ISSN 2347 - 3983

International Journal of Emerging Trends in Engineering Research (IJETER), Vol. 3 No.6, Pages : 243- 247 (2015)
Special Issue of NCTET 2K15 - Held on June 13, 2015 in SV College of Engineering, Tirupati
http://warse.org/IJETER/static/pdf/Issue/NCTET2015sp47.pdf

Reversible Color Transformations Technique for Secret-Fragment-Visible Mosaic Images

[1]O.S.SumaPriya , [2]P.Suresh Babu

[1]M.Tech (DSCE), Dept of ECE, S.V.College of Engineering, Tirupati, os_sumi@yahoo.com

[2]Associate professor, Dept of ECE, S.V.College of Engineering, Tirupati, sureshbabu476@gmail.com

Abstract
A New secure picture transmission method is proposed, which changes naturally a given vast volume mystery picture into an alleged mystery section noticeable mosaic picture of the same size. The mosaic picture, which seems to be like a subjectively chosen target picture and may be utilized as a disguise of the mystery picture, is yielded by separating the mystery picture into parts and changing their shading qualities to be those of the relating squares of the target picture. Dexterous procedures are intended to direct the shading change prepare so that the mystery picture may be recuperated about losslessly. A plan of taking care of the floods/undercurrents in the changed over pixels' shading values by recording the shading contrasts in the untransformed shading space is likewise proposed. The data needed for recouping the mystery picture is implanted into the made mosaic picture by a lossless information concealing plan utilizing a key. Great exploratory results demonstrate the achievability of the proposed strategy.

***Index Terms*—Color transformation, data hiding, image encryption, mosaic image, secure image transmission**.

I.INTRODUCTION

Today, images from various sources are frequently utilized and transmitted through the internet for various applications, such as online personal photograph albums, confidential enterprise archives, document storage systems, medical imaging systems, and military image databases. These images usually contain private or confidential information so that they should be protected from leakages during transmissions. Nowadays, many methods have been proposed for securing image transmission, for which two common approaches are image encryption and data hiding. Encryption of an image is a procedure which use the natural properties of images, such as redundancy and spatial correlation, to get an image already encrypted which use the Shannon's confusion and diffusion properties. The image that is encrypted becomes an image with noise so that no one can obtain the transmitted secret image from it unless having the correct key. But, the encrypted image still is a meaningless document, which cannot give more information before the decryption is done. Thus, this may evoke an attacker's attention during the transmission of the image because of its arbitrary innature. Another possibility to avoid this problem is hiding of data that conceals a secret message into another image so that no one can anticipate the survival of the secret text, in which the type of data of the secret message that is examined in this paper is an image. The methods of data hiding already known mostly use the techniques such as LSB substitution, histogram shifting, recursive histogram modification, discrete cosine/wavelet transformations etc. However, in order to reduce the distortion of the resulting image, an upper bound for the distortion value is usually set on the payload of the cover image. Thus, the main limitation of the methods for data hiding in images is the difficulty in embedding a huge amount of message data into one image. Specifically, if one wants to hide a secret image into another image with the same size, the secret image must be highly compressed in advance. For example, for a data hiding method with an embedding rate of 0.5 bits per pixel, a secret image with 8 bits per pixel must be compressed at a rate of at least 93.75% beforehand in order to be hidden into a cover image. But, for many applications, such as keeping or transmitting medical pictures, military images, legal documents, etc., that are valuable with no allowance

ISSN 2347 - 3983

International Journal of Emerging Trends in Engineering Research (IJETER), Vol. 3 No.6, Pages : 243- 247 (2015)
Special Issue of NCTET 2K15 - Held on June 13, 2015 in SV College of Engineering, Tirupati
http://warse.org/IJETER/static/pdf/Issue/NCTET2015sp47.pdf

of serious distortions, such data compression operations are usually impractical. However, the techniques for compression of images, such as JPEG compression, are not appropriate for line drawings and graphical texts, in which sharp contrasts between neighbouring pixels are usually destroyed to become less noticeable. In this paper, a different method is proposed for the transmission of the image securely. This method transforms the secret image to be transmitted into a meaningful mosaic tile image with the same size which looks like another image which was preselected as the target image. The process of transformation is done with the help of some relevant information that is embedded and only with the help of this embedded information can a person losslessly recover the transmitted secret image from the mosaic tile image. This proposed method is magnified by Lai and Tsai where an aesthetic type of a new computer image, called mosaic tile image, was proposed. The mosaic tile image is the outcome of arranging of the tile fragments of a transmitted secret image is concealed in another image called the target image which was earlier selected from the database.

