An Efficient Steganography Using Mosaic Image with Enhanced Security

Anisha S[1], Neethu Maria John[2]

[1]PG Scholar, Dept of CSE, Mangalam College of Engineering, Mahatma Gandhi University, Ettumanoor, Kottayam, Kerala, India

[2]Assistant Professor, Dept of CSE, Mangalam College of Engineering, Mahatma Gandhi University, Ettumanoor, Kottayam, Kerala, India

Abstract: ***This paper presents an image hiding method using secret fragment visible mosaic image. In this method the confidential image is converted into secret fragment mosaic image of same or varied sizes. Mosaic image is created by composing small fragments of the secret image in to target image, resulting an effect of embedding the confidential image secretly in the resulting mosaic image. Color characteristics of the tile images are changed to make it similar as the target image. Further improvement on security is conducted by shuffling the mosaic image again and dividing the tile images in different sizes. Secret image is recovered from the mosaic image without any distortions.***

Keywords: mosaic image, encryption, shuffling.

1. Introduction

Steganography is the science of hiding of some data into another data. There are different types of steganography like text, image and video steganographies. Image steganography is hiding a secret image into another cover image.

The construction of mosaic images and the use of such images on several computer vision or graphics applications have been active areas of research in many years. Mosaic is a kind of artwork created by composing small pieces of materials, such as stone, glass, tile, etc. There are different types of mosaic images like crystallization mosaic, ancient mosaic, photo-mosaic, and puzzle image mosaic. The first two types are from decaying a source image into tiles and reconstructing the image by correctly painting the tiles, and so they both may be called *tile mosaics*. The other two types of mosaics are by placing images from a database to cover an assigned source image, and both may be called *multi-picture mosaics*.

In this paper, a new methodology for secure image transmission is proposed, which is to change a confidential image into a Mosaic image seeming to be like the preselected target image. The mosaic image is the result of organizing the piece parts of a confidential image in a manner in order to camouflage the other image called the cover image. The transformation process is followed by another shuffling and encryption which will enhance the security of the method. Appropriate schemes are also proposed to conduct *nearly-lossless* revival of the original secret image.

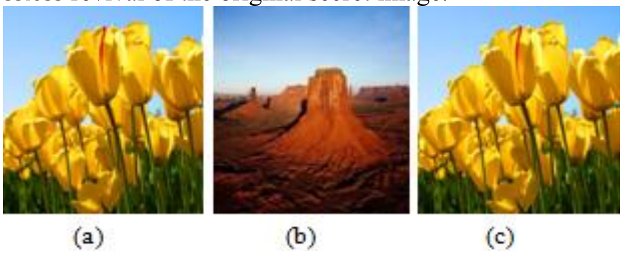

Figure1: Result of the proposed method (a)secret image (b)cover image(c)secret fragment mosaic image from (a) and (b) by the method

2. Related Works

2.1 A New Secure Image Transmission Technique via Secret-Fragment-Visible Mosaic Images by Nearly Reversible Color Transformations

In this paper, Ya-Lin Lee propose a technique for the transmitting of the secret image securely and lossless. This method transforms the secret image into a mosaic tile image having the same size like that of the target image which is preselected from a database. This color transformation is controlled and the secret image is recovered lossless from the mosaic tile image with the help of the extracted relevant information generated for the recovery of the image [1].

2.2 Secret Fragment Visible Mosaic Image Using Genetic Algorithm

This paper presents an image hiding method using fragment visible mosaic image. In this method the secret image is divided into blocks or tiles and they are shuffled or reordered to become a target image in the mosaic form. In the existing method an image similarity measure, h-feature is defined using the color distribution in the pixels. The h-feature is used to select the most appropriate cover image for the secret image from an image database and also for the tile shuffling process. Since the tile re-ordering is done in a single iteration the performance is limited. So a genetic algorithm is used here in the tile shuffling by choosing PSNR as the match criterion to improve the quality of encrypted image.[2]

2.3Hiding data in images by simple LSB substitution

In this paper, a data hiding scheme by simple LSB substitution is proposed. By applying an optimal pixel adjustment process to the stego-image obtained by the simple LSB substitution method, the image quality of the stego-image can be greatly improved with low extra computational complexity. The worst case mean-square-error between the stego-image and the cover-image is derived. Experimental results show that the stego-image is visually indistinguishable from the original cover-image. The obtained results also show a significant improvement with respect to a previous work.[3]

3. Proposed Scheme

In this paper, a new technique for secure image transmission is proposed, which transforms a confidential image into a significant mosaic image with the same size and looking like a preselected cover image. The alteration process is followed by a shuffling method which is controlled by a secret key, and only with the key can a person recuperate the secret image nearly lossless from the mosaic image. The mosaic image is the result of reorganization of the fragments of a secret image in cover up of another image called the cover image which is selected freely from any where.

