International Journal of Electronics, Electrical and Computational System
IJEECS
ISSN 2348-117X
Volume 6, Issue 8
August 2017

Academic Science

Secret-Fragment Visible Mosaic Image Technique for Image Hiding

Manisha Ghortale
JSPM's Institute, RSCOE
Prof. R.R. Itkarkar, Dr. D. S. Bormane
AISSMS College of Engineering

ABSTRACT

The secret-fragment-visible mosaic image technique is developed for covert communication or secure keeping of secret images which is created automatically by composing small fragments of a given image to become a target image in a mosaic form, achieving an effect of embedding the given image visibly but secretly in the resulting mosaic image. Based on Standard Deviations calculated for all the tiles the secret tile image is fitted into similar tile image. Laβ color space technique is used to ensure similarity in colour characteristics of target image and secret image. Also it is logarithmic, which means that to a first approximation the uniform changes in channel intensity are equally detectable. The information of the tile image fitting sequence is embedded into randomly-selected pixels in the created mosaic image by a lossless LSB replacement scheme using a secret key; without the key, the secret image cannot be recovered.

INTRODUCTION

Security of Information transmitted over internet is a Crucial Issue now-a-days as many applications or fields require transmitting secret image over the internet that may contain private and confidential information that is needed to be protected from hacker or from unintended users. Many techniques and methods have been proposed to ensure security, out of them most commonly used techniques are encryption and data hiding. Problem with Image Encryption is that it ensures security but the resultant noise image attracts the attention of hacker so it may be possible after many trials they can be decrypted by hacker. Hence the most secure way of transmitting the secret information through the internet is by hiding the existence of secret image. This is data hiding method in which pieces of secret information is hidden behind a carrier that may be anything audio,text file, video or an image. Now a day's, for secure image transmission a new concept that is of mosaic image is used in the field of data hiding. Data hiding techniques focus on how to efficiently embed a piece of information into cover media data (also called "cover" or "host" data) to carry out specific missions used in the field of data hiding.

When viewed at low magnifications, the individual pixels appear as the primary image, while close examination reveals that the image is in fact made up of many hundreds or thousands of smaller images. Most of the times they are a computer-created type of montage. There are two types of mosaic, depending on how the matching is done. In the simpler kind, each part of the target image is averaged down to a single color. Each of the library images is also reduced to a single color. Each part of the target image is then replaced with one from the library where these colors are as similar as possible. In effect, the target image is reduced in resolution, and then each of the resulting pixels is replaced with an image whose average color matches that pixel.

In this project a new type of art image, called secret-fragment-visible mosaic image, which contains small fragments of a given source image is proposed Observing such a type of mosaic image, one can see all the fragments of the source image, but the fragments are so tiny in size and so random in position that the observer cannot figure out what the source image looks like. Therefore, the secret image may be said to be secretly embedded in the resulting mosaic image, though the fragment pieces which are all visible. And this is

the reason why the resulting mosaic image is named as secret-fragment-visible. The tiles are rearranged according to the values of Standard Deviation for the tiles of Secret Image and of Target Image. The rearranged image is then colour transformed using lαβ colour transformation method. This colour transformation converts the rearranged image to appear like the target image. This is how the fragments of secret image are made to look same as Target Image. This is useful for the application of covert communication or secure keeping of secret images such as transmitting military images, medical imaging system, confidential document, online personal photograph album and so on. Generally these images contain some secret and confidential information that is required to be protected from leakage so that only the intended users should be able to read that image. A secret fragment visible mosaic image is an image formed by dividing a given secret image into small tiles and transmitting these tiles of secret image in disguise of another image called as carrier image. Thus the resultant mosaic image can be used for covert communication or for secret image transmission. Only the person with authentication key can then convert this image into the secret image. The key is actually entered while processing of secret image; it can be of any length, alphanumeric, special characters etc. if the receiver have this unique key only then the secret image retrieval is done otherwise the process is aborted and the user sees only the cover image. It is very difficult to get the key for hackers as no specific standardization is used for the key there can be infinite no. of possibilities for the key. The proposed method is new in that a meaningful mosaic image is created, in contrast with the image encryption method that only creates meaningless noise images. Also, the proposed method can transform 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.