II. REVIEW OF LITERATURE:

This section describes the various existing schemes which are compared in this paper.

1) An Approach to Securely Transfer a Secret Image Using Reversible Color Transformations and HSV Color Model, In this paper, Ya-Lin Lee shows a technique for the transmission of the secret image securely and losslessly. This method transforms the secret image into a mosaic tile image having the same size like that of the target image which is preselcted from a database. This colour transformation is controlled and the secret image is recovered losslessly from the mosaic tile image with the help of the extracted relevant information generated for the recovery of the image.

2) Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption, In this paper, Kede Ma shows a method for data hiding into an image by reserving room before encryption of the image. This paper shows that first enough space is reserved in the image after which it is converted into encrypted form.

3) A Keyless Approach to Image Encryption, by Indian Institute of Technology Roorkee This paper shows a keyless approach to encryption methods which are used to encrypt images. We make the use of this paper to apply the keyless approach in the proposed method. This is done by generating relevant information with the help of some RMSE value which help to rotate the tile images to a certain angle.

4) JPEG: Still Image Data Compression Standard Here, W. B. Penne baker tries to explain that the main obstacle in many applications is the quantity of data required to represent a digital image. For this we would need an image compression standard to maintain the quality of the images after compression. To meet all the needs the JPEG standard for image compression includes two basic methods having different operation modes: A DCT method for “lossy” compression and a predictive method for “lossless” compression.

III. PROPOSED METHOD

The embedding of text into secret image by Data Hiding, the embedding of secret image into the target image in tile form and maintaining the visibility of the original target image. The proposed method includes

1) mosaic image creation and
2) secret image recovery.

Mosaic image creation block diagram

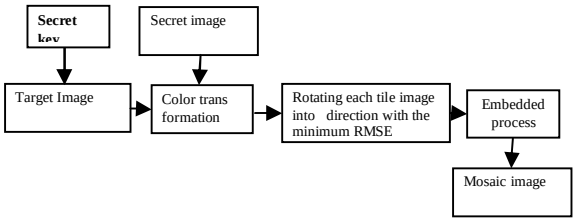

Figure1: Mosaic image creation block diagram

In the first phase, a mosaic image is yielded, which consists of the fragments of an input secret image with color corrections according to a similarity criterion based on color variations. The phase includes four stages: 1) fitting the tile images of the

ISSN 2347 - 3983

International Journal of Emerging Trends in Engineering Research (IJETER), Vol. 3 No.6, Pages : 243- 247 (2015)
Special Issue of NCTET 2K15 - Held on June 13, 2015 in SV College of Engineering, Tirupati
http://warse.org/IJETER/static/pdf/Issue/NCTET2015sp47.pdf

secret image into the target blocks of a preselected target image; 2) transforming the color characteristic of each tile image in the secret image to become that of the corresponding target block in the target image; 3) rotating each tile image into a direction with the minimum RMSE value with respect to its corresponding target block; and 4) embedding relevant information into the created mosaic image for future recovery of the secret image.

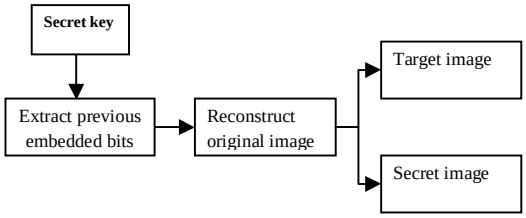

Figure: 2 Extract secret image and target image Block diagram

In the second phase, the embedded information is extracted to recover nearly loss lessly the secret image from the generated mosaic image. The phase includes two stages: 1) extracting the embedded information for secret image recovery from the mosaic image, and 2) recovering the secret image using the extracted information.

