover image in such a way that the people cannot identify the existence of the hidden data in the resulting stego-image . Hiding data behind texture images with the hidden data being easily and faultlessly recoverable from images captured from print media reversibly is implemented in watermarking.The characteristic of the art image creation process can be used effectively to carry out the data embedding work. Information hiding also called as aesthetic data includes combining art image creation with the data to kept hidden from attackers. The main criteria for designing data hiding techniques are embedding capacity that will not lead to distortion of stego image and how the original image gets recovered from stego image.

Generally, secret message that is to be kept hidden is embedded during the image creation process by shifting the colors of the pixels using Cubism-like image with the image regions for the minimum amounts of addition or deletion and keeping the average colors of the regions unchanged. As a result the color differences in the resulting image are difficult to be found by a hacker .

A. Patch Based Algorithm

Earlier the secret messages to be used were encoded into colored dotted patterns and then they were embedded behind an image that was a blank image. To implement this pixel-based algorithm was used with the help of pixel-based texture synthesis method, that works with the existence of dotted patterns. However, using pixel based algorithm had a small error rate of the message extraction. Hence patch based algorithm has been applied to remove this disadvantage.

For image hiding in steganography texture synthesis “patch based algorithm” is being used instead of pixel based algorithm. A patch denotes an image size of a source texture where its size can be specified by the user. It can be represented by its width (*Pw*) and height (*Ph*). It basically consist of two parts i.e central part and an outer part where the central part also known as the kernel region with size of *Kw*×*Kh*, and the part surrounding the central region is referred to as the boundary region with the depth (*Pd*). Kernel block consist of source texture with the size of *Sw*×*Sh*.Here the source texture can be further divided into different number of non-overlapped kernel blocks,each having size of *Kw*×*Kh*, where*KB* represent the collection of all kernel blocks thus generated, and ||*KB*|| denotes the number of elements in the given set. Indexing is implemented for each source patch *kbi*, i.e., *KB*={*kbi*| *i* =0 to ||*KB*||-1}. Here IndexTableGenerationProcess is used in which an index table maintains the record of location of all the source patch. This leads toeasily recognize the synthetic texture and hence retrieve the source texturecompletely and easily. This is one of the major advantage of using indexing in our algorithm.