Figure 2: (a) (b) (c)

(a) Secret Image. (b) Target Image. (c) Secret-fragment-visible-mosaic image obtained by this project.

Any image can be selected as a secret and that of target image. Images are then resized automatically such that both the images have same dimension.

The whole process can be explained by Figure 3:

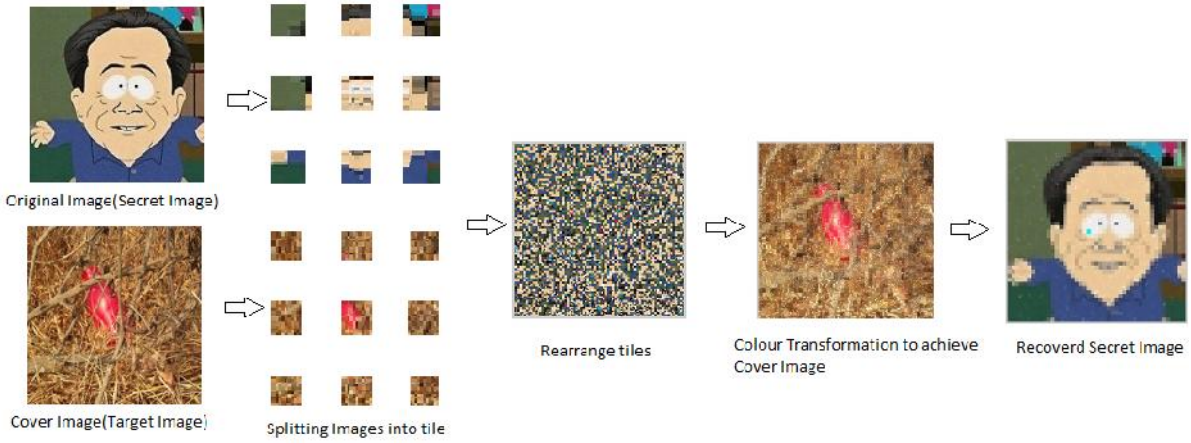


Figure 3. Illustration of creation of secret-fragment-visible mosaic image

RELATED WORKS

In this paper a new technique for creating a secret fragment visible mosaic image is proposed, in which the author select any random image of any size as carrier image for given secret image and by using this target image the author arrange the titles of secret image to form resultant mosaic image and performed reversible color transformation on mosaic image to reduce the distortion and also to recover the secret image exactly from the carrier image. [2]

Here In this paper the tile images obtained from secret images are rotated with θ = 0˚, 90˚, 180˚, 270˚ to get minimum RMSE value. RMSE is measure to show that the created image is mosaic image looks like preselected image; the method proposed in this paper provides minimum RMSE and lowest probability to guess the permutation correctly without the key. So breaking the system by this way of guessing is computationally infeasible.[3]

Here database is stored for target images a proper target image is selected for a particular secret image this is called content-based image retrieval. 1-D h colour scale technique is used for extracting Global Characteristics of colour distribution in image. This technique is more sensitive to human eye and also has lesser noise. Single-source shortest path problem, aims to find a path in a graph with the smallest sum of between-vertex edge weights. [4]

The tile shuffling done using Genetic Algorithm as raster-scan ordering is not that efficient as single iteration procedure for finding the most similar block limits the list of blocks from which match can be selected when the procedure is near to end. Experiment result of this technique shows that it gets better PSNR than the earlier method; the dissimilarity between the encrypted image and the target image is also reduced.[1]

Here MATLAB is used for LSB algorithm programming. The methodology followed is as follows: Conversion of image to matrix, Embedding process, Conversion of matrix to image, Extraction process. LSB doesn't contain any information there is no loss of information and secret image re-covering back become undistorted. Here the secret image is first converted into gray scale image and then compared with the size of target image. It must be smaller than that of target image only then LSB algorithm can be applied to the image. [5]

METHODOLOGY

The proposed method includes two main phases as shown by the flow diagram of Fig. 4:
1) Mosaic image creation and
2) Secret image recovery.

