ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Dynamic transformation of huge volume Secret images into Mosaic Images

SaiVinay
MTech Student
Department of ECE
KBR Engineering College

A.BhanuChandar, MTech
Guide
Department of ECE
KBR Engineering College

***Abstract:**In computer science, secure transmission refers to the transfer of data such as confidential or proprietary information over a secure channel. Many infrastructures such as hospital &banks rely on secure transmission protocols to prevent a catastrophic breach of security. Secure transmissions are put in place to prevent attacks such as ARP spoofing and general data loss. Images from various sources are often used and are transmitted through the internet for various purposes, such as confidential enterprise archives, document storage systems, medical imaging systems, and military image databases. These images may contain secret or confidential information since it should be protected from leakage during transmissions. An approach for secure image transmission is needed, which is to transform a secret image into a meaningful Secret Fragment Mosaic image with size almost same and looking similar to the preselected target image. The mosaic image is the outcome of arranging of the block fragments of a secret image in a way so as to disguise the other image called the target image. The mosaic image, which looks similar to a randomly selected target image, which is used for hiding of the secret image by color transforming their characteristics similar to the blocks of the target image. Such technique is necessary so for the lossless recovery of the transmitted secret image. The appropriate information is embedded into the mosaic image for the recovery of the transmitted secret image.*

***Keywords:** Secure Transmission, Image conversion, Color transformation, data hiding, encryption of image, mosaic image, reversible data hiding.*

Introduction:

The Internet continues to grow, driven by ever greater amounts of online information and knowledge, commerce, entertainment and social networking. During the late 1990s, it was estimated that traffic on the public Internet grew by 100 percent per year, while the mean annual growth in the number of Internet users was thought to be between 20% and 50%. As of 31 March 2011, the estimated total number of Internet users was 2.095 billion (30.2% of world population). File sharing is an example of transferring large amounts of data across the Internet. A computer file can be emailed to customers, colleagues and friends as an attachment. It can be uploaded to a website or File Transfer Protocol (FTP) server for easy download by others. It can be put into a "shared location" or onto a file server for instant use by colleagues. The load of bulk downloads to many users can be eased by the use of "mirror" servers or peer-to-peer networks. Digital media streaming increases the demand for network bandwidth. For example, standard image quality needs 1 Mbit/s link speed for SD 480p, HD 720p quality requires 2.5 Mbit/s, and the top-of-the-line HDX quality needs 4.5 Mbit/s for 1080p.

Nowadays, images from various sources are often used and are transmitted through the internet for various applications, such as 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. Recently, many methods have been proposed for securing image transmission, for which two common approaches are image encryption and data hiding.

Encryption of image is a technique that make use of the natural property of an image, such as high redundancy and strong spatial correlation, to get an encrypted image. The encrypted image is meaningless and this may arouse the third parties attention due to its randomness in form during transmission. Another method for secure image transmission is data hiding that hides a secret entity into a cover image so that a third party cannot found the presence of the secret entity. The problem of data hiding is the difficulty in embedding large volume of secret entity into a single image. If anyone wants to hide a secret entity into a cover image, the secret entity must be highly compressed earlier. During retrieval this will cause distortion of the secret entity. In this paper, we propose an approach for secure image transmission is needed, which is to transform a secret image into a meaningful Secret Fragment Mosaic image with size almost same and looking similar to the preselected target image. The mosaic image is the outcome of arranging of the block fragments of a secret image in a way so as to disguise the other image called the target image. The mosaic image, which looks similar to a randomly selected target image, which is used for hiding of the secret image by color transforming their characteristics similar to the blocks of the target image. Such technique is necessary so for the lossless recovery of the transmitted secret image. The appropriate information is embedded into the mosaic image for the recovery of the transmitted secret image.

Related Work:

A New Secure Image Transmission Technique via Secret-fragment-Visible Mosaic Images by Nearly Reversible Colour 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 colour 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].

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 [2].

JPEG: Still Image Data Compression Standard

Here, W. B. Pennebaker 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 [3].

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.

