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

Priyanka V.Patil, Dr. A.M. Patil

Abstract: A latest secure image transmission technique is proposed, which transforms automatically a given large-volume secret image into a so-called secret-fragment-visible mosaic image of the similar size. The mosaic image, which looks related to an arbitrarily selected target image as well as may be used as a camouflage of the secret image, is yielded by separating the secret image into fragments plus transforming their colour characteristics to be those of the corresponding blocks of the target image. Skilled techniques are planned to conduct the colour transformation development so that the secret image may be recovered almost losslessly. A plan of handling the overflows/underflows in the converted pixels' colour values via recording the colour differences in the untransformed colour space is too proposed. The information essential for recovering the secret image is embedded into the formed mosaic image through a lossless data hiding scheme by a key. Good quality experimental results illustrate the feasibility of the proposed method.

Key words- Color transformation, data hiding, image encryption, mosaic image, secure image transmission.

1. INTRODUCTION

In recent times, images from a variety of sources are sent and received over the internet for various applications, such as online classified enterprise archives, document storages, medical image databases, and military imaging systems. The images typically contain confidential information i.e they should be protected from leakages and attacks during transmissions. Various methods have been planned for secure image transmission, in which there are two common approaches- image encryption plus data hiding. Image encryption is a method in which the natural property of an image like high redundancy and strong spatial correlation, to obtain an image encrypted based on Shannon's confusion and diffusion properties [1]–[7] are used.

The resultant image is presently a noiseful file so as to no one can understand or obtain the secret image from it unless has the accurate key. But, the encrypted image is a worthless, noiseful image, which is totally unusable before decryption along with may arouse an attacker's attention during transmission because of its randomness and chaotic form.

Manuscript received Jan 04, 2017.

Priyanka V. Patil, *Master Student, Dept of EXTC, J.T.Mahajan, College of Enginnering, Faizpur ,(email id:patilpriya2913@gmail.com)*

Dr. A. M. Patil, *Professor and HOD, Dept of EXTC J.T.Mahajan,College of Enginnering,Faizpur*

An extra aspect of information security data hiding [8] to hides a secret image into a cover image so that it is hard to realize the subsistence of the secret data**.** Existing methods generally make utilize of the techniques of LSB substitution [8], histogram shifting, prediction-error extension, difference expansion, recursive histogram modification, and discrete cosine/wavelet transformations. A major disadvantage of the methods used for data hiding is that there is difficulty in embedding a great amount of message into a single image. Also, if one needs to hide a secret image into a cover image with the similar size, the image must be extremely compressed before custom. However, for many applications, such as transmission of medical pictures, legal documents, military images, etc., those are valuable with no possiblity of serious distortions, such as data compression operations are typically impractical. In this paper, a innovative method for secure image transmission during videos is proposed, which transforms a secret image into a significant mosaic image with the similar size moreover which looks like a preselected target image of the accessible video frames. The development is forced by a secret key for security. This key has to be used by the person in command to recover the secret image lossless since the video otherwise called as target image. The existing scheme is quoted by Lai and Tsai, in which a called secret-fragment-visible mosaic image was proposed. It is the result of rearrangement of the fragments of a secret image in disguise of another image called the target image which is selected priory from a database. The drawback of Lai and Tsai is that it requires a large image database so that the formed mosaic image appropriately resembles the particular target image. In this, the user is not authorized to select freely his/her favourite image for use as the target image. Hence, to remove this weakness of the above method while retaining its advantage, this is aimed to develop a new method that can transform a secret image into a same sized secret fragment-

Figure 1 Result yielded by the proposed method.(a)Secret image.(b)Target image.(c)Secret-fragment-visible mosaic image created from(a)and(b)by the proposed method

Above Fig. 1 shows a effect obtained by the planned scheme. Behind a target image is selected arbitrarily, the given secret image is first divided into rectangular fragments called tile images, which are next fit into analogous blocks in the target image, they are called as target blocks, according to the similarity principle based on color variations. Then color feature of each tile image is transformed according to the particular target block in the target image, which results into a mosaic image looks like the target image. Similar methods are also proposed to take out nearly lossless recovery of the unique secret image from the resulting mosaic image. In the planned technique, in contrast with the image encryption process, a meaningful mosaic image is formed. Also, the proposed method able to transform a secret image into a disguising mosaic image with no compression, as a data hiding scheme hide a highly compressed version of the secret image into a cover image while the secret image as well as the cover image having the same data volume.