IV.ALGORITHM OF PROPOSED SYSTEM

Mosaic image creation algorithm

- Input: a secret image S, a target image T, and a secret key K.
- Output: a secret-fragment-visible mosaic image F.
- Stage 1: fitting the tile images into the target blocks.
- Stage 2: performing color conversions between the tile images and the target blocks.
- Stage 3: rotating the tile images.
- Stage 4: embedding the secret image recovery information.

Secret image recovery algorithm

- Input: a mosaic image F with n tile images {T1, T2, . . . , Tn} and the secret key K.
- Output: the secret image S.
- Stage 1: extracting the secret image recovery information.
- Stage 2: recovering the secret image.

V. EXPERIMENTAL RESULTS

As show the experiments have been conducted to test the proposed method using many secret and target images with sizes 1024×768 or 768×1024. 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. An example of the experimental results is shown in Fig. 3; Fig. 3(c) shows the created mosaic image using Fig. 3(a) as the secret image and Fig. 3(b) as the target image. The tile image size is 8×8. The recovered secret image using a correct key is shown in Fig. 3(d) which looks nearly identical to the original secret image shown in Fig. 3(a) with RMSE= 0.948 with respect to the secret image. It is noted by the way that all the other experimental results shown in this paper have small RMSE values.Moreover, Fig. 3(e) shows the recovered secret image using a wrong key, which is a noise image. Fig. 3(f)–(i) show more results using different tile image sizes. It can be seen from the figures that the created mosaic image retains more details of the target image when the tile image is smaller. It can also be seen that the blockiness effect is observable when the image is magnified to be large; but if the image is observed as a whole, it still looks like a mosaic image with its appearance similar to the target image.

ISSN 2347 - 3983

International Journal of Emerging Trends in Engineering Research (IJETER), Vol. 3 No.6, Pages : 243- 247 (2015)
Special Issue of NCTET 2K15 - Held on June 13, 2015 in SV College of Engineering, Tirupati
http://warse.org/IJETER/static/pdf/Issue/NCTET2015sp47.pdf

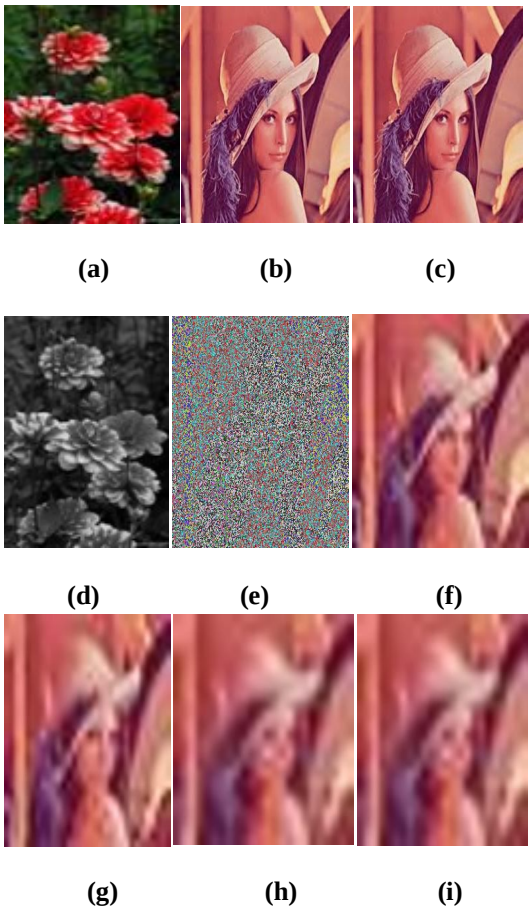

Fig. 3. Experimental result of mosaic image creation. (a) Secret image. (b) Target image. (c) Mosaic image created with tile image size.(d) Recovered secret image using a correct key with RMSE= 0.948 withrespect to secret image (a). (e) Recovered secret image using a wrong key.(f)-(i) Mosaic images created with different tile image sizes: 16×16, 24×24, 32×32, and 40×40.

