RESEARCH ARTICLE OPEN ACCESS

Confidential Audio Transmission using Image Slicing

Vivek Solavande
Department of Computer Science
LTCOE
Mumbai - India

ABSTRACT

As we know internet is the backbone for information sharing and retrieval. Large amount of information is being shared. It is necessary to protect this information from unauthorised access. In this the secret colour image of any format in which secret audio is hidden is divided into multiple slices. And individual slice does not give any idea about the original secret image. The secret image is visible after merging the slices. These slices can be sent over the internet to the desired receiver. The receiver can get the secret image and can extract secret audio file from that image. In this proposed method the secret image and secret audio file is encrypted in order to avoid the hacker's intervention and transmitted securely.

Keywords:- Slice,Block,Patch Etc.

I. INTRODUCTION

The digital information such as documents, images and audio file can be transmitted over the internet. During the transmission this information may be accessed by the unauthorised users. For the secure transmission of such digital data various mechanisms are developed up to now.For transmission of such type of data, there are two different technologies. In first technology the information is protected by changing the information using some mathematical function which act as the key this process is known as encryption. In second technology secret data is hidden in other information this process is known as cryptography.

Our aim is to develop a mechanism which will encompasses the encryption as well as embedding secret data. The image slicer will divide the secret image which contains the secret audio file into slices which does not reveal the secret image and message. If the images are printed on transparent pages and it that copies are superimposed we get the secret image without the help of the computer. If we create few slices we could get only outline of the secret image. If we increase the no of slices and stacked together the original secret image will be more visible. The generated slices are random looking images which creates the interest of the hackers. With the image encryption the secret audio file is embedded and it is transmitted through this image.

In the following section II the background overview on image slicing is discussed. In section III drawback of the current system, section IV discussed proposed system and conclusion is discussed in section V and references used are listed at the end of this paper.

II. LITERATURE SURVEY

- Up to now various techniques are developed in order to create the slices of an image. The experiments were performed on black and white image in which the secret image is partitioned into n slices and and only one slice is transmitted to receiver if k or more slices are merged together the secret images is visible without the help of the computer. If the number of slices is less than k then the secret image is not visible. But due to the expansion of pixels caused the storage space was wasted.[1] .
- The (2, 2) VC scheme divides the secret image into two slices and getting secret image from a slice is impossible. Each slice is printed in transparencies. Fig 1 gives the idea about how slices are merged and depending on the white and black pixel the resultant slice is appeared.

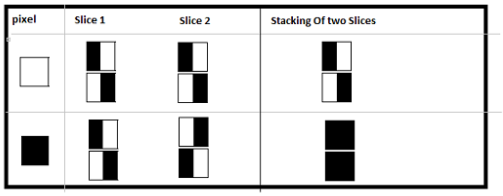

Fig.1

- Then experiments were performed with taking into consideration the probability [2] with conventional image slicing.
- Then slices with different sizes were created of binary images [3-4].
- In paper [5] the two images were encrypted at the same time in which pixel expansion technique is not used which reduced the storage space.
- Later the slices were created in which the contrast of the grey image is reduced [6] .
- Then multi-resolution techniques is used in which pixels are divided into 3×3 blocks [7] of which eight pixels gives idea about grey value and one pixel gives idea about halftone value.

- Research carried out by dividing image into more slices [8]. Black pixel of the secret image is expanded by dividing into four blocks and white pixel is converted into two white and two black blocks. As the selection of the blocks the slice is random in nature it is not guaranteed that black pixel of the secret image stacked onto all black blocks and white pixels onto two white and two black blocks after stacking all the slices. Therefore the image quality may be poor.
- Then enhancement is done [9] in which the two matrices are created which gives idea of the sharing of the pixel. In first matrix all the elements of first row will be one and remaining elements will be zero. And in second matrix all the diagonal elements will be one and remaining will be zero. Because of this when the pixels are shared the index of the black pixel on every slice will be same and it will appear on the same index and probability of the white pixel will be 0.5 if there are two images which results into good quality of the image as the black and white contrast gets sharpen.
- Then an experiment carried out in which the number of slices are increased to get the image clearer [10].

III. DRAWBACK OF CURRENT SYSTEM

- As the pixel expansion is used the slice size becomes larger compare to secret image which require large space to store and recovered image may be of poor quality .The slices generated are of fixed numbers.
- All the methods are applicable to black and white images.
- The research on hiding one multimedia data in other multimedia is done such as hiding text message into image, hiding one image in another image without changing the property of an image. This process is known as image steganography. Up to now many researches has been done in which audio file was carrier for any other file such as message, image and audio file .No research is done on hiding the audio file in image.

IV. PROPOSED SYSTEM

To overcome the drawbacks of the various methods which are applied up to now we propose a new innovative method. In proposed system we develop the encoder and decoder. The encoder takes the original secret image and secret audio file with number of slices to be made as input. The encoder will embed the audio file in image and divide the image into number of slices as per the need. Up to now the number of slices created was fixed. In this proposed system we can provide the facility to create the slices in dynamic nature. According to the input we can calculate the statistics. As per the block size the image is divided into rows and columns.

Then we can create the blank images according to the number of slices in which pixels value will be zero. We can calculate the index position of the blocks and maintain in an array. As the slices should be random images the random block is being taken and it is put on the slice on the same position. At the same time counter needs to be maintained in order move on to the other slice. Thus pixels are put on the slices randomly. The created slices can be stored and transmitted via distinct route.

