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

Niveditha G Biradar
Department of Computer Science
AMC Engineering College
Bangalore, India

Under the guidance of,
Mrs. Nandita
Assistant professor, Dept of Computer Science
AMC Engineering College
Bangalore, India

***Abstract*—A new technique of transmitting an image securely over any channel is proposed. This technique automatically transforms a given secret image into a secret-fragment-visible mosaic image. The mosaic image, which definitely looks similar to an arbitrarily selected target image and can be used as a camouflage of the secret image. This is yielded by dividing the secret image into fragments and transforming their color characteristics to be those of the corresponding blocks of the divided target image. Highly skillful techniques are employed to conduct the color transformation process so that the secret image may be recovered nearly losslessly. The information required for recovering the secret image is embedded into the created mosaic image by a nearly lossless data hiding scheme using a key. The key can be sent to the recipient in a secure manner. The experimental results on various secret and target images show that the proposed method is highly feasible.**

***Key Words — Data hiding, Image encryption, Key encryption, Mosaic image, Reversible color transformation, Secure image transmission, Secret image*.**

I. INTRODUCTION

Images from various sources are frequently used and transmitted through the internet for various applications, such as online personal photographic albums, confidential enterprise data, document storage systems, bio medical imaging systems, and military secrecy image databases. These images usually contain highly private and confidential information such that they should be protected from leakages and hacking during transmissions. Recently, several methods have been proposed for secure image transmission, for which two common techniques are encryption and data hiding. Image encryption [13] is a technique that makes use of the inherent natural properties of an image, such as high redundancy and strong spatial correlation [3], to get an encrypted image based on Shannon's [7] confusion and diffusion properties [1]–[7]. The encrypted image is a noise image so that no one can obtain the secret image from it unless he/she has the correct key.

However, the encrypted image is an entirely meaningless file, which cannot provide additional information [1] before decryption and may arouse a hacker's attention during transmission due to its randomness in form. An alternative solution to avoid this problem is data hiding [6] that hides a secret message into a cover image so that no one can realize, at any cost the existence of the secret data, in which the data type of the secret message is investigated in this paper is an image. The existing data hiding methods mainly utilize the techniques of LSB substitution [6], histogram shifting [8], difference expansion [1]–[9], prediction-error expansion [13]–[14], recursive histogram modification [14], and discrete cosine/wavelet transformations [14]–[18].

However, in order to reduce the distortion [13] of the resulting image, an evaluated upper bound for the distortion value is usually set on the selected cover image. A detailed discussion on this rate distortion issue can be found in [8]. Thus, a main issue of the methods for hiding data [15] in images is the difficulty to embed a large amount of message into a single image. Specially, if one wants to hide a preselected secret image into a cover image with the same size, the preselected secret image must be highly compressed [16] in advance. For example, for a data hiding method with an embedding rate of 0.6 bits per pixel, a secret image with 8 bits per pixel must be compressed at a rate of at least 94% beforehand in order to be hidden into a cover image. But, for many applications, such as keeping or transmitting Medical, military images, legal documents, etc., that are valuable [13] with no allowance of serious distortions, such data compression operations [2] are usually impractical [15]. Moreover, most image compression methods, such as JPEG compression [3], are not suitable for line drawings and textual graphics, in which slightly sharp contrasts between adjacent pixels are often destructed to become noticeable artifacts [11].

In this paper, a new and latest technique for secure image transmission is proposed, which transforms a selected secret image into a meaningful mosaic image with the same size and looking like a preselected target image [3]. The transformation process is controlled by a secret key [14], and only with the key can a person recover the secret image nearly losslessly [16] from the mosaic image. The proposed method is inspired by Lai and Tsai [11], in which a new type of computer art image, called total secret-fragment-visible mosaic image, was proposed. The mosaic image is the result of reordering or rearrangement of the fragments of a secret image in disguise [6] of another image called the target image preselected from a database. But an obvious and assured weakness of Lai and Tsai [11] is the requirement of a large image database so that the generated mosaic image can be sufficiently similar to the selected target image [13]. Using

their method, the user is not allowed to select freely his/her favorite image for use as the target image. It is therefore desired in this study to remove this [12] weakness [11] of the method while keeping its merit [4], that is, it is aimed to design a new method that can transform a given secret image into a secret fragment- visible mosaic image of the same size that has all the visual appearance of any freely selected target image without the need of a database. Specifically, after a target image is selected arbitrarily, then the given secret image is first divided into rectangular equal sized fragments called tile images, which then are fit into similar corresponding blocks in the target image, called target blocks, according to a similarity criterion based on the available color variations. Next, the color characteristic of each tile image are transformed to be that of the corresponding target block in the target image, which results in a mosaic image which looks like the target image. Relevant schemes are also proposed to conduct nearly lossless recovery of the original secret image from the resulting mosaic image. The proposed method is totally new in that a meaningful mosaic image is created, which is in contrast with the image encryption method that only creates meaningless noise images. Also, the proposed method can transform totally a secret image into a totally disguising mosaic image without compression, while a data hiding or encryption method must hide a highly compressed version of the secret image into a cover image when the secret image and the cover image have nearly the same data volume.