Existing System:

Existing work on secure image transmission involved techniques, such as, image encryption, data hiding, and JPEG compression. Image encryption which only creates meaningless noise image and encrypts the image using a secret key, does not provide additional information before decryption and may arouse attacker’s attention during transmission. In order to avoid this problem, data hiding technique was used, that hides the secret message into a cover image in order to hide the existence of secret data. The main issue here was to hide a large amount of data into secret image. Also, when the secret and cover image were of the same size, the secret image was highly compressed in advance, which affected the quality of image. Different techniques used in data hiding methods were LSB substitution, histogram shifting, difference expansion, prediction-error expansion, recursive histogram modification, and discrete cosine/wavelet transformations. Image compression methods were also used, such as JPEG compression, which was not meant for line drawings and textual graphics, in which the sharp contrasts between adjacent pixels are often destructed to become noticeable artifacts.

Proposed System:

To securely transmit a secret image and recovering it without any loss by method of creating a mosaic image. The proposed method is new in that a meaningful mosaic image is created.

The proposed method includes two main phases

1) Mosaic image creation

2) Secret image recovery

The result is the mosaic image, which consists of block fragments of an input secret image which has color characteristics same as that of a preselected target image.

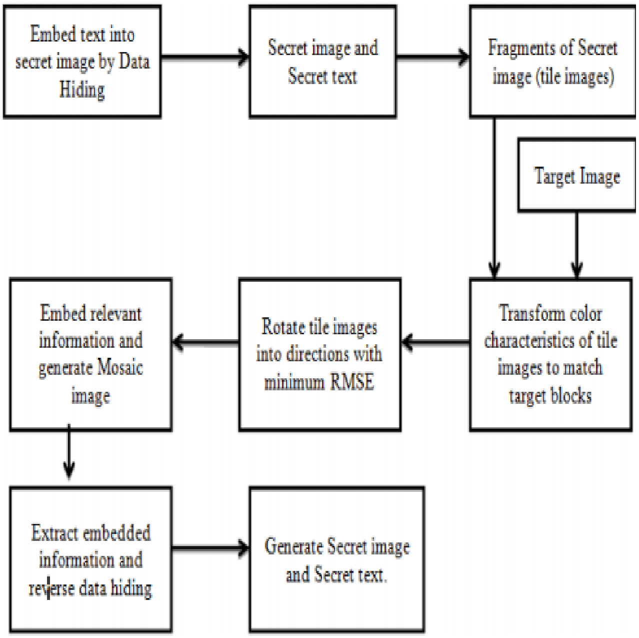

Embed text into secret image by Data Hiding
Secret image and Secret text
Fragments of Secret image (tile images)
Target Image
Transform color characteristics of tile images to match target blocks
Rotate tile images into directions with minimum RMSE
Embed relevant information and generate Mosaic image
Extract embedded information and reverse data hiding
Generate Secret image and Secret text.

Fig: Flow Diagram

In the first phase, mosaic image is created, which consists of the fragments of an input secret image having color corrections according to a similarity criterion based upon color variations. The phase consists of four stages:

1) fit the tile images of the secret image into the target blocks of a preselected target image;

2) Transform the color characteristic of each tile image in the secret image to become that of the corresponding target block in the target image;

3)Rotate each tile image into a direction with the minimum RMSE value with respect to its corresponding target block; and

4)Embed relevant information for future recovery of the secret image into the created mosaic image.

In the second phase, the embedded information is extracted to recover nearly losslessly the secret image from the generated mosaic image. This phase includes two stages:

1)Extract the embedded information for secret image recovery from the mosaic image, and

2)Recover the secret image using the extracted information.

Algorithm1 for mosaic image creation

Input: S->secret image , T->target image , and k->secret key . Output: F->secret-fragment-visible mosaic image . Steps:

Stage 1. Fit the tile images into the target blocks.