A. Algorithm for Encoder

1. Input: Secret image with secret audio file, block size, number of slice
2. Output: slices of secret image. Key file
3. Accept secret image
4. Accept the secret audio file.
5. Substitute the bit of the audio file into least significant bit of the image.
6. Accept block size and get total slice.
7. Calculate all statistics like,
8. Cols = width / block size
9. Rows = height / block size
10. Total blocks = rows * cols
11. Blocks per slice = total patches / slices
12. Generate blank slice images and store in slide array
13. Generate XY coordinates of all patches and store in BlockXY array
14. Generates blockID array for shuffling
15. Shuffle the array
16. For(i=0; i<=total blocks; i++)
    a. Fetch the coordinate of x,y of current block
    b. Copy all the pixels of current block to the selected slice
17. Increment slices and goes to step 8.
18. Save slice.
19. Store all the information about the pixel positions in key file.

B. Algorithm for Decoder

Input: key file

Output: final images same as secret image and secret audio file

1. Open key file.

2. Read all the positions of the pixels.
3. For (i=o; i<total slices; i++)
   3.1. Perform XOR operation of all the pixel of current slice and stacked slice
4. Extract the audio file by reverse process of substitution of bits.
5. Get the secret image
6. Get the secret audio file.
7. Save image

C. Modules

There are two models in proposed system encoder and decoder.

Encoder : This Encoder take the input as a secret image and audio file .The number of pixels of the audio file should be less than the number of bits of image file. The encoder first embeds the audio file and then divides that image into n slices as shown in figure 1.The slices are created by randomly putting the pixels of the secret image onto the blank images.

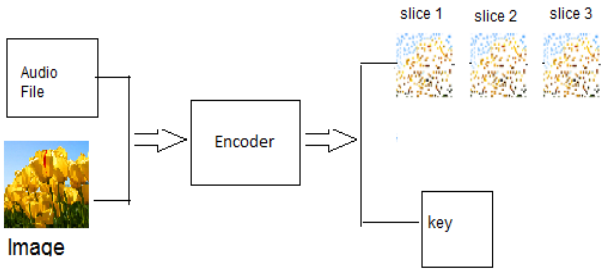

Fig.2

Decoder: The decoder takes the key file generated by encoder as input. It reads the key file and generates the secret image file by putting all the pixels and extracts the secret audio file from image.

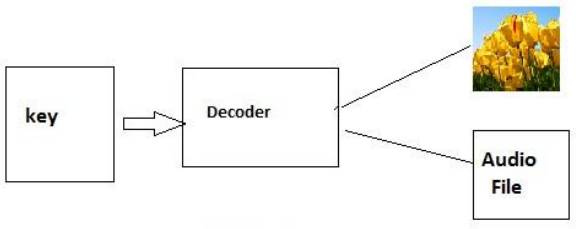

Fig.3

V.CONCLUSIONS

The proposed method is a two-in-one method that not only shares an input image, but also hides an extra audio file that is more confidential. Because slices are transmitted using different channels or stored in different places, the chance that slices are intercepted is very low. However, unauthorized person who might intercept or access slices cannot get the secret image and finally audio file without key .The original secret image can be visually obtained only when all the slices are available and well stacked together.

REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," in Proc. Adv. Cryptal: EUROCRYPT, vol. 950. 1995, pp. 1–12.

[2] R. Ito, H. Kuwakado, and H. Tanaka, "Image size invariant Visual cryptography,"IEICE Trans. Fundamentals Electron. Common. Comput.Sci. vol. E82-A, no. 10, pp. 2172–2177, 1999.

[3] G. Ateniese, C. Blonde, A. D. Santi's, and D. R. Stinson, "Visualcryptography for general access structures," *Inform. Computat.* vol. 129,no. 2, pp. 86–106, 1996.

[4] P. A. Eisen and D. R. Stinson, "Threshold visual cryptography Schemes with specified whiteness levels of reconstructed pixels," *Des. Codes Crypt.* vol. 25, no. 1, pp. 15–61, 2002.

[5] S. J. Shyu, "Image encryption by random grids," Patt. Recog., vol. 40,no. 3, pp. 1014–1031, 2007.

[6] Y. C. Hou, C. Y. Chang, and C. S. Hsu, "Visual cryptography For colour images without pixel expansion," in Proc. CISST, vol. I. 2001, pp. 239–245.

[7] "Multi-pixel Visual Cryptography for colour images with Meaningful Shares" by Ms. Kiran Kamari et. al. / International Journal of Engineering Science and Technology Vol. 2(6), 2010, 2398-2407

[8] W. P. Fang and J. C. Lin, "Progressive viewing and sharing of Sensitive images," *Patt. Recog. Image Anal.*, vol. 16, no. 4, pp. 638–642, 2006.

[9] Young-Chang Hou and Zen-Yu Quan "Progressive Visual Cryptography with Unexpanded Shares", Ieee Transactions On Circuits and Systems for Video Technology, Vol. 21, No. 11, November 2011

[10] Progressive visual cryptography with watermarking for Meaningful shares, JITHI P V, ANITHA T NAIR. 978-1-4673-5090-7/13/$31.00 ©2013 IEEE.