II. REVIEW OF LITERATURE

The images which actually enclose private data must be protected from leakages during transmissions for that many methods have been proposed for securing image transmission. Up to now whatever the existing system are and work related to this technique is explained below: Ya-Lin Lee[9], shows a technique for the transmission of the secret image securely and losslessly. This system transforms the secret image into a mosaic tile image having the similar size like that of the target image which is preselected from a database. This color transformation is controlled with 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. The secret image transforms automatically into a so-called secret-fragment visible mosaic image of the similar size. The mosaic image, is used as a camouflage of the secret image, and is yielded by separating the secret image into fragments with transforming their color characteristics to be those of the corresponding blocks of the target image. Kede Ma[10] shows a method for data hiding into an image by reserving room previous to encryption of the image. In this paper shown that first enough space is reserved in the image after which it is converted into encrypted form. Siddharth Malik, Anjali [11] proposed a keyless approach to encryption method is used to encrypt images. Authors make the use of the paper to apply the keyless approach in the planned technique. This is done by generating appropriate information with the help out of some RMSE value which help to rotate the tile images to a certain angle. I. J. Lai and Tsai [9], proposed a new type of computer art image called secret-fragment-visible mosaic image is planned which is formed automatically by arranging small fragments of a known image in a mosaic form, along with it embedding given secret image in the resulting mosaic image. This kind of information hiding is helpful for covert communication with secure keeping of secret images. W. B. Pennebaker [12] tries to explain that the main obstacle in many applications is the quantity of data necessary to signify a digital image. For this we would need an image compression criterion to uphold the quality of the images behind compression [13]. To meet all the wants the JPEG standard for image compression includes two basic methods having dissimilar operation modes: A DCT method for ―lossy compression as well as a predictive method for ―lossless‖ compression.

A innovative technique for secure image transmission is proposed, which transforms a secret image into a meaningful mosaic image with the same size and looking like a preselected target image. The transformation procedure is controlled with a secret key, and just with the key can a person recover the secret image almost losslessly from the mosaic image. The planned method is stimulated by Lai and Tsai [9], in which a novel type of computer art image, called secret-fragment-visible mosaic image, was proposed. The mosaic image is the effect of rearrangement of the fragments [14][15] of a secret image in disguise of an additional image called the target image preselected as of a database[16]. But a noticeable weakness of Lai and Tsai [9] is the condition of a large image database so that the generated mosaic image can be adequately alike to the selected target image. Using their method, the user is not approved to select freely his/her favourite image used for use as the target image. It is therefore desired in this study to remove this weakness of the method [17][18] while keeping its merit, that is, it is aimed to plan a original scheme that can transform a secret image into a secret fragment- visible mosaic image of the similar size that has the visual appearance of any freely selected target image without the need of a database[16].

III. PROPOSED WORK

The embedding of manuscript into secret image by Data Hiding [19][20][21], the embedding of secret image into the target image in tile form as well as maintaining the visibility of the unique target image. The proposed technique includes

1) Mosaic image creation
2) Secret image recovery.

Mosaic image formation block diagram

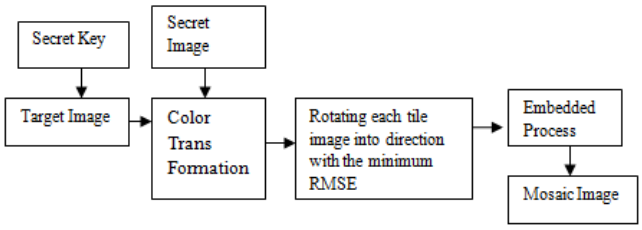


Figure 2 Mosaic image creation block diagram

In the initial phase, a mosaic image is yielded, which consists of the fragments of an input secret image by color corrections according to a similarity measure based on color variations. The phase include four stages: 1) fitting the tile images of the secret image interested in the target blocks of a preselected target image; 2) transforming the color characteristic of each one tile image in the secret image to become that of the equivalent target block in the target image; 3) rotating each tile image into a direction with the lowest RMSE value with respect to its corresponding target block; and 4) embedding relevant information into the produced mosaic image for future recovery of the secret image.