II. PROPOSED METHODOLOGY

Figure 1 shows the proposed approach. It involves two main phases. 1) Mosaic Image Creation, 2) Secret Image Recovery.

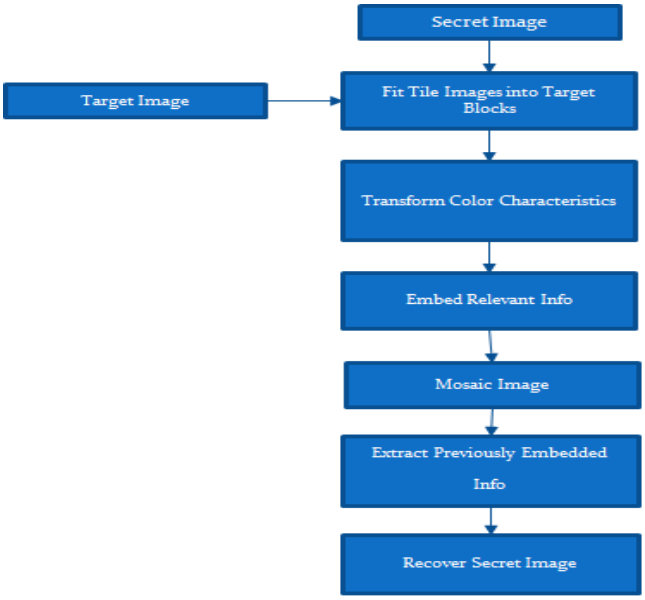

Fig.1. The Proposed Method

In the first step, a new mosaic image is yielded, which consists of the fragments of an input secret image with color transformation according to a similarity condition based on color variations.

The step includes four stages: 1) fitting the tile images of the secret image into the target blocks of a preselected target image; 2) transforming the color characteristic of each square shaped tile image in the secret image to become that of the corresponding target block in the target image; 3) embedding sufficient information into the created mosaic image for future recovery of the secret image. In the next phase, the embedded information is extracted to recover nearly losslessly the secret image from the generated mosaic image. The step includes two stages: 1) extracting the embedded information for secret image recovery from the selected mosaic image, and 2) successfully recovering the secret image using the extracted information.

III. MOSAIC IMAGE GENERATION

Some of the ideas of mosaic image generation are discussed here.

A. Applying Color Transformations

In the first stage of the proposed method, each of the tile image T in the given/selected secret image is fit into a target block B [11] in a preselected target image. Since the color characteristics of target T and block B are different from each other, how to change their color characteristics distributions such that to make them look alike is the main issue here. Reinhard et al. [11] proposed a color transfer scheme in this aspect, which converts the color characteristic of a selected image to be that of the one in the lαβ color space. This idea is an answer to the issue and has been adopted in this paper, except that the RGB color space instead of the lαβ one is used to reduce the volume of the required information for recovery of the original secret image.

B. Choosing Approporiate Target Blocks

In transforming the color characteristic of a tile image T to be that of a corresponding target block B as described above, how to choose an appropriate B for each T is a problem. Specially, we sort all the tile images to form a sequence, S_tile, and all the target blocks to form another, S_target. Then, we fit the first in S_tile into the first in S_target, fit the second in S_tile into the second in S_target, and so on.

C. Embedding Information

In order to successfully recover the secret image from the selected mosaic image, we have to embed relevant necessary recovery information into the mosaic image. For this, we implement a unique technique proposed by Coltuc and Chassery [3] and apply it to the least significant bits of the pixels in the created mosaic image to conduct data embedding. Highly unlike the classical LSB replacement methods [7], [24], [29], which substitute LSBs with message bits directly, the reversible contrast mapping method [11] applies simple integer transformations to pairs of pixel values. Specifically and iteratively, the method conducts forward and reverse integer transformations [11] as follows, respectively, in which (x, y) are a pair of pixel values and (x', y') are the transformed ones.

$$x' = 2x - y, \quad y' = 2y - x$$
$$x = \left\lceil \frac{2}{3}x' + \frac{1}{3}y' \right\rceil, \quad y = \left\lceil \frac{1}{3}x' + \frac{2}{3}y' \right\rceil.$$

This method yields high data embedding capacities almost close to the highest bit rates and has the lowest complexity reported so far yet.