Fig. 4 shows a comparison of the results yielded by the proposed method with those by Lai and Tsai [21], in which Fig. 4(a) is the input secret image, Fig. 4(b) is the selected target image, Fig. 4(c) is the mosaic image created by Lai and Tsai [21], and Fig. 4(d) is that created by the proposed method. It can be seen from these results that the mosaic image yielded by the proposed method has a smaller RMSE value with respect to the target image, implying that it is more similar to the target image in appearance. The other results of our experiments also show the same conclusion, and more importantly, the proposed method allows users to select their favorite images.

Fig. 4. Comparison of results of [13] and proposed method.(a) Secret image. (b) Target image. (c) Mosaic image created from (a) and (b) by [13] with RMSE= 47.651. (d) Mosaic image created from (a) and (b) by proposed method with RMSE= 33.935.

VI. CONCLUSION

A new secure image transmission method has been proposed, which not only can create meaningful mosaic images but also can transform a secret image into a mosaic one with the same data size for use as a camouflage of the secret image. By the use of proper pixel color transformations as well as a skillful scheme for handling overflows and underflows in the converted values of the pixels' colors, secret-fragment visible mosaic images with very high visual similarities to arbitrarily-selected target images can be created with no need of a target image database. Also, the original secret images can be recovered nearly losslessly from the created

ISSN 2347 - 3983

International Journal of Emerging Trends in Engineering Research (IJETER), Vol. 3 No.6, Pages : 243- 247 (2015)
Special Issue of NCTET 2K15 - Held on June 13, 2015 in SV College of Engineering, Tirupati
http://warse.org/IJETER/static/pdf/Issue/NCTET2015sp47.pdf

mosaic images. Good experimental results have shown the feasibility of the proposed method. Future studies may be directed to applying the proposed method to images of color models other than the RGB.

VII. REFERENCES

[1] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *Int. J. Bifurcat. Chaos*, vol. 8, no. 6, pp. 1259–1284, 1998.

[2] G. Chen,Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos Solit. Fract.*, vol. 21, no. 3, pp. 749–761, 2004.

[3] L. H. Zhang, X. F. Liao, and X. B. Wang, "An image encryption approach based on chaotic maps," *Chaos Solit. Fract.*, vol. 24, no. 3, pp. 759–765, 2005.

[4] H. S. Kwok and W. K. S. Tang, "A fast image encryption system based on chaotic maps with finite precision representation," *Chaos Solit. Fract.*, vol. 32, no. 4, pp. 1518–1529, 2007.

[5] S. Behnia, A. Akhshani, H. Mahmodi, and A. Akhavan, "A novel algorithm for image encryption based on mixture of chaotic maps," *Chaos Solit. Fract.*, vol. 35, no. 2, pp. 408–419, 2008.

[6] D. Xiao, X. Liao, and P. Wei, "Analysis and improvement of a chaosbased image encryption algorithm," *Chaos Solit. Fract.*, vol. 40, no. 5, pp. 2191–2199, 2009.

[7] V. Patidar, N. K. Pareek, G. Purohit, and K. K. Sud, "A robust and secure chaotic standard map based pseudorandom permutationsubstitution scheme for image encryption," *Opt. Commun.*, vol. 284, no. 19, pp. 4331–4339, 2011.

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

[9] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 16, no. 3, pp. 354–362, Mar. 2006.

[10] J. Tian, "Reversible data embedding using a difference expansion," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 890–896, Aug. 2003.

11] X. Hu, W. Zhang, X. Hu, N. Yu, X. Zhao, and F. Li, "Fast estimation of optimal marked-signal distribution for reversible data hiding," *IEEE Trans. Inf. Forens. Secur.*, vol. 8, no. 5, pp. 187–193, May 2013.

[12] W. B. Pennebaker and J. L. Mitchell, *JPEG: Still Image Data Compression Standard*. New York, NY, USA: Van Nostrand Reinhold, 1993, pp. 34–38.

[13] I. J. 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.

[14] E. Reinhard, M. Ashikhmin, B. Gooch, and P. Shirley, "Color transfer between images," *IEEE Comput. Graph. Appl.*, vol. 21, no. 5, pp. 34–41,Sep.–Oct. 2001.