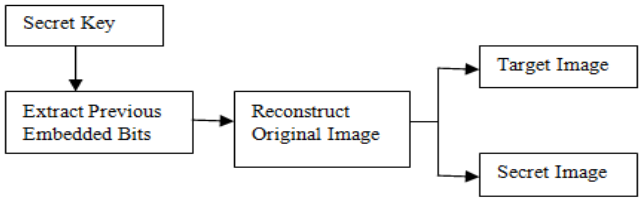


Figure 3 Extract secret image and target image Block diagram

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

IV.ALGORITHM OF PROPOSED SYSTEM

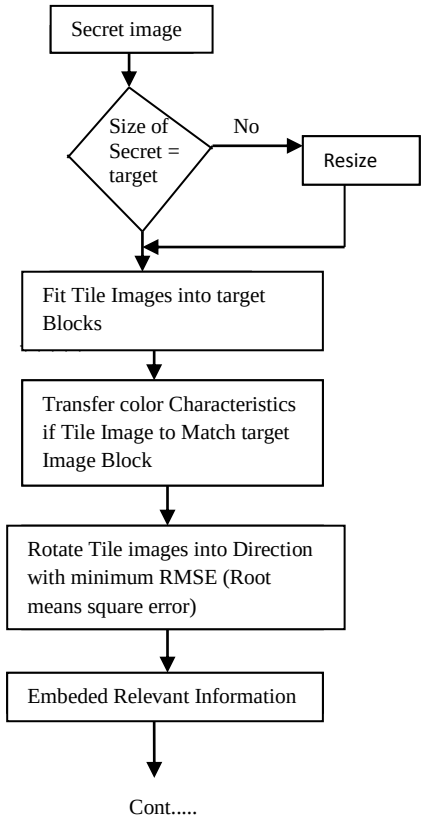
Mosaic image creation algorithm

- 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 in between the tile images as well as the target blocks.
- Stage 3: turning the tile images.
- Stage 4: embedding the secret image recovery information.

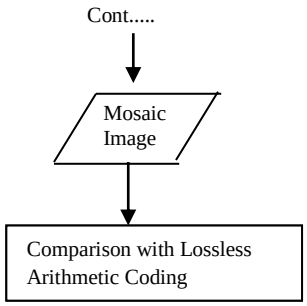
Secret image recovery algorithm

- 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.

Sender Side



Cont.....



Receiver Side

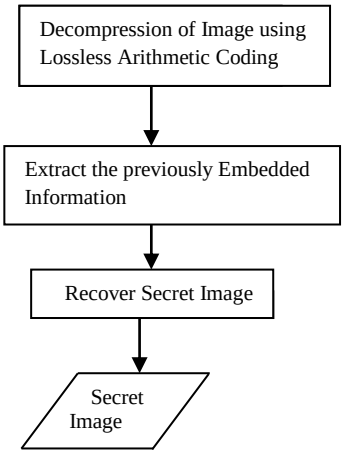


Figure 4: Flow chart of proposed algorithm

The detailed algorithms for mosaic image formation as well as secret image recovery may now be described in Algorithms 1 along with Algorithms 2 respectively.

Stage 1. Fitting blocks of secret images into the blocks of target blocks

1. If the size of T is dissimilar from S, change the size
2. Divide S and T into n blocks of same size
3. Compute the means and the standard deviations(SD) of each tile [1]
4. Calculate the average SD
5. Sort the tile images in S and T
6. Map tile between S and T
7. Create F

Stage 2. Transforming color characteristics of blocks of secret image analogous to target image

8. For each mapping from secret to target analyse the mean and SD
9. Each pi in every block of F with color value ci, transform ci into a new value [10] by ci''=qc (ci-μc) + μc'

a. If ci'' is not less than 255 or if it is not greater than0, then next change to be 255 or 0.

Stage 3. Rotating secret image blocks in the direction through minimum RMSE value

10. Compute the RMSE values
11. Rotate tile into the optimal direction with the smallest RMSE value

Stage 4. Embed information for recovery intention
12. For each tile image in F, create a bit stream M for recovering T
- Index, rotation angle θ°, means with the SD quotients

13. Create a bit stream Mt by K
14. Embed Mt into F

Algorithm 2 Secret image recovery
T-target image, S-secret image, F-mosaic image.

