An Enhanced and Secure Image Transmission Technique using Secret Fragment Visible Mosaic Image

Ms. Vimitha A
Student, M.Tech (DECS)
Department of E & C Engineering
St Joseph Engineering College,
Mangaluru, D.K, Karnataka, India

Ms. Shama B. N
Assistant Professor
Department of E & C Engineering
St Joseph Engineering College,
Mangaluru, D.K, Karnataka, India

***Abstract*— Paper deals with the creation of a new type of computer art image called the secret fragment visible mosaic image, which contains small fragments of secret image. The preliminary mosaic image is created by dividing the secret image into fragments called tile images and embedding them into the target image based on the image similarity measure between the tile image and target blocks. The preliminary mosaic image is created by fitting small fragments of secret image in to target image, achieving an effect of embedding. The given source image is secretly embedded into the resulting preliminary mosaic image. The information of the tile image fitting sequence is embedded into the preliminary mosaic image, which is required to recover the original secret image. The image obtained after embedding the required information, to recover the original secret image is called as mosaic image. The receiver first recovers the tile image fitting sequence from the mosaic image and this information is used to retrieve the original secret image. This method is used to ensure secrecy of the image, secure image transmission and for covert communication.**

I. INTRODUCTION

Currently images from various sources are frequently utilized and transmitted via internet for various applications such as, document storage systems, online personal photograph albums, banking applications, military image database and medical imaging system. These images usually contain private or confidential information so that they should be protected against leakages during transmission. There are many techniques proposed for secure image transmission. The two most common approaches for secure image transmission are image encryption and data hiding. Image encryption is a technique that makes use of natural property of an image, such as strong spatial correlation and high redundancy, to get an encrypted image based on Shannon's confusion and diffusion properties [1]. The encrypted image is a noise image that no one can figure out the secret image without the exact key. However, the encrypted image is a meaningless file, which does not provide any additional information before decryption. Due to its randomness in form it may arouse an attacker's attention during transmission. An alternative to avoid this problem is data hiding that hides secret data into a cover image so that no one can realize the existence of the secret data. The techniques involved in the data hiding methods are LSB substitution [2], histogram shifting [3], difference expansion [4], prediction error expansion [5], discrete cosine transformation [6] and discrete wavelet transformation [7].

A new type of art image, called secret fragment visible mosaic image, contains small fragments of a given secret image. By observing the mosaic image one can see all fragments of the source image but the fragments are so small and arranged in random position that no one can figure out the original source image. Therefore the source image is said to be secretly embedded into the resulting mosaic image though the fragments are all visible to the observer.

The secret image is first divided into fragments called secret tiles which are fit into target blocks based on the similarity criteria between the secret tiles and target blocks. The resulting image is called as the preliminary mosaic image. The information required to retrieve the original secret image is embedded into randomly selected blocks by a secret key. The image obtained after the data hiding technique is called as the secret fragment visible mosaic image.

II. BASIC IDEA OF MOSAIC IMAGE CREATION

A. Flow diagram of mosaic image creation and secret image recovery

A flow diagram of the technique is illustrated in figure 1, which include mainly three phases:

Phase 1- Selecting the target image which is most similar to the secret image.

Phase 2- Creation of mosaic image using the secret tiles of secret image and the selected target image.

Phase 3- Extraction of the original secret image from the mosaic image.

The first phase includes selecting the target image which is slightly similar to the secret image according to the similarity criteria between target image and secret image.

The second phase includes two steps of operation:

Step1 - Fitting the secret tiles of the secret image into target blocks of the target image to create preliminary mosaic image;

Step2 - Embedding the information necessary to recover the original secret image.

The third phase includes two steps of operation:

Step1 – Retrieving the information embedded into the mosaic image;

Step2 – Recovering the original secret image using the information retrieved from the mosaic image.