IV. ALGORITHM

The detailed algorithms for creation of mosaic images and the recovery of secret images are given below. They are treated as Algorithm 1 and Algorithm 2.

A. Algorithm1: Creation of Mosaic Image:

Input: A selected secret image S, a selected target image T, and a secret key K.
Output: a secret- mosaic image F.
Steps:
Stage 1. Fitting the tile images into the target blocks.
Step 1: If the size of the target image T is different from that of the secret image S, change such that the size of T to be identical to that of S; and divide the secret image S into n tile images $\{T_1, T_2, \ldots, T_n\}$ as well as the target image T into n target blocks $\{B_1, B_2, \ldots, B_n\}$ with each T_i or B_i being of size NT.
Step 2: Evaluate the means and the standard deviations of each tile image Ti and each target block B_j for the three color channels; and evaluate accordingly the average standard deviations for T_i and B_j , respectively, for i = 1 through n and j = 1 through n.
Step 3: Sort the tile images in the set S_tile = $\{T_1, T_2, \ldots, T_n\}$ and the target blocks in the set S_target = $\{B_1, B_2, \ldots, B_n\}$ map in order the blocks in the sorted Stile to those in the sorted S_target in a 1-to-1 manner; and if necessary reorder the mappings according to the indices of the tile images, resulting in a mapping sequence L of the form: $T_1 \rightarrow B_{j1}$, $T_2 \rightarrow B_{j2}$, . . . , $T_n \rightarrow B_{jn}$.
Step 4: Now create a mosaic image F by fitting all the tile images into the corresponding target blocks.
Stage 2. Performing color conversions between the tile images and the target blocks.
Step 5. Create a new table with 256 entries, each of which with an index corresponding to a listed residual value, and assign an initial value zero to each of the entry.
Step 6. For each mapping $T_i \rightarrow B_{ji}$ in a sequence L, represent the means of T_i and B_{ji}, respectively, by eight bits; and represent the standard deviation quotient by seven bits, where c = r, g, or b.
Step 7. For each pixel pi in each tile image T_i of mosaic image F with color value ci where c = r, g, or b, transform ci into a new value cii; if cii is not smaller than 255 or if it is not larger than 0, then change cii to be either 255 or 0;
Stage 3. Embedding the secret image recovery information.
Step 8. Construct a table HT using the content of the counting table TB to encode all the values computed previously.
Step 9. 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 B_{ji}; 2) the optimal rotation angle θ° of T_i; 3) the means of T_i and B_{ji} and the related standard deviation quotients of all three color channels;
Step 10. Concatenate the bit streams M_i of all T_i in F in a raster-scan order to form a total bit stream Mt; use the secret key K to encrypt M_t into another bit stream M_{ti}
Step 11. Construct a bit stream I including: 1) the number of conducted iterations N_i for embedding M_t; 2) the number of pixel pairs N_{pair} used in the last iteration; and 3) The table HT constructed for the residuals; and embed the bit stream I into mosaic image.

Stage 3. Embedding the secret image recovery information
Step 12: Embedded sufficient information into the target block. Then generate a key based on any of the properties of the image. The key can be based on the rmse value, mean or standard deviation of the embedded blocks.

B. Recovery of the secret image

Input: A mosaic image F with n tile images $\{T_1, T_2, \ldots, T_n\}$ and the secret key K.

Output: The secret image S.
Stage 1. Extracting the secret image from the mosaic image.
Step 1: For the selected mosaic image, the first step is to extract the bit stream I by a reverse version of the scheme proposed in [14] and decode them to obtain the following: 1) the number of iterations N_i for embedding M_t; 2) the total number of used pixel pairs N_{pair} in the last iteration; and 3) the table HT for encoding the values of the residuals of the overflows or underflows.
Step 2. Extract the bit stream M_t using the values of N_i and N_{pair} by the same scheme used in the last step.
Step 3. Decrypt the bit stream M_t into M_t by K.
Step 4. Decompose Mt into n bit streams M_1 through M_n for the n to-be-constructed tile images T_1 through T_n in S, respectively.
Step 5. Decode Mi for each tile image T_i to obtain the following: 1) the index j_i of the block B_{ji} in F corresponding to T_i; 2) the optimal rotation angle θ° of T_i; 3) the means of T_i and B_{ji} and the related standard deviation quotients of all color channels; and 4) the overflow/underflow residual values in T_i decoded by the table HT.
Stage 2. Recovering the secret image.
Step 6. Recover one by one in a raster-scan order the tile images T_i, i = 1 through n, of the desired secret image S by the following steps: 1) rotate in the reverse direction the block indexed by j_i, namely B_{ji}, 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 according to (4); 3) use the extracted means, standard deviations, and compute the two parameters c_S and c_L; 4) scan Ti to find out pixels with values 255 or 0 which indicate that overflows or even underflows, respectively, have occurred there; 5) then add respectively the values c_S or c_L to the corresponding residual values of the found pixels; and 6) take the results as the final pixel values, which result in a final tile image T_i.
Step 7. Compose all the final tile images to form the desired secret image S as output.