Stage 1. Extracting the embedded information.
1. Extract the bit stream Mt by K
2. Decompose Mt into n bit streams
3. Decode M for each tile image to obtain the data items
- Index, rotation angle θ°, means with SD quotients

Stage 2. Recovering the secret image.
4.Improve tile images with the following steps
- Rotate tile in the reverse direction as well as fit the resulting block content into T to form an initial tile image
- make use of the extracted means with related SD quotients
- calculate the original pixel value
- scan T to find out pixels by values 255 or 0
- obtain the results as the final pixel values

5. Create all the final tile images to form the required secret image S.

IV. EXPERMINETAL RESULTS

As illustrate the experiments has been conduct to test the proposed scheme by many secret as well as target images with sizes 1024×768 or 768×1024. To show that the formed mosaic image looks approximating the preselected target image[22], the quality metric of root mean square error (RMSE) is utilized, which is definite as the square root of the mean square difference between the pixel values[23] of the two images. The pattern of the experimental results is shown in Fig. 5; Fig. 5(c) shows the created mosaic image using Fig. 5(a) as the secret image and Fig. 5(b) as the target image. The tile image size is 8×8. The recovered secret image using a correct key is shown in Fig. 5(d) which looks practically alike to the creative secret image shown in Fig. 5(a) with RMSE= 0.948 with respect to the secret image. It is illustrious by the way that all the previous experimental results shown in this paper have small RMSE values. Furthermore, Fig. 5(e) shows the improved secret image by a wrong key, which is a noise image. Fig. 5(f)–(i) show additional results by dissimilar tile image sizes. It can be seen from the figures that the formed mosaic image retains added details of the target image when the tile image is lesser. It can also be seen that the blackness result is observable when the image is overstated to be large; but if the image is observed as a whole, it still looks similar to a mosaic image with its appearance similar to the target image.

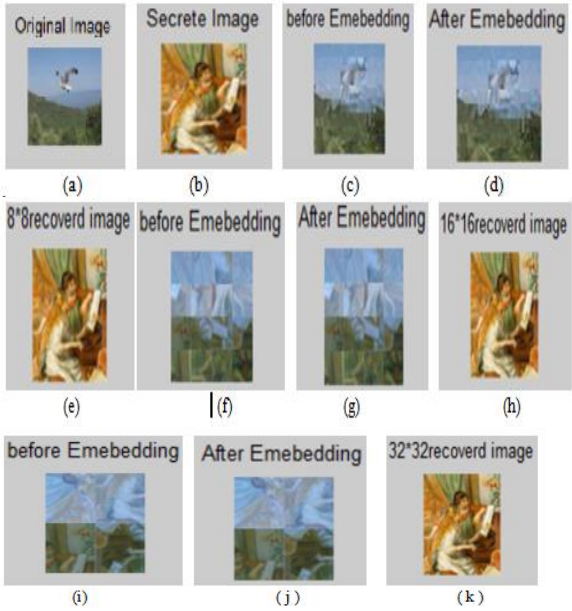


Figure 5. Comparison of results of Lai and Tsai [5] and proposed method. (a) Target image. (b) Secret image. (c) Mosaic image created by method proposed by Lai and Tsai [5] (d) Mosaic image created by proposed method with RMSE = 33.935. (e) Recovered secret image with RMSE=0.993 with respect to secret image (a). (f) Secret image of another experiment. (g) Target image. (h) Mosaic image created by Lai and Tsai [5] with RMSE=38.036. (k) Mosaic image created by proposed method with RMSE=27.084. (j) Recovered secret image with RMSE=0.874 with respect to secret image (g). (e) (h) (k) Mosaic images created with different tile image sizes: 8 x 8,16 x 16, 32 x 32.