As an illustration, Fig. 1 shows a result yielded by the proposed method. Explicitly, after a target image is selected randomly, the given secret image is first divided into fragments called tile images, which then are fit into comparable blocks in the target image, called target blocks, according to a resemblance measure based on color variations. Next, the color characteristic of each tile image is altered to be that of the related target block in the target image, resulting in a mosaic image which looks like the target image. The mosaic image is encrypted using a key followed by shuffling of the image which enhances the security. Appropriate schemes are also proposed to carry out nearly lossless recovery of the original secret image from the resulting mosaic image. The proposed method can alter a secret image into a disguising mosaic image without compression, while a data hiding method must hide a highly compressed version of the secret image into a cover image when the secret image and the cover image have the same data volume.

3.1 Phases of the Scheme

The main phases of the system are shown in the flow diagram

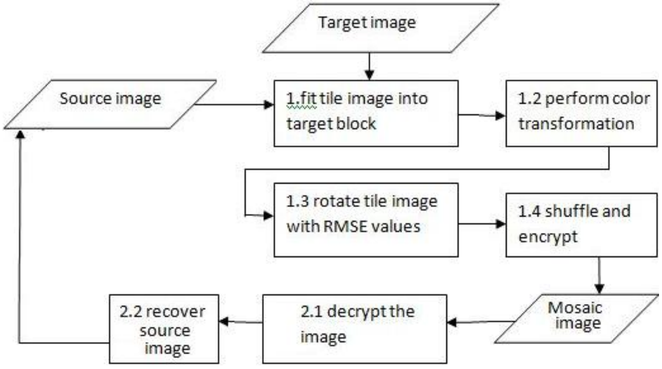
Target image
Source image
1.fit tile image into target block
1.2 perform color transformation
1.3 rotate tile image with RMSE values
1.4 shuffle and encrypt
Mosaic image
2.1 decrypt the image
2.2 recover source image

Figure 2: Flow diagram of the method

3.1.1 Mosaic image generation

This phase includes the following stages:

a) A cover image is selected freely.
b) Placing the tile images of the secret image into the target blocks of the selected cover image
c) Alter the properties of the cover image to make it similar to the secret image
d) A new image is created to store the mosaic image
e) After the mosaic image is created it is encrypted and shuffled again
f) Embedding relevant information into the created mosaic image for future recovery of the secret image

3.1.2 Secret image recovery

This phase includes the following stages

a) decrypt the mosaic image
b) retrieving the embedded information from the mosaic image
c) reconstructing the secret image from the mosaic image using the retrieved information.

a. Image Parts Creation

After the selection of the cover image, the very first step is to divide the secret image and the cover image into different parts**.** The size of the parts can be fixed or varied .The varied sized parts make the retrieval of the secret image more difficult for an attacker. The cover image should be larger than the secret image so that one pixel of the secret image is mapped in to one byte of the cover image. So in order to keep the three bytes of the secret image we need more pixels of the cover image. In addition to this extra information should be kept on the cover image like the order, position of the parts etc. So the cover image size should be larger than data image.

b. Finding pixel to pixel relation of the parts

The pixel to pixel relation between the parts is found to get the most similar parts of the secret image and the cover image. It is calculated using the R.M.S.E values of the parts of the images. The average values of the red, green and blue component of each part in the secret image and the cover image is calculated. Their differences give the R.M.S.E values of the corresponding parts. Using these methods the RMSE values of all the parts of the images are calculated and all these values are compared with each other to find out the minimum value. These minimum valued part of the cover image is selected to place the corresponding part of the secret image

c. Mosaic image generation

After finding out the most similar parts of both images, each of the pixels are combined together. Each pixels of the source and destination are stored in array. A new pixel is created to store the combined image. Each of these pixels are combined and stored in the new pixel. Additional information like height, width, position of the source image is also stored for further recovery.

After obtaining the mosaic image the image is encrypted and shuffled. A key is given for the encryption. Sequence generating functions are used for generating a random sequence for the shuffling of the image. The key is given as the seed of the function. Corresponding integer sequence is generated for each of the keys. So for the decryption part the same key should give as the seed so that the image should be recovered.

d. Secret image extraction

This is the last step of the project. The output of the extracted image is the same as the input. Before extracting the image first decrypt using the correct key. A wrong key will generate errors. After that do the creation process in reverse process. De-embedded the recovery information stored in the newly created image..There are two steps in the process. The regain process is based on width and height of tile image in mosaic making process.