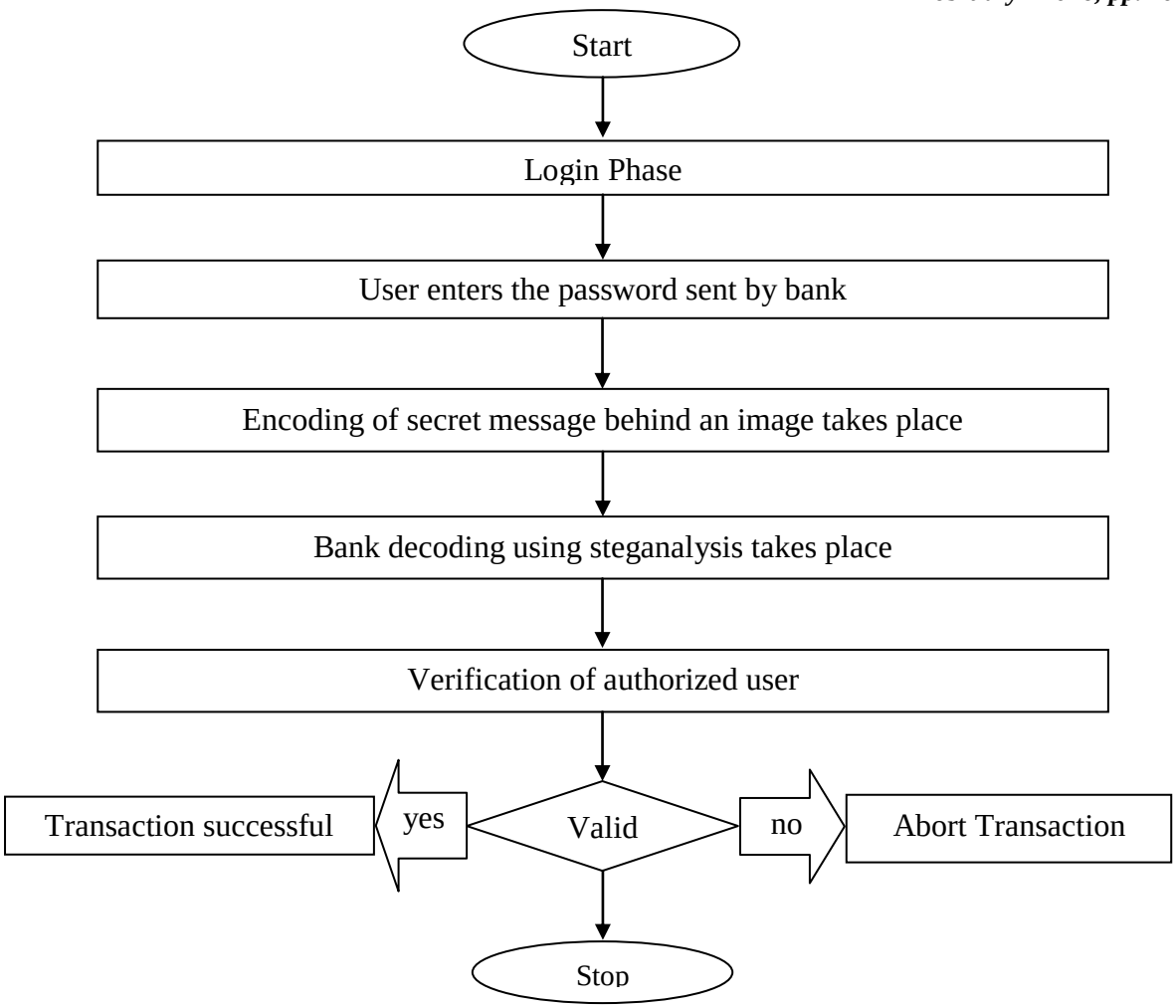

Fig. 1 Flowcart of proposed system

B. Message Encoding Steps

When any kernel block is located around the boundary of a source texture, then it can be implemented using the boundary mirroring through the kernel block's symmetric contents to produce the outer region.

1. Filling necessary data required to be transferred through a given network.
2. Using secret message as a password used for authenticity and confidentiality.
3. Converting this secret message into encoded bit pattern.
4. Using patch based algorithm and steganography to hide message behind an image.
   Finally encrypted message is then sent through a network to the required user.

C. Message Decoding Steps

1. The message which is in binary format is decoded using steganalysis method.
2. Using reverse steganography the message to be hidden is separated from the image that is used for hiding the secret message.
3. The secret message received is verified for authentication and confidentiality.

By applying reversibility to the encoded message guarantees that to extract the secret message which is embedded in the stego-image helps to get back the original contents of the cover image which is used for hiding losslessly.

III. APPLICATIONS

3.1 Steganography includes hidding messages behind an image.The message to be hidden may be in the form of text message,video message,audio message or text message.Online banking transactions may use steganography where users personal details are to be hidden for securely transfer of message.The message submitted by the customer and applying steganography is in encoded format.This encoded message is then decoded for authorisation using steganalysis algorithm.After sucessfull authorisation further transaction takes place.Modification in a stego image takes place using patch based algorithm.

3.2 Steganography can also be used in E-commerce where users have to protect their username and password for securely transaction over a network.

3.3 It can also be applied to Biometric finger printing, which uses unique session key embedded into the fingerprint images that will allow for a very secure option to network transaction verification .

3.4 Data transportation method from E-Mail to
images on Internet websites can also use steganography for securely transmission of message.

IV. COMPARISON WITH PREVIOUS METHODS

Earlier steganography was implemented to hide secret data but the capacity of message size to be hidden is short. By using two component least based method the size of message to be hidden increases considerably.Also the distortion rate of an image which is used as a cover hasbeen reduced with the help of Pseudo Random number generators.The secret message to be hidden was only text message in earlier time.Now we can hide text message along with audio message behind an image.

V. CONCLUSIONS

Steganography is implemented for securely hiding mulimedia message.This method implemented with reversibility to get the original source texture from the decoded stego synthetic texture increases the confidentiality and integrity of the message. The algorithm will work correctly even if the secret message consisting of bit pattern that includes an uneven appearance of probabilities or not. As a result more security and robustness is achieved against an RS steganalysis attack. Such steganographic applications can also be implemented in other uses that requires high security.

ACKNOWLEDGMENT

Sneha Deokate and others wants to thank IEEE Explore.ORG for helping to access database for references.

REFERENCES

[1] Kuo-Chen Wu and Chung-Ming Wang, *Member, IEEE* ,"Steganography Using Reversible Texture Synthesis" *IEEE Trans. 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] C. Dragoi and D. Coltuc, "Local-prediction-based difference expansion reversible watermarking," *IEEE Trans. Image Process.*, vol. *23*, no. 4, pp.1779-1790, 2014.

[4] 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.

[5] *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.*