Number of experiments have been conducted to test the proposed method by selecting the secret images and a document of 8X8, 16 X16 , 32X32 sizes. Furthermore, as shown in fig.3, we have drawn plots of the trends of various parameters verses different tiles image sizes including the parameters of 1) RMSE values of created mosaic images with respect to Secret images,2) RMSE values of created extracted images with respect to secrete images. 3) the numbers of required bits embedded for recovering the secret image. 4) The MSSIM values of extracted images with respect to secret mosaic images. It can seen from Figure 6 (a) that mosaic images created with smaller tile image sizes have smaller RMSE values with respect to the target image. On other hand, the number of required bits embedded for recovering the secret image is increased when the tile image becomes smaller, as can seen from Figure 6(c).We can see from Figure (d) that the MSSIM value of the created mosaic image with respect to the target image varies from 0.986 to 0.998, which is good enough, and this is the main concern of the proposed method because our goal is to create globally visually similar mosaic image which contains a secrete image.

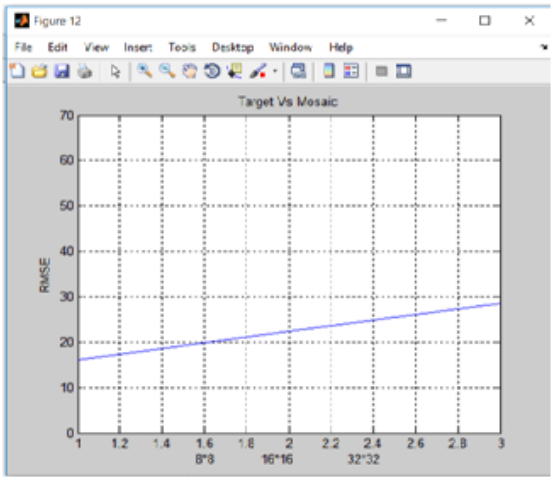
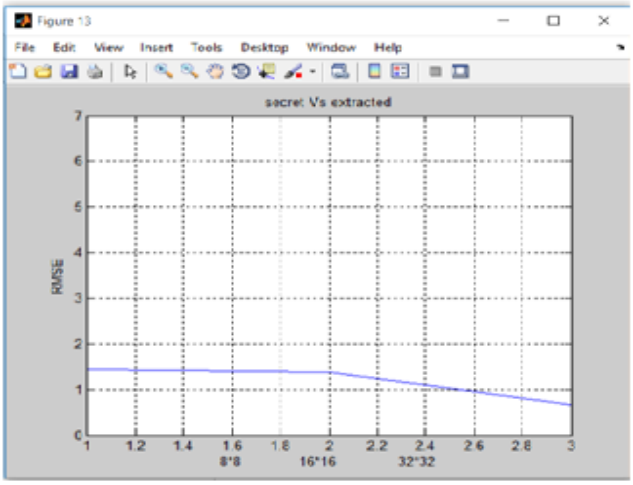
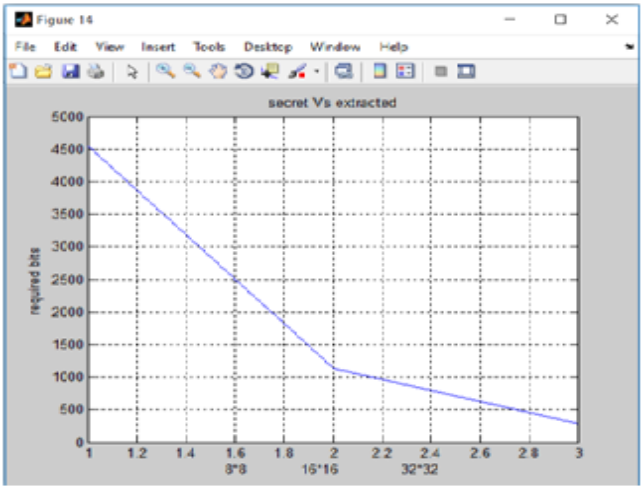