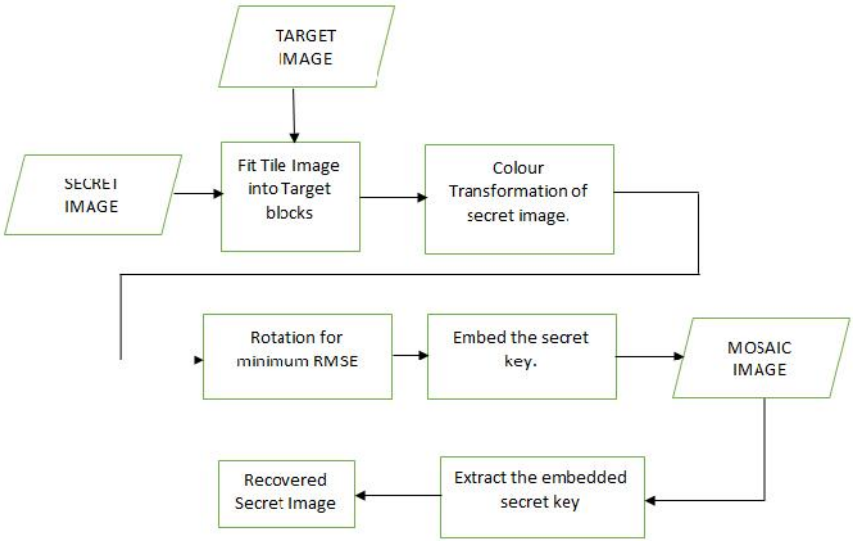


Figure 4: Flow diagram of the proposed method

International Journal of Electronics, Electrical and Computational System
IJEECS
ISSN 2348-117X
Volume 6, Issue 8
August 2017

Algorithm 1: Mosaic image creation

Input: The input to the algorithm are a secret image S, a target image T, and a secret key K.

Output: a secret-fragment-visible mosaic image F.

Step 1: Take the input s are secret image, target image and key.

Step 2: produce the tile blocks for secret image and target blocks for target image.

Step 3: Compute the mean and standard deviation for every tile block and target block.

$\mu_c = \frac{1}{n}\sum_{i=i}^{n} c_i$, where c_i - pixel values of C-channels such as red, green and blue. n – No. of pixels.

$$\sigma_c = \sqrt{\frac{1}{n}\sum_{i-1}^{n} (c_i' - \mu_c')^2}$$

Step 4: Compute the average standard deviation for every block and sort them.

$$c_i'' = q_c(c_i - \mu_c) + \mu_c'$$

Where q_c - standard deviation quotient

Step 5: Sort the tile blocks and target blocks according to the sorted average standard deviations individually.

Step 6: Map sorted tile blocks with the sorted target blocks.

Step 7: Create mosaic image fitting tile box according to the mapped target blocks.

Step 8: Transform the color of all the pixel of every tile image by utilizing mean and standard deviations.

Step 9: Pivot each changed tile to 90,180 and 270 degrees and compute root mean square error.

Step 10: Hold the pivot with least RMSE.

Step 11: Change over the mean and standard deviations for every tile block and mapped target block to binary.

Step 12: Convert tile rotation performed into binary.

Step 13: Concatenate the bit stream and compress into data to be implanted into the comparing tile box of the mosaic image.

Step 14: Will at last get the yield of mosaic image.