Step 1-If the size of the selected target image T is different from the secret image S then change the size of T so that it is identical to the S; and divide the secret image S into n fragments called as tile images {T1, T2,.., Tn} as well as the target image T into n target blocks {B1, B2,.., Bn} with each Ti or Bi being of size NT. Step 2- Calculate the means and the standard deviations of each tile image from T1 to Tn and each target block Bj for the three color channels; and compute the average standard deviations for Ti and Bj, respectively, for i = 1 to n and j = 1 to n. Step 3-Sort the tile images in the set Stile={T1,T2,...,Tn} and the target blocks in the set Starget = {B1,B2,.., Bn} according to the computed average standard deviation values of the blocks; map in order the blocks in the sorted Stile to those in the sorted Starget in a 1-to-1 manner; and according to the indices of the tile images reorder the mappings which resulted in a mapping sequence L of the form: T1→Bj1,T2→ Bj2,..., Tn→Bjn.Step 4- by fitting the tile images into the respective target blocks create a mosaic image F according to L.

Stage 2. Perform color conversions between tile images and target blocks

Step 5-Create a counting table TB having 256 entries, so that each index corresponding to a residual value, and assign an initial value of zero to each entry (noteeach residual value should be in the range of 0 to 255). Step 6-Represent the means μc and μ'c of Ti and Bji, for each mapping Ti→Bji in sequence L, respectively, by eight bits; and represent the standard deviation quotient qc by seven bits, where c = r, g, or b. Step 7- For each pixel pi of each tile image Ti in mosaic image F having color value ci where c = r, g, or b, transform ci into a new value c‖i; if c‖i is greater than 255 or if it is smaller than 0, then change c‖i to be 255 or 0, respectively; compute a residual value Ri for pixel pi and increment the count by 1 in the counting table TB whose index is identical to Ri.

Stage 3. Rotate the tile images.

Step 8-Calculate the RMSE values of each color transformed tile image Ti in mosaic image F with respect to its corresponding target block Bji after rotating Ti into each of the directions θ =0°,90°,180° and 270°; and rotate Ti into the optimal direction θ with the smallest RMSE value.

Stage 4. Embed the secret image recovery information.

Step 9-using the content of the counting table TB Construct a Huffman table HT to encode all the residual values computed previously. Step 10-For each tile image Ti in mosaic image F, construct a bit stream Mi for recovering Ti including the bit-segments which encode the data items of: 1.the index of the corresponding target block Bji; 2. the optimal rotation angle θ° of Ti; 3.the means of Ti and Bji and the related standard deviation quotients of all three color channels; and 4.the bit sequence for overflows/underflows with residuals in Ti encoded by the Huffman table HT constructed in Step 9. Step 11-To form total bit stream Mt, Concatenate the bit streams Mi of all Ti in F in a raster-scan order; encrypt Mt using the secret key K so as to obtain another bit stream M't; and by using reversible contrast mapping scheme proposed embedM't into F . Step 12-Construct a bit stream I including: 1.the number of conducted iterations Ni for embedding M't; 2.the number of pixel pairs Npair used in the last iteration; and 3.the Huffman table HT constructed for the residuals; and embed the bit stream I into mosaic image F by the same scheme used in Step 11.

Algorithm 2 Secret image recovery

Input: a mosaic image F with n tile images{T1, T2,Tn} and the secret key K. Output: secret image S. Steps:

Stage1. Extract the secret image recovery information.

Step 1-Extract the bit stream I from F by a reverse version of the scheme proposed and decode them to obtain the following data items: 1) the number of iterations Ni for embedding M't; 2) the total number of used pixel pairs Npair in the last iteration; and 3) the Huffman table HT for encoding the values of the residuals of the overflows or underflows. Step 2-Using the values of Ni and Npair extract the bit stream M't by the same scheme used in the last step. Step 3-Decrypt the bit stream M't into Mt by K. Step 4-Decompose Mt into n bit streams M1 to Mn for the n to-be-constructed tile images T1 through Tn in S, respectively. Step 5-Decode Mi for each tile image Ti so as to obtain the following data items: 1) the index ji of the block Bji in F corresponding to Ti; 2) the optimal rotation angle θ° of Ti; 3) the means of Ti and Bji and the related standard deviation quotients of all color channels; and 4) the overflow/underflow residual values in Ti decoded by the Huffman table HT.