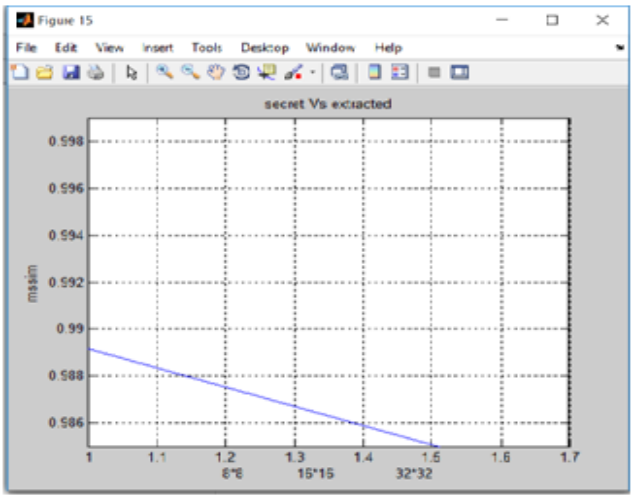
Figure (a) RMSE plot for created mosaic image w.r.t target image



Figure(b) RMSE values of recovered secret image



Figure(c) Numbers of required bits embedded in Secret image target image



Figure(d) MSSIM plot for created extracted images w.r.t secret images

V. CONCLUSION

A new secure image transmission technique has been proposed, which not just can create meaningful mosaic images but moreover can transform a secret image into a mosaic one with the similar data size for use as a camouflage of the secret image. By the use of appropriate pixel color transformations with a skilful scheme for handling overflows moreover underflows in the converted values of the pixels' colors, secret-fragment visible mosaic images with extremely high visual similarities to arbitrarily-selected target images can be formed with no need of a target image database. Also, the original secret images can be recovered almost losslessly from the created mosaic images. Good experimental results have shown the feasibility of the proposed method.

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 permutation substitution 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] 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.
[10] E.Reinhard, M. Ashikhimin, B. Gooch and P. Shirley, "Color transfer between images", IEEE Comput. Graph. Appl., Vol.21, no.5, pp.34-41, Sep.-oct.2001
[11] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," IEEE Trans. Image Process., vol. 13, no. 4, pp. 600–612, Apr. 2004.
[12] D. Coltuc and J.-M. Chassery, "Very fast watermarking by reversible contrast mapping," IEEE Signal Process. Lett., vol. 14, no. 4, pp. 255–258, Apr. 2007.

[13]C. C. Chang, C. C. Lin, C. S. Tseng, and W. L. Tai, "Reversible hiding in DCT-based compressed images," Inf. Sci., vol. 177, no. 13, pp. 2768–2786, 2007.

[14] T. S. Cho, S. Avidan, and W. T. Freeman, "A probabilistic image jigsaw puzzle solver," in Proc. IEEE CVPR, 2010, pp. 183–190.

[15] D. Pomeranz, M. Shemesh, and O. Ben-Shahar, "A fully automated greedy square jigsaw puzzle solver," in Proc. IEEE CVPR, 2011, pp. 9–16.

[16]Related images of the experiments [Online]. Available: http://people.cs.nctu.edu.tw/ yllee/yllee&whtsai sfv.html.

[17] S. Lee, C. D. Yoo, and T. Kalker, "Reversible image watermarking based on integer-to-integer wavelet transform," IEEE Trans. Inf. Forens. Secur., vol. 2, no. 3, pp. 321–330, Sep. 2007.

[18] W.-H. Lin, S.-J. Horng, T.-W. Kao, P. Fan, C.-L. Lee, and Y. Pan, "An efficient watermarking method based on significant difference of wavelet coefficient quantization," IEEE Trans. Multimedia, vol. 10, no. 5, pp. 746–757, Aug. 2008.

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

[20] Y. Hu, H.-K. Lee, K. Chen, and J. Li, "Difference expansion based reversible data hiding using two embedding directions," IEEE Trans. Multimedia, vol. 10, no. 8, pp. 1500–1512, Dec. 2008.

[21] 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.

[22] V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y.-Q. Shi, "Reversible watermarking algorithm using sorting and prediction," IEEE Trans. Circuits Syst. Video Technol., vol. 19, no. 7, pp. 989–999, Jul. 2009.

[23] X. Li, B. Yang, and T. Zeng, "Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection," IEEE Trans. Image Process., vol. 20, no. 12, pp. 3524–3533, Dec. 2011.

[24] W. Zhang, X. Hu, X. Li, and N. Yu, "Recursive histogram modification: Establishing equivalency between reversible data hiding and lossless data compression," IEEE Trans. Image Process., vol. 22, no. 7, pp. 2775–2785, Jul. 2013.