In the new file the position are not in the same order . Repetitively select randomly an unselected block other than the first block from using the random number generator with the key as the seed, extract bits from all the pixels of using a reverse edition of the lossless LSB substitute scheme proposed in and concatenate them successively, until all the bits of are extracted. Transform every bits into an numeral which specify the index of a tile image in the original secret image, resulting in the secret recovery series. After getting the tile images from position file then there is no replication of images because the image is repeated then the name would be same and overwrite the previous image.

4. Experimental Results

A sequence of experiments have been conducted to test the projected method using many secret and target images with various sizes. To show that the created mosaic image looks like the preselected target image, the quality metric of root mean square error (RMSE) is utilized, which is defined as the square root of the mean square difference between the pixel values of the two images.

The quality of the project is measured in terms of the difficulty to recover the original image for an attacker. This difficulty increases as the degree of randomness is more. It is the measure of which the two parts of the source and cover image are how randomly placed. The degree of randomness can be saved each time when the project is run. There are four conditions to be considered. The number of divisions of the parts may be fixed or varied. The parts of the mosaic image may be shuffled or not. A set of experiments have been conducted with all these conditions and the results are saved. These results are used to plot a graph with number of parts in the x-axis and degree of randomness in the y-axis.

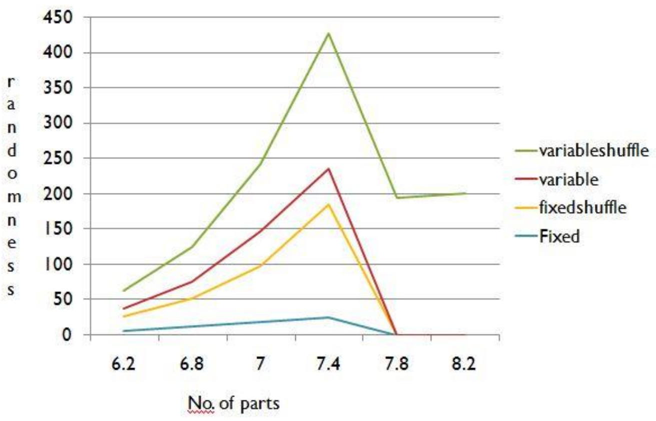

Figure 2: no. of parts against randomness

From the graph we can see that the level of randomness is the minimum in the fixed division of the parts without shuffling and the level is higher in the variable part division with shuffling, which is our proposed system .

5. Conclusion

Secret portion observable Mosaic Image can be used in image communication and also for secure keeping of secret images. The secret image is divided into blocks or tiles and these tiles are rearranged to form the mosaic image which visually looks like the cover image. The created image is encrypted and shuffled again with a secret key. Only with proper key the image can be extracted. Good experimental results have shown the achievability of the projected method

References

[1] Ya-Lin Lee, Wen-Hsiang Tsai," New Secure Image Transmission Technique via Secret fragment-Visible Mosaic Images by Nearly Reversible Color Transformations", IEEE Transactions on Circuits and systems for video Technology, vol. 24, no. 4, April 2014.

[2] Nithya Francis, Naveen N, "Secret Fragment Visible Mosaic Image Using Genetic Algorithm", International Journal of Advanced Trends in Computer Science and Engineering, (IJATCSE), Vol.2 , No.5, Pages :64-69 (2013) Special Issue of ICCECT 2013

[3] C. K. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution," Pattern Recognit.., vol. 37, pp. 469–474, Mar. 2004

[4] S Shen Wang, Bian Yang and Xiamu Niu, "A Secure Steganography Method based on Genetic Algorithm", Journal of Information Hiding and Multimedia Signal Processing Volume 1, Number 1, January 2010

[5] D. Coltuc and J. M. Chassery, "Very fast watermarking By reversible contrast mapping", IEEE Signal ProcesS, Lett., vol.14, no.4, pp. 255258, Apr. 2007

[6] Shakir M. Hussain1 and Naim M. Ajlouni," Key Based Random Permutation (KBRP)", Journal of Computer Science 2 (5): 419-421, 2006

Author Profile

Anisha S pursuing M.Tech in Computer Science and Engineering from Mangalam College of Engineering, Mahatma Gandhi University. She received B.Tech degree in 2009 from Ilahiya College of Engineering, Mahatma Gandhi University, Kottayam, Kerala, India. Her research interests are Relational databases,security, etc.

Neethu Maria John, received the M.Tech degree in Computer science & Engineering from Anna University, Chennai, in 2007. In 2007, she joined the Department of Computer Science & Engineering, Viswajyothi college of Engineering & Technology, Vazhakulam where she was an Assistant Professor. In 2010, she joined the Department of Computer Science & Engineering, Mangalam College of Engineering, Ettumanoor, as an Associate Professor. Her current research interests include Computer Architecture and Data Management and Theory of Computation. She is a Life Member of the Indian Society for Technical Education (ISTE).