Image Steganography for locked communication scheme

Anvesh. K[#1], P. Madhuri[#2], T. Navyasri[#3]
*1. Assistant Professor (Guide), Department of Information Technology & JNTU Hyderabad
*2. Student, Department of Information Technology
*3. Student, Department of Information Technology

Abstract*—We propose a novel approach for steganography using a reversible texture synthesis. A texture synthesis process resamples a smaller texture image, which synthesizes a new texture image file, a new audio file, a new video file and a new text file with a similar local appearance and an size is directly proportional to the secret file which embedding by a texture image. We weave the texture synthesis process into steganography to conceal secret file. In contrast to using an existing cover image to hide secret file, our algorithm conceals the source texture image and embeds secret file through the process of texture synthesis. This allows us to extract the secret file and source texture from a stego synthetic texture. Our approach offers three distinct advantages. First, our scheme offers the compression capacity that is up to the size of the stego texture image. Second, our steganographic approach very different from existing approaches on steganography. Third, the quality output is one, which meets the requirements of the end user and presents the information clearly. 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 secret file.*

Keywords*: - Texture Synthesis, Plausible Texture Steganography.*

I. INTRODUCTION

Steganography is the art and science writing such that the presence of the message is only know to sender and receiver.Steganography word is derived from greek words stego means “covered or protected” graphia means “writing”.First appears in the literature in steganography by Johannes Trithemius published in 1606,it is the technique of embedding information into something else for the solepurpose of hiding that information from the casual observer.

The advantage of steganography, over cryptography alone, is that messages do not attract attention to themselves.

Some steganography techniques:

- Physical steganography.
- Digital steganography.
- Network steganography.
- Printed steganography.

Physical steganography:

Is the art of concealing a message, image, or file within another message, image, or file. The "physical" part comes in when said secret message is not so much coded into an image as it is literally stuffed inside.

Digital steganography:

Digital steganography makes use of the fact that in a number of file formats, data is reduplicated or some data is of little importance, and the hidden message does not cause noticeable changes to the file.

Network steganography:

Uses modification of a single network protocol. The protocol modification may be applied to the PDU (Protocol Data Unit), time relations between exchanged PDUs, or both (hybrid methods).

Printed steganography:

Is type of steganographyhiding data within data “\where tiny yellow dots are added to each page. The dots are barely visible and contain encoded printer serial numbers and timestamps.

Different Kinds of Steganography

In our proposal system we are working the different kinds of steganography techniques. The first technique we are hiding image inside of a stego image, second technique is hiding a message inside a stego image and third technique we are hiding audio, video and text file inside a stego image.

We weave the texture combining process into steganography to conceal secret file

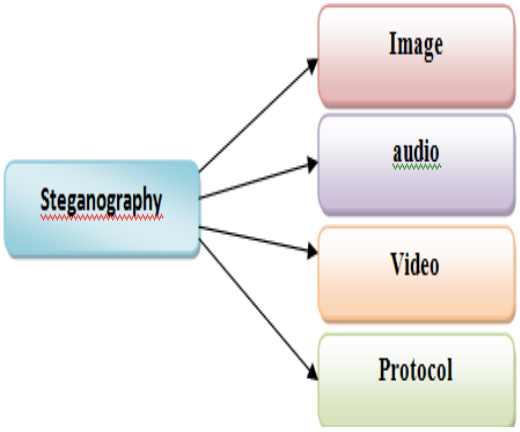

Fig 1.different kinds of steganograpy

Text Steganography:

Text steganography is a sub part of steganography that hides the message behind other cover text file. Moreover, hiding the text behind HTML coding of web pages makes detection of steganography impractical as web pages are a fundamental building blocks of the internet.

Video Steganography:

Video Stenography is a sub part of steganography that hides the video file behind other cover text file or behind the image file.

Audio Steganography:

Audio steganography is sub part of the steganography. In the audio steganography we can hide a secret voice file behind the other cover file or behind the image file.

ANALYSIS

Most image steganographic algorithms adopt an existing image as a cover medium. Otori and Kuriyama pioneered the work of combining data coding with pixel-based texture synthesis.

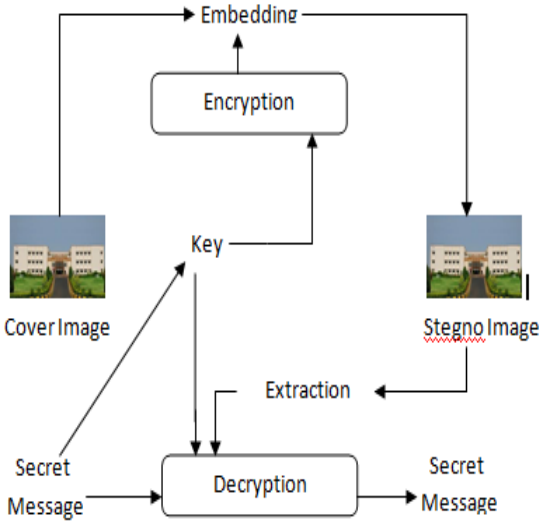

Fig 2.Existing system

In the existing steganography technique first we selecting a secret message and we giving a secret key to the secret message for encryption. After encryption we are selecting a cover image, we are embedding encrypted message with selected cover image. After embedding a encrypted message inside a cover image that image we are calling as stego image.Sender send the stego image to receiver, receiver extract the secret message by using decryption process.