Algorithm 2: Secret image recovery

Input: The inputs to the algorithm are a mosaic image F with n tile images and secret key k.

Output: the secret image S.

Step 1: Separate the bit stream from mosaic image F by performing converse operation.

Step 2: Decode the bit stream by utilizing secret key K.

Step 3: Recuperate the desired secret image S by pivoting the tile images in a converse direction.

Step 4: Use the separated mean and standard deviation quotients to recover the original pixel values.

Step 5: Take the outcome as a final pixel values, resulting in a final tile image.

Step 6: Compose all the final tile images to form the desired secret image S as output.

RESULTS

Here I have considered the image of size 512*256 pixels and Tile Size = 4*4 pixels.

Figure 5

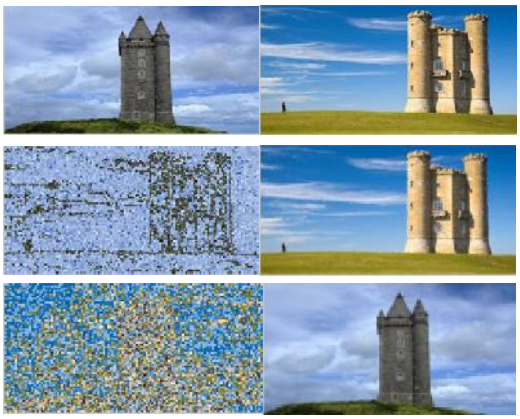


Figure 6

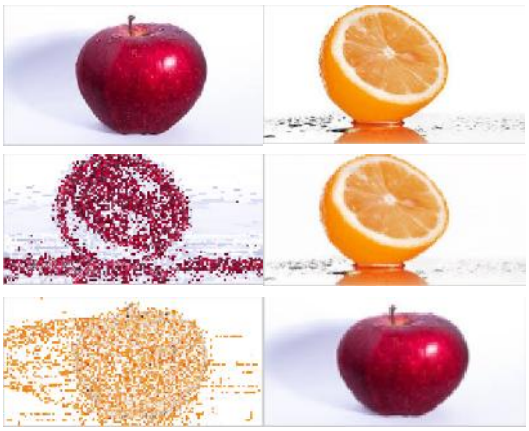


Figure 7

Figure 8

Sr. No.	Figures used as Secret Target Image (Image Size = 512x256,Tile Size = 4x4)	RMSE for Cover Image	RMSE for Recovered Secret Image
1	Figure 5	6.1679	6.2031
2	Figure 6	6.6140	4.1354
3	Figure 7	4.5162	2.4545
4	Figure 8	3.7374	2.3543

Table 1: RMSE values of images of same sizes and tile sizes.