V. SECURITY ISSUES

In order to increase the security of the proposed system, the embedded information for later recovery is encrypted with a secret key as given in the Algorithm 1 and only the receiver who has the key can decode the secret image. However, a hacker who does not have the key may still try to find all possible permutations of the tile images in the mosaic image to get the original secret image back. The number of all possible permutations is n!, and hence the probability for the hacker to correctly guess the permutation is p=1/n! which is very small in value. For e, for the typical case in which we divide a secret image of size 1024×768 into tile images with block size 8×8, the value n is (1024×768)/(8×8) = 12,288. So the probability to guess the permutation correctly without the key is 1/n! = 1/ (12,288!). Hence breaking away the system by this way of guessing is computationally infeasible [15]. In fact, we can view the addressed problem here as a square jigsaw puzzle [12] problem, which is to reconstruct a complete image from a set of unordered square puzzle parts [17]. Recently, many methods have been proposed to try to solve this problem automatically by utilizing measures of feature-based similarity [8], dissimilarity-based compatibility [9], prediction-based compatibility [10], and so on. But these state-of-art methods can only solve partially problems with limited numbers of puzzle parts automatically [6]. Also, the jigsaw puzzle [4] problem has been proved to be NP-complete [3], which means that we cannot solve the problem in polynomial time. In fact, the time complexity is n! $\approx\sqrt{2\pi n}$ (n/e) n as mentioned in [3], which is too big a number as well for our case here with n = 12,288. However, when n is much smaller than 1000, some compatible metrics may be utilized to solve the square jigsaw problem [3]. So, a large value of n should be used to increase the security of the proposed method. In addition to that, the addressed puzzle problem of the proposed method is more complicated than the conventional square jigsaw puzzle problem because the color characteristics of the puzzle parts have been changed, that is, adjacent puzzle [16] parts have different types color appearances, meaning is that, use of a greedy search using color similarities between originally adjacent fragments for image reconstruction as done in conventional manual reconstruction techniques is totally infeasible.

Furthermore, even if one happens to guess the permutation 100% correctly, such as the correctly guessed permutations, the hacker still does not know the correct parameters for recovering the original color appearance of the secret image because such parameter information for color recovery is encrypted as a bit stream using a generated secret key. Even so, it still should be assumed, in any case, that the hacker will observe the content of the mosaic image with an accurate permutation, and try to figure out the necessary useful information out of it. A hacker might analyze the spatial continuity of the mosaic image in order to estimate a rough version of the secret image. In order to increase the security of the proposed method against this type of attack, one of the possible ways is to use the key to randomize [2] important information of a selected secret image, such as the actual positions of the pixels in the secret image, before transforming the selected secret image into a new mosaic image by the proposed method. As a result of this, only authorized users with the key can know the correct secret image while a hacker cannot at any cost.

VI. RESULTS ANALYSIS

A series of experiments have been conducted to test the proposed method using many secret and target images with varying sizes. The algorithm is implemented in Matlab 2013. To show that the created mosaic image looks like the preselected target image, the quality metric of root mean square error (MSE) is utilized, which is defined as the square root of the mean square difference between the pixel values of the two images.

