Concealing of secret Information Using Steganography

Architha H[1], Grace Sushmitha J[1], Mohamed Aqib Ali R[1], Mohan Kumar C[1], Rekha T S[2]

[1.] UG Students, Dept. of CSE, SRS Institute of Technology, Bangalore, India

[2.] Assistant Professor, Dept. of CSE, SRS Institute of Technology, Bangalore, India

Abstract: The Internet allows for easy extraction of messages over large areas. This is both an advantage and disadvantage since people all over the world can view your image but not your information. Encrypting data has been the most popular approach of protecting information but this protection can be broken with enough computational power. An approach to encrypting data [1] would be to hide it by making this information look like something else. This way people would realize its true content. In particular, if the important data is inside an image then everyone can view it as a picture. This technique is often called data hiding or steganography.

Keywords: Security, Secret data hiding, Steganography, low capacity.

I. Introduction

Stego means covered and graphia means writing which is mainly derived from Greek language[1]. Steganography is mainly used for maintaining secrecy in communication in which highly confidential messages are hidden behind the images by sending source texture into composite table. Steganography and cryptography are merely related to each other where in cryptography information is hidden inside the text, but in steganography information is hidden inside the image so that even if tried to see the hidden information only image is seen but not the information which is behind the image. Knowing a hidden message will only be possible with knowledge of the key that is required to uncover it. So this method will be more effective when compared to the cryptographic methods.

Steganography plays a very major role in maintaining security. When compared with steganography, cryptography is very much low in maintaining security. In cryptography only 60-70% of security is given. In our daily life we all know that communication is very important, moreover all our message cannot be shared with everyone.(Eg: if a military people wants to communicate with each other and if their opponents hack the data cable the entire information will be known to the hacker). To avoid such conditions we mainly go for steganography technique.

Hiding information behind an image uses different types of techniques like LSB (least significant bit) and image steganography [2], to conceal information. Here true color images (24 bit images) are generally used as covered data. The input messages are broken up into square blocks of 8*8 pixels. If the data to embed (8*8 blocks at a time in the cover file is found to be complex, it can be directly embedded into the complex box of the cover image. If not it would conjugate (exclusive-OR) the data with a white checker board pattern (the most complex pattern)[3] to ensure minimum complexity.

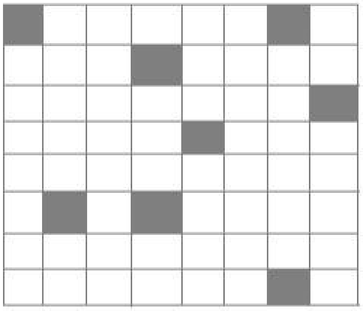


Fig 1. Checker Board

If an algorithm called steganalytic is implemented on this 8*8 checker board image pixel, the clarity of an image goes down and the unknown person can easily view the secret information, it is clearly shown in the below figure(a).

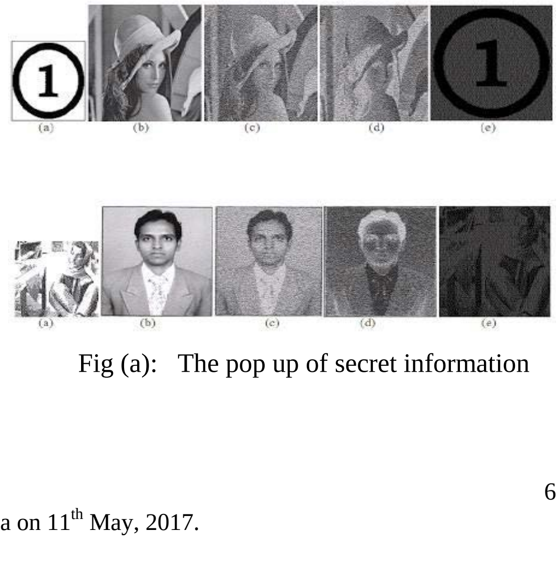


Fig (a): The pop up of secret information

The above fig (a) tells that the secret information when hidden behind the image, the clarity of the image goes down so that the hacker can easily get to know that there is some information hidden behind the image [4] and when the steganalytic algorithm is applied the hidden message is easily popped up.

II. Proposed System

To overcome the problems faced in the existing system (i,e., dividing the image into 8*8 checker board pixels) we are making the copies of an image(8*8 copies). Here we make use of Reversible Texture Synthesis algorithm to make the copies of an image. When this algorithm is used even if steganalytic algorithm [1] is applied on the source image the clarity of an image regains, it doesn't go down and local appearance remains same. In this method the same image can be reused several times.

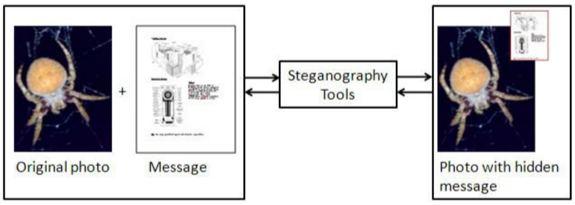


Fig 2. Concealing information using texture Synthesis

A. *Message Embedding Procedure*

For message embedding, we make use of Image Steganography technique to hide the information behind an image. Also this procedure uses three types of the following process.