In the existing system we have lot of disadvantages the first disadvantage is the size of the cover image is fixed,sender can able to send only fixed size of data to the receiver if size of secret file is more then the cover image then a attacker easily identify something data is hidden inside the image this is the second disadvantage in the existing system.

II. CONTRIBUTION &INVITED WORK

In proposal system we are proposing a experimental approach for steganography for locked communication scheme . A texture synthesis process resamples a smaller texture image, which combines a new texture image file, a new audio file, a new video file and a new text file with a similar local appearance and an size is directly proportional to the secret file which embedding by a texture image. We weave the texture combining process into steganography to conceal secret file. In contrast to using an existing cover image to hide secret file, our algorithm conceals the source texture image and embeds secret file through the process of texture synthesis. This allows us to extract the secret file and source texture from a

Synthesis Table		
	Conventional texture synthesis	Message oriented texture synthesis
Shape of the overlapped area	L- shape only	Five different shapes
Candidate selection	A threshold with random selection	Referring to the secret file
Synthesized Result	A pure large texture	A large texture containing source texture and secret file

stego synthetic texture. Our approach offers three distinct advantages. First, our scheme offers the compression capacity that is up to the size of the stego texture image. Second, our steganographic approach very different from existing approaches on steganography. Third, the quality output is one, which meets the requirements of the end user and presents the information clearly. Experimental results have verified that our proposed algorithm can provide various numbers of embedding capacities, produce a visually plausible textureimages, and recover the source secret file.

III. RELATED WORKS& THESIS

Texture synthesis has received a lot of attention recently in computer vision and computer graphics. The mostrecent 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 newsynthesized texture image with similar local appearance and arbitrary size.

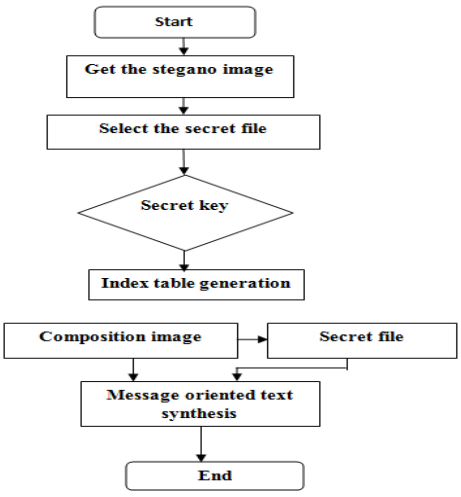

Fig 2.Data flowchart of proposal system

A. SECRET FILE EMBEDDING PROCEDURE:

In the proposal system secret file embedding procedure is different when compare to the existing system.In the proposal system Sender can select any size of file to send,after selecting a secret file sender can able to compress the cover image up to size of the secret image.After compression process we need to provide 8 digit or character secret key to the message for encryption process.After encryption we embed the encrypted message with cover image, after embedding process it will convert as stego image

B.EMBEDDING CAPACITY

In the secret file each latter Representation by its equivalent ASCII code. Conversion of ASCII code to equivalent 8 bit binary number. Division of 8 bit binary number into two 4 bit parts Choosing of suitable letters from file related to the 4 bit parts. Meaningful sentence construction by using letters obtained as the first letters of suitable words.

DECODING PROCESS

First letter in each word of cover message is taken and represented by corresponding 4 bit number. 4 bit binary numbers of combined to obtain 8 bit number ASCII codes are obtained from 8 bit numbers Finally secret message is recovered from ASCII code

IV. EXPERIMENTAL RESULTS

A. Hiding secret image file inside a cover image

Hiding image inside a cover image is sub part of the stegnography.First we are selecting a secret image and we converting that image file to byte code and we are storing that byte code in to defined byte array.After that we combining that secret file with cover image.

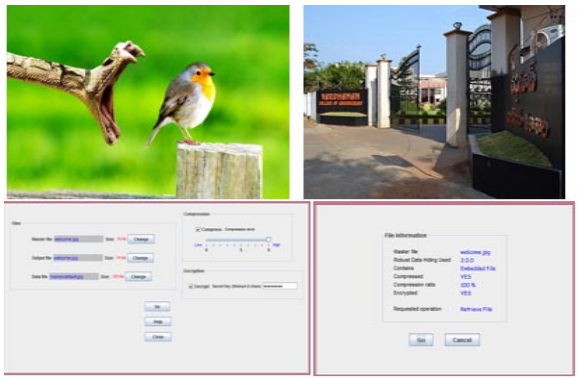

Fig. 4 Hiding image file

B. Hiding message inside a cover image

In the proposal system Sender can select any size of file to send,after selecting a secret message file sender can able to compress the cover image up to size of the secret message.After compression process we need to provide 8 digit or character secret key for encryption process.After encryption we embed the encrypted message with cover image, after embedding process it will convert as stego image