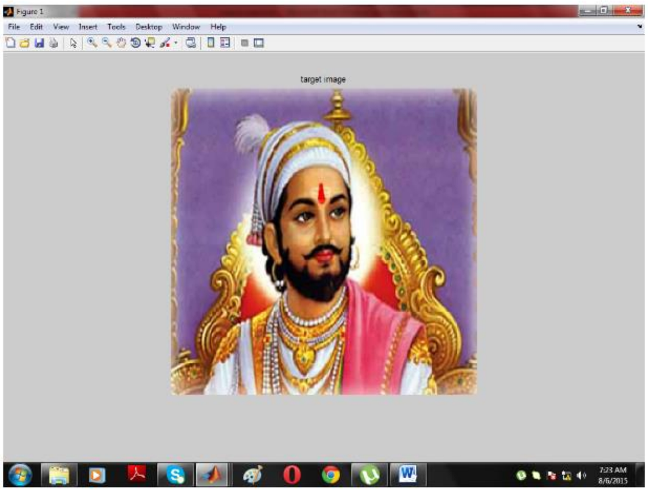
Stage 2. Recover the secret image.

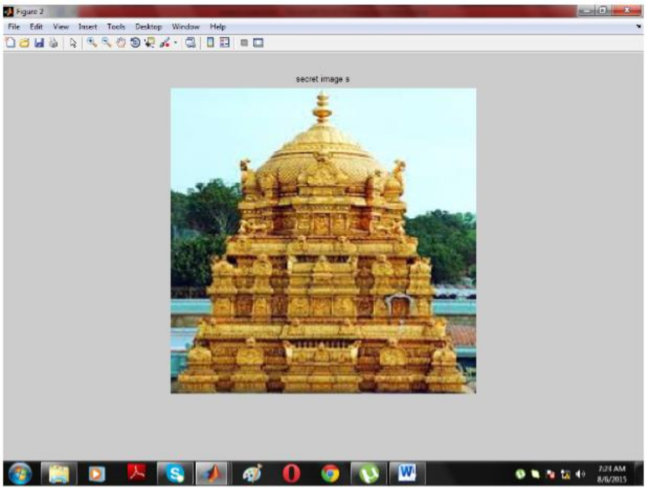
Step 6-Recover one by one in a raster-scan order the tile images Ti, i = 1 to n, of the desired secret image S

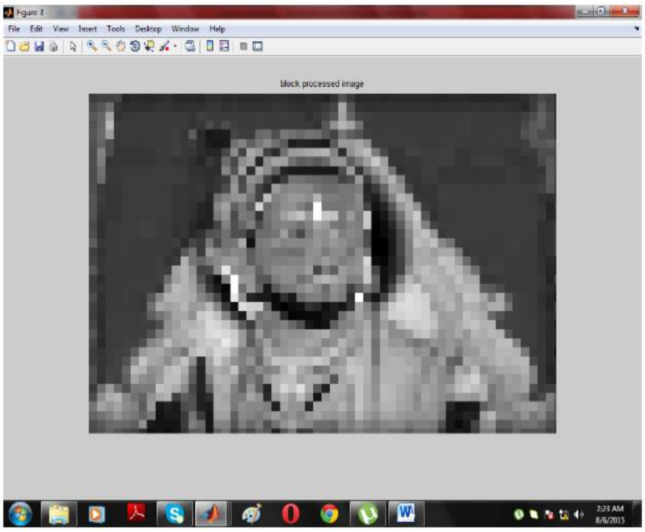
ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

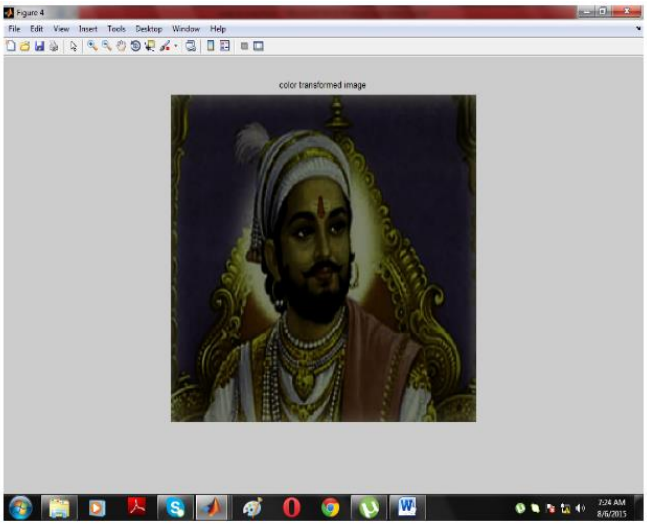
by the following steps: 1.rotate in the reverse direction the block indexed by ji, namely Bji, in F through the optimal angle θ° and fit the resulting block content into Ti to form an initial tile image Ti; 2.use the extracted means and related standard deviation quotients to recover the original pixel values in Ti; 3.use the Extracted means, standard deviation quotients to compute the two parameters cS and cL; 4.scan Ti to find out pixels with values 255 or 0 which indicate whether the overflows or underflows, respectively, has been occurred there; 5.add respectively the values cS or cL to the corresponding residual values of the found pixels; and 6.take the obtained results as the final pixel values, which is getting resulting in a final tile image Ti. Step 7-Compose all the final tile images so as to get the desired secret image S as output.