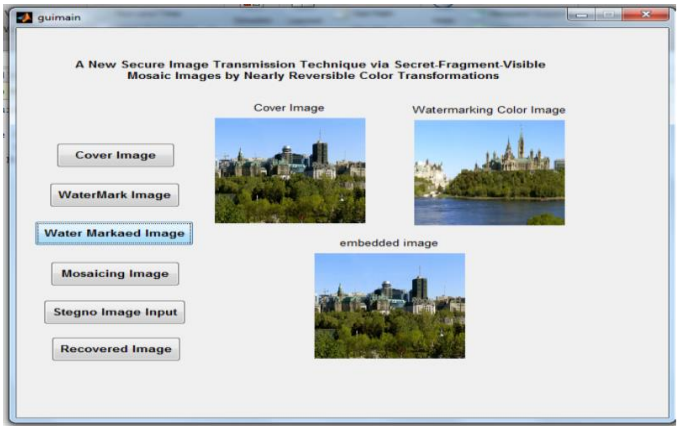

Fig.2 Image Embedding Process

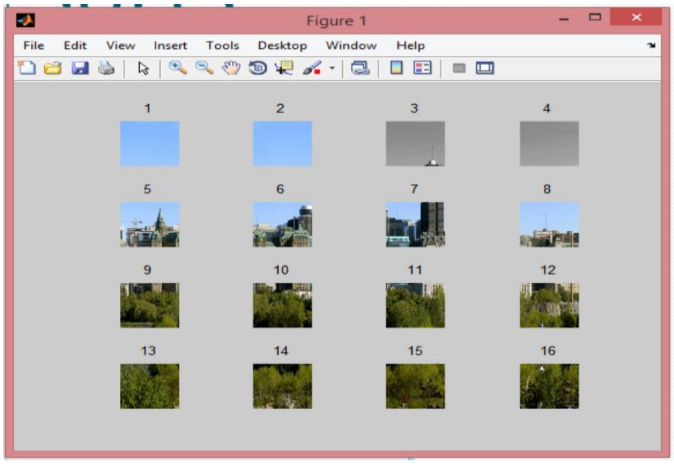

Fig.3 Divided cover image

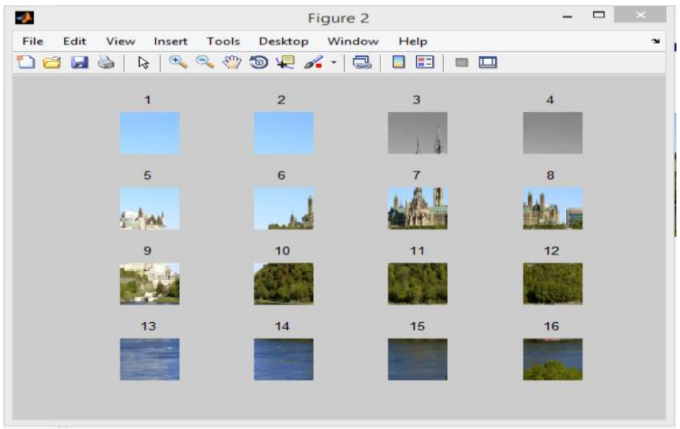

Fig. 4 Divided secret image

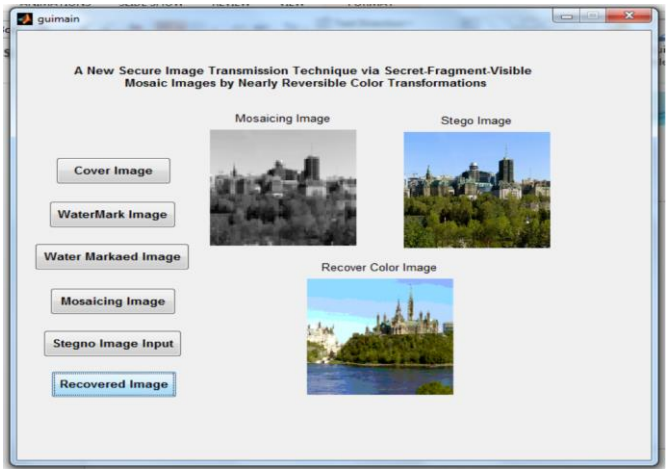

Fig.5 Recovered Color Image

VII. CONCLUSIONS

In this paper a new secure image transmission method has been proposed, which not only can create mosaic images but also can transform a given secret image into a mosaic one with the same data size for use as a cover of the secret image. By the use of appropriate pixel color transformations as well as a skillful technique for embedding secret information in the converted values of the pixel intensity colors, secret and fragment visible mosaic images with very highly similar visual characteristics to arbitrarily-selected target images can be created with no need of a prior target image database. Also, the original secret image can be recovered almost nearly losslessly from the created mosaic images. Experimental results on various randomly selected secret and target images have shown the accuracy 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 chaos based 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] 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] 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.
[12] 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.
[13] 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.
[14] 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.
[15] J. Fridrich, M. Goljan, and R. Du, "Invertible authentication," Proc. SPIE, vol. 3971, 2001, pp. 197–208.
[16] 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.
[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] 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.
[20] W. B. Pennebaker and J. L. Mitchell, JPEG: Still Image Data Compression Standard. New York, NY, USA: Van Nostrand Reinhold, 1993, pp. 34–38.
[21] 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.
[22] 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.
[23] 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, IEEE Transactions on Circuits AND Systems for Video Technology, VOL. 24, NO. 4, April 2014