Recovered image for size 1024 x 512 Retrieved image for 1024 x 512


Recovered Image in 512 x 256 Retrieved image for 512 x 256


Recovered Image for 256 x 128Retrieved image for 256 x 128

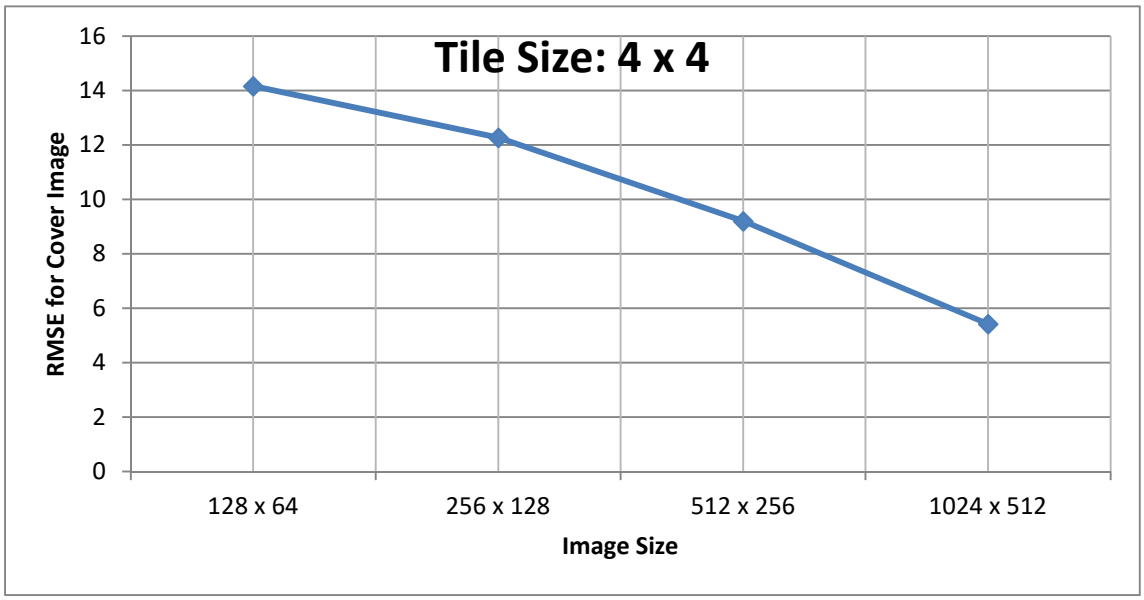

Recovered Image for 128 x 64 Retrieved image for 128 x 64

Figure 9

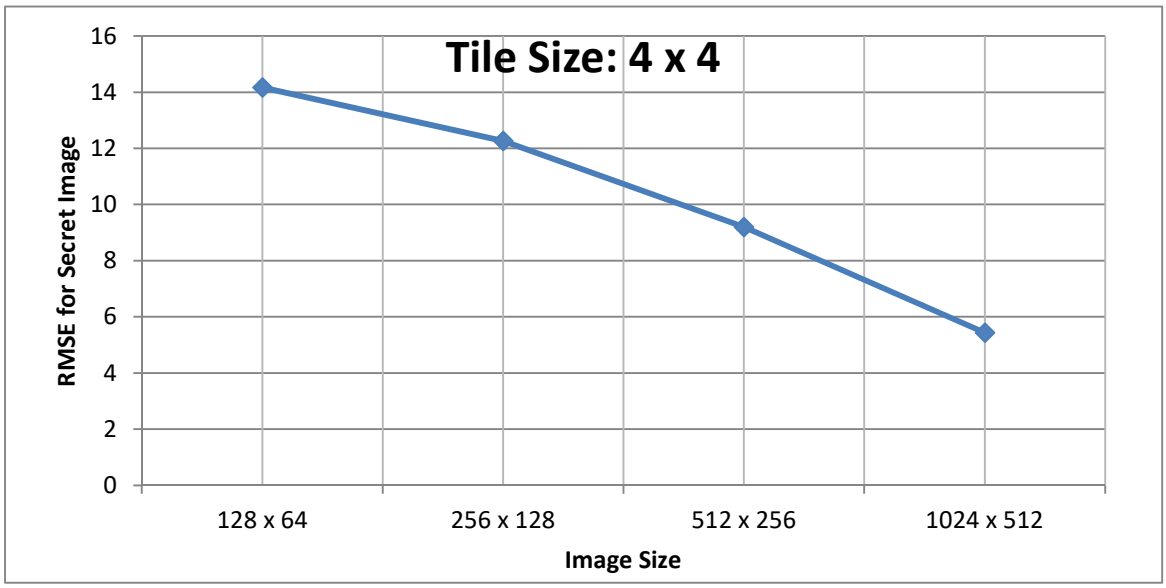
The tile size of image is kept constant as for Figure 9

Sr. No.	Figures used as secret Image and Target Image (Tile Size = 4x4)	RMSE for cover Image	RMSE for Recovered Secret Image
1	Image Size = 1024 x 512	5.4317	1.4816
2	Image Size = 512 x 256	9.2002	3.5237
3	Image Size = 256 x 128	12.2658	4.6808
4	Image Size = 128 x 64	14.1620	9.3618

Table 2: RMSE values of images of different sizes and constant tile sizes.