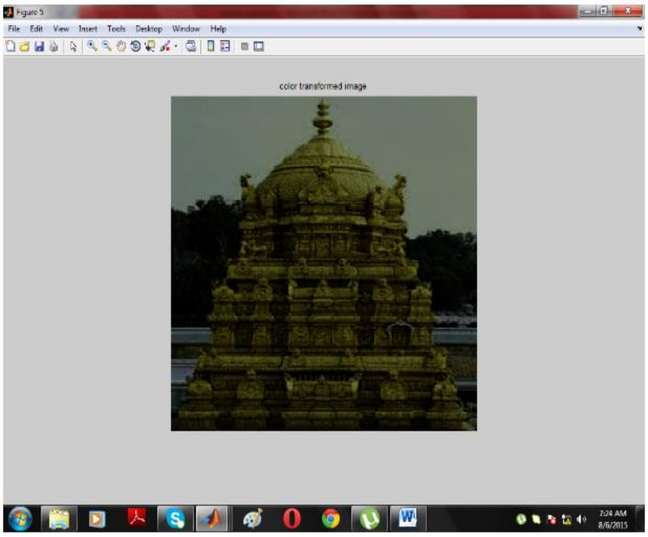
Screenshots:

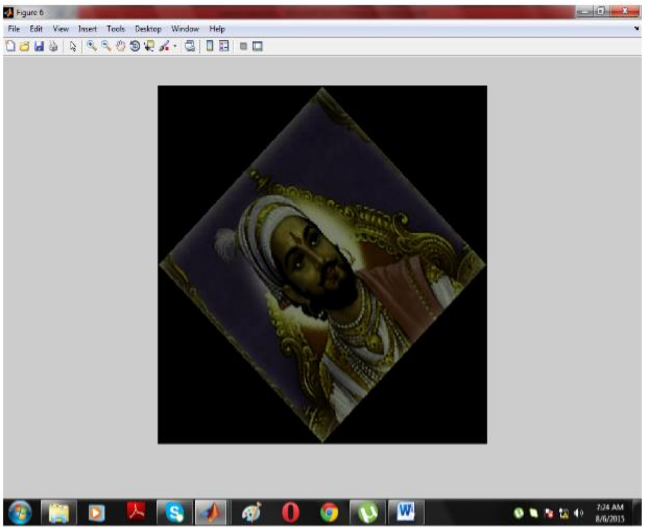


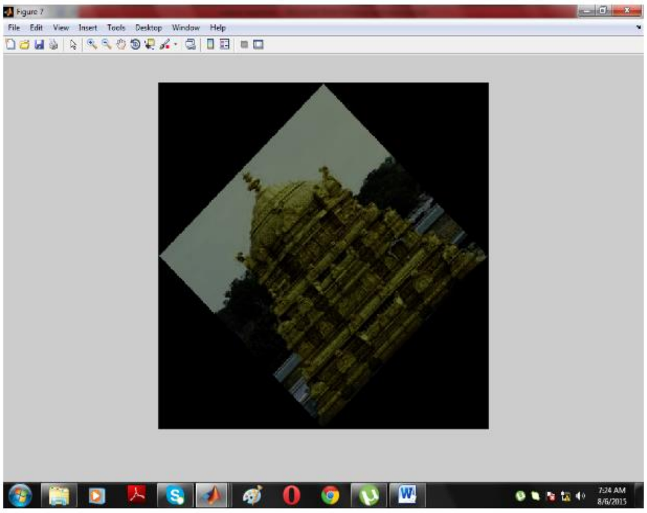


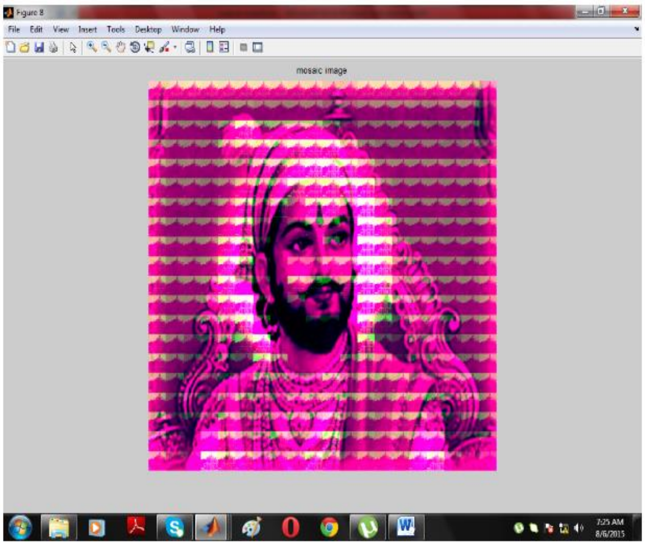


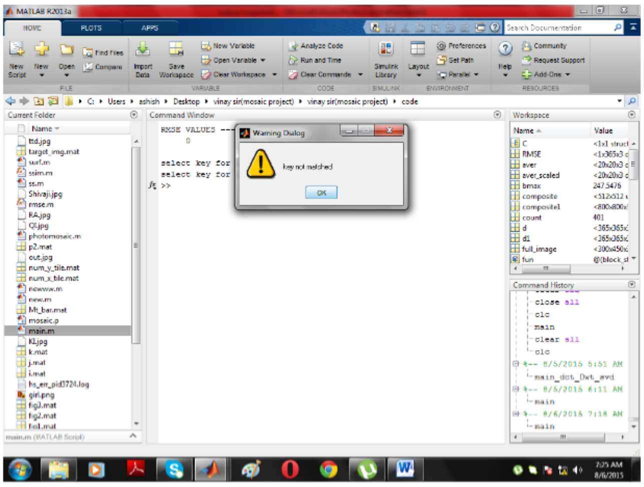












```
RMSE VALUES ---
      0

select key for
select key for
>>
```

Warning Dialog

key not matched

OK

Conclusion:

Images from different sources are transmitted through the internet for various applications. These images usually contain private or secret data so that they should be protected from leakages during transmissions. A method is proposed to securely transmit a secret image that create mosaic images which also can transform a secret image into a mosaic tile image with the same size of data for concealing the secret image. This is done by the use of proper color transformations pixel by pixel in mosaic tile images with large color similarities. The original secret image can be reconstructed nearly lossless from the created mosaic images.

References:

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

[2] A Keyless Approach to Image Encryption, Siddharth Malik, Anjali. Sardana Indian Institute of Technology Roorkee, India. 2012 International Conference on communication Systems.

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

[4] 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.

[5] 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.

[6] D. Xiao, X. Liao, and P. Wei, “Analysis andimprovement of a chaosbasedimageencryptionalgorithm,” Chaos Solit. Fract., vol. 40, no. 5,pp. 2191–2199, 2009.

[7] V. Patidar, N. K. Pareek, G. Purohit, and K. K. Sud, “A robustand secure chaotic standard map based pseudorandom permutationsubstitutionscheme for image encryption,” Opt. Commun., vol. 284, no. 19, pp. 4331– 4339, 2011

[8] J. Tian, “Reversible data embedding using a difference expansion,” IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug2003.

[9] D. Coltuc and J.-M. Chassery, “Very fast watermarking by re- versible contrast mapping,” IEEE Signal Process. Lett., vol. 14, no. 4, pp. 255–258,Apr.2007.

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