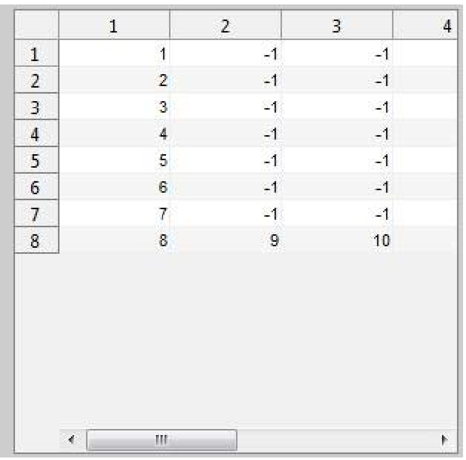
a) Index Table Generation Process

b) Patch composition process

c) Message Oriented Texture Synthesis Process

a) Index Table Generation Process

The primary procedure is the list table generation where we deliver a list table to record the location of source patch in the synthetic texture.



	1	2	3	4
1	1	-1	-1	
2	2	-1	-1	
3	3	-1	-1	
4	4	-1	-1	
5	5	-1	-1	
6	6	-1	-1	
7	7	-1	-1	
8	8	9	10	

Fig (b): Generation of Index Table

The above fig(b) shows that where exactly an information can be embedded. In the fig(b), -1 tells us that the information can be stored at that particular location. The numbers other than -1 tells us that the location is already embedded with some information.

b) Patch Composition Process

The second process of our algorithm is to paste the source patches into a workbench to produce a composition image. First, we establish a blank image as workbench which is equal to the size of the workbench is equal to the synthetic texture. By referring to the source patch IDs stored in the index table, we then paste the source patches into our workbench. During the pasting process, if no overlapping of the source patches is happened [5], we paste the source patches directly into our workbench, however , if pasting locations cause the source patches to overlap each other, we employ the image quilting technique to reduce the visual artifact on the overlapped area.

c) Message Oriented Texture Synthesis

Now we have index table and composition image, and we have pasted source patches directly into the work bench. We will embed our secret message via the message-oriented texture synthesis to produce the final stego synthesis texture [3]. The source texture being converted into a number of source patches has been pasted as part of the content in the large synthetic texture. In additional, the output large texture has been concealed with the secret message.

d) Capacity Determination

The embedding capacity of our algorithm can offer be related to the capacity in bits that can be concealed at each patch(BPP, bit per patch), and to the number of embeddable patches in the stego synthetic texture(EPn). Each patch can be conceal atleast one bit of the secret message[6]; thus the lower bound of BPP will be one and the maximal capacity in bits that can be concealed at each patch is the upper bound of BPP, has denoted by BPP max.

e) Message Extraction Procedure

The message extraction process at the reciever side involves generating the index table, retrieving the source texture, performing the texture synthesis and extracting and authenticating the secret message hidded into the stego synthetic texture. The extracting procedure contains 4 steps. The secret key held in the receiver side, the same index table as the embedding procedure can be generated. The next step is source texture recovery. In the third step, we apply the composition image generation to paste the source patch into the work bench to produce composition image by referring to the index table[3]. Final step is the message extracting and authentication step.

III. Experimental Work

The proposed contains the findings of the present system and recommendations to overcome the limitations and problems of the present system and uses REQUIREMENTS [5].

To describe the system study more analytically, the system study phase passes through the following steps:

- Problem identification and project initiation.
- Background analysis.
- Interface or findings.

a) Economic feasibility

This is carried out to check the economic impact that the system will have on the organization. The amount of fund that company can pour into the research and develop of the system is limited [8]. The expenditure must be justified. Thus the developed system is well within the budget and this was achieved because most of the technologies are freely available [7]. Only customized products had to be purchased.

b) Techincal Feasibility

This is to check the technical feasibility, i,e., the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. This will lead to high demands on the available technical resources. This will lead to high demands being faced on the client[4]. The developed system must have a modest requirement; as only minimal or null changes are required for implementing this system.

c) Social Feasability

The aspect of study is to check the level of acceptance of the system by the user. This includes the process of training the user to use the system efficiently. The user must no threatened by the system, instead must accept it as a necessity. The level acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make him familiar with it[9]. Their level of confidence must be raised so that he is also able to make some constructive criticism, which is welcomed, as they are the final users of the system.

IV. CONCLUSION

This proposes concealing of information by algorithm called reversible texture synthesis. If a source texture is given, it produces a stego synthetic texture. The techniques and algorithms used in these methods is the best of our knowledge. We assume that the proposed method will provide many opportunities for remaining applications of steganography.

Our future study is to use the algorithm for non-uniform and coloured images. Another study would be combining many steganographic approaches which increase the embedding capacity.

REFERENCES

[1] IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 24, NO. 1, JANUARY 2015 Steganography Using Reversible Texture Synthesis Kuo-Chen Wu and Chung-Ming Wang, Member, IEEE.

[2] 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, Oct. 2013.

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

[4] N. Provos and P. Honeyman, “Hide and seek: An introduction to steganography,” IEEE Security Privacy, vol. 1, no. 3, pp. 32–44, May/Jun. 2015

[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, Oct. 2015.

[6] S.G.K.D.N. Samaratunge, (August 2015): New Steganography Technique for Palette Based Images, Second International Conference on Industrial and Information Systems, ICIIS 2015.

[7] N. Provos and P. Honeyman, “Hide and seek: An introduction to steganography,” IEEE Security Privacy, vol. 1, no. 3, pp. 32–44, May/Jun. 2013.

[8] R.J. Anderson, F.A.P. Peticolas, (May 2014): On the Limits of Steganography, IEEE Journal of Selected Areas in communication.

[9] Y.-M. Cheng and C.-M. Wang, “A high-capacity steganographic approach for 3D polygonal meshes,” Vis. Comput., vol. 22, nos. 9–11, pp. 845–855, 2016.