Graph of RMSE for Different Image size and constant tile size for Cover Image



Graph of RMSE for Different Image size and constant tile size for Secret Image

CONCLUSION

In this project secret image and target image are converted into a meaningful mosaic image. This technique allows the user to choose the image of their choice for use as a target image without the requirement of large database. Also we can recover the original secret image with no loss in the image quality. RMSE values for different images of different sizes with different tile size are calculated. From the graph plotted according to tile size and image of different sizes it is easily concluded that images of large sizes with small tile size have highest quality of retrieved secret image i.e. minimum RMSE value.

ACKNOWLEDGEMENT

I acknowledge with gratitude and humility our indebtedness to Mrs. R. R. Itkarkar, under whose guidance I had the privilege to work on this project. She helps us through critical stages and her timely suggestions enabled us.I also convey my sincere thanks to Mr.A. N. Paithane, HOD of E&TCfor his encouragement and cooperation. I express my special gratitude towards him. I express my heartfelt gratitude towards for Prof. Dr. R. K. Jain, Principal, Rajarshi Shahu College of EngineeringPune.

REFERENCES

[1] Nithya Francis, Naveen N. “Secret Fragment Visible Mosaic Image Using Genetic Algorithm” Special Issue of ICCECT 2013.
[2] Deepali G. Singhavi, P. N. Chatur, “A new method for creation of secret-fragment-visible-mosaic image for secure communication” IEEE Aug 2015.
[3] Y. L. Lee and W. H. Tsai, "A New Secure Image Transmission Technique via Secret-Fragment-Visible Mosaic Images by Nearly Reversible Color Transformations," IEEE Trans. on circuit and systems for video Tech., vol. 24, no. 4,pp. 695-703,april 2014
[4] Lai and W. H. Tsai, "Secret-fragment-visible mosaic image-A new computer art and its application to information hiding," IEEE Trans. Inf. Forens. Secur., vol. 6, no. 3, pp. 936-945, Sep. 2011
[5] Champakamala .B.S, Padmini.K, Radhika .D. K Asst Professors, Department of TCE, Don Bosco Institute of Technology “Least Significant Bit algorithm for image steganography”
[6] Daniel L. Ruderman, Thomas W. Cronin and Chuan-Chin Chiao, “Statistics of cone responses to natural images: implications for visual coding”, J. Opt. Soc. Am. A/ Vol. 15, pp. 8, August, 1998.
[7] Renji Elsa Jacob, Prof. Anita Purushotham, “Contrast Enhancement Based Reversible Image Data Hiding” National Conference on Signal Processing, Instrumentation and Communication Engineering (SPICE' 16), Vol. 5, Special Issue 4, March 2016.
[8] K. Sakthisudhan ,P. Prabhu, P. Thangaraj, “Secure Audio Steganography for Hiding Secret information” International Conference on Recent Trends in Computational Methods, Communication and Controls.
[9] Ali M. Meligy , Mohammed M. Nasef and Fatma T. Eid, “ An Efficient Method to Audio Steganography based on Modification of Least Significant Bit Technique using Random Keys” I. J. Computer Network and Information Security, 2015, 7, 24-29
[10] S. Gayathri, C.S.Manikanda Babu “Reversible Image Watermarking Using Modified Reversible Contrast Mapping” International Journal of Innovative Research in Science, Engineering and Technology, Vol. 5, Issue 5, May 2016.
[11] Mrs. Smriti Kumar, Mr.Deepak Singh, “ Colorization Of Gray Image In Lαβ Color Space Using Texture Mapping And Luminance Mapping” International Journal Of Computational Engineering Research (ijceronline.com) Vol. 2 Issue