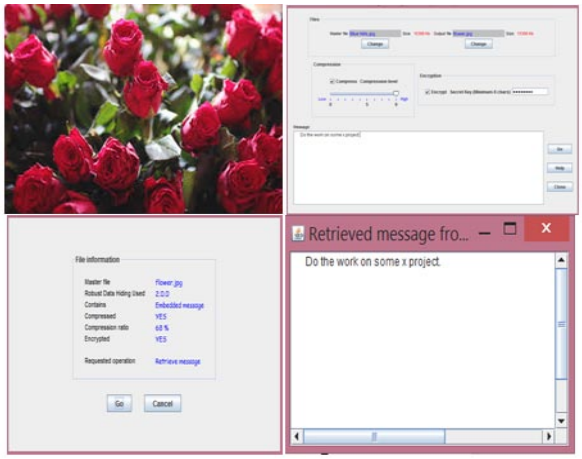

Fig. 5Hiding a secret message

C. Embedding file(Video or audio)

Audio and video steganography is sub part of the steganography.In the steganography we can hide a secret audio or video file behind the other cover file or behind the image file.

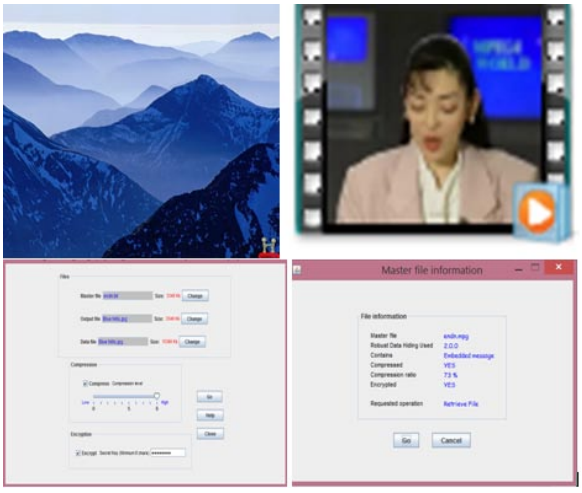

Fig.6 Hiding a audio or video file

d. Results of Different Message Probabilities

The secret messages consist of bit stream “0” or “1.” The experimental results shown so far consider thatbit “0” or “1” has equal probability of appearance. However, equal probability may not be the case for somekinds of information to be served as a secret message. Wegeneralize our scheme by considering the probability of appearance

D.Steganalysis

The process of detecting presence of a message that has been hidden using steganography.

Steganalysis approaches:

a. Targeted steganalysis.

b. blind steganalysis.

V. CONCLUSION

We have proposed a novel based apporach for improving the steganalysis performance and also analyzing the hiding capacities of the existing research work. The steganalysis performance of state-of-the-art detectors is near-perfect against current steganographic schemes. A novel, robust and secure hiding schemes that can resist steganalytic detection must be implemented. Hiding schemes are characterized by three complementary requirements-security against steganalysis, robustness beside distortions in the transmission channel, and capacity in terms of the embedded method. This work would be able to be extended for different formats of images. This work may be extended using other transforms methods also.

REFERENCES

[1]Kuo-Chen Wu and Chung-Ming Wang, “Steganography Using Reversible Texture Synthesis”, IEEE Trans., Image Processing, Vol 24, no. 1,pp.130-139,2015.
[2] N. F. Johnson and S. Jajodia, “Exploring steganography: Seeing the unseen,” Computer, vol. 31, no. 2, pp. 26-34, 1998.
[3] N. Provos and P. Honeyman, “Hide and seek: an introduction to steganography,” Security & Privacy, IEEE, vol. 1, no. 3, pp. 32-44, 2003.
[4] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, “Information hiding-a survey,” Proceedings of the IEEE, vol. 87, no. 7, pp. 1062-1078, 1999.
[5] 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.
[6] 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.
[7] 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.
[8] 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.
[9] 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.
[10] 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.
[11] A. A. Efros and T. K. Leung, "Texture synthesis by non-parametric sampling," in Proc. of the Seventh IEEE International Conference on Computer Vision, 1999, pp. 1033-1038.
[12] C. Han, E. Risser, R. Ramamoorthi, and E. Grinspun, "Multiscale texture synthesis," ACM Trans. Graph., vol. 27, no. 3, pp. 1-8, 2008.
[13] 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.
[14] H. Otori and S. Kuriyama, "Texture synthesis for mobile data communications," IEEE Comput. Graph. Appl., vol. 29, no. 6, pp. 74-81, 2009.
[15] 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.
[16] K. Xu, D. Cohen-Or, T. Ju, L. Liu, H. Zhang, S. Zhou, and Y. Xiong, "Feature-aligned shape texturing," ACM Trans. Graph., vol. 28, no. 5, pp. 1-7, 2009.