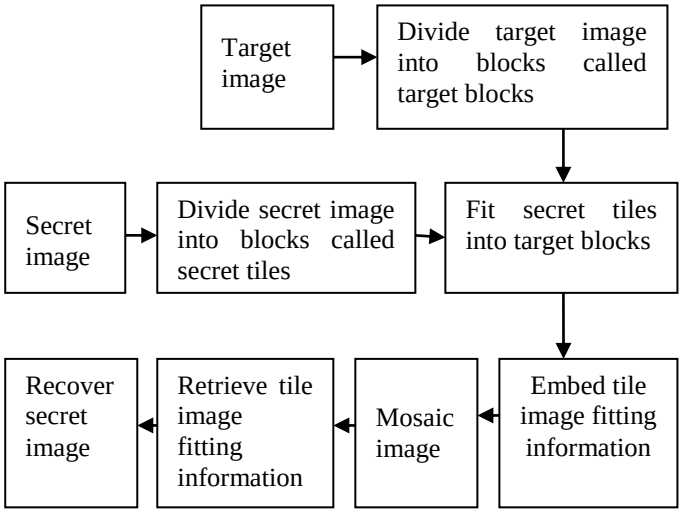


Figure 1. Flow diagram for mosaic image creation and secret image recovery.

B. Target Image Selection

The selection of target image plays a very important role in the creation of preliminary mosaic image as proposed in [8]. If a selected target image is not similar to a given secret image, then it reduces the information hiding effect in the preliminary mosaic image. To generate better results, the target image selected should be similar to the secret image. The similarity between the secret image and target image can be obtained based on the similarity criteria. One such method to obtain the similarity between two images is by One-Dimensional color transformation technique. The technique first requantizes the color values (r, g, b) into fewer levels, such as N_r, N_g, N_b respectively, which results in the new color values (r_a, g_a, b_a). Then it converts the three values (r_a, g_a, b_a) into a single one which is defined by

$$f(r_a, g_a, b_a) = r_a + N_r \times g_a + N_r \times N_g \times b_a \qquad (1)$$

The mosaic image obtained using one dimensional color transformation technique is noisy.

Therefore a new color transformation function 'h' is proposed in [8] and is defined as follows.

$$h(r_a, g_a, b_a) = b_a + N_b \times r_a + N_b \times N_r \times g_a \qquad (2)$$

where the number of levels N_b, N_r and N_g are set to 8. The green channel value 'g_a' is assigned the largest weight and the value 1 is assigned to blue channel value 'b_a' as human eye is most sensitive to green color and least sensitive to blue one.

C. Similarity measure between secret and target image

To generate the preliminary mosaic image as proposed in [8] for a given secret image it is required to select a target image which is slightly similar to the secret image so as to increase effect of hiding the secret image into the target image. First divide the secret image 'S' into blocks of size 'S_C', where the blocks are called as secret tiles. Compute the mean of RGB color values of all pixels in the secret tiles. Calculate the h-feature value for all the secret tiles. Divide the target image into blocks of size 'S_t', where the blocks are called as target blocks. Compute the mean and h-feature value for all the target blocks. An image similarity value 'm' between secret tiles and target blocks is defined as follows

$$m = \frac{1}{h_s - h_t} \qquad (3)$$

Where 'h_s' and 'h_t' are the h-feature of the secret and target image blocks. Larger the value of 'm' indicates that there is more similarity between the secret tiles and target blocks.

III. BASIC IDEA OF DATA EMBEDDING TECHNIQUE

To extract the original secret image from the mosaic image the necessary data to recover the secret image has to be embedded into the preliminary mosaic image. Reversible contrast mapping technique as proposed in [9] is used for data embedding.

A. *Reversible contrast mapping technique*

Let the image gray level range be [0, M], where M =255 for eight bit gray level images and let the pair of pixels be (p, q). The forward RCM converts pairs of pixels (p, q) into pairs of pixels (p', q') which is defined by equations (4) and (5).

$$p' = 2p - q \qquad (4)$$

$$q' = 2q - p \qquad (5)$$

The conversion is restricted to a sub domain D $\subset$ [0, M] x [0, M] defined by equation (6).

$$0 \le 2p - q \le M, 0 \le 2q - p \le M \qquad (6)$$

The inverse transform is defined by equations (7) and (8)

$$p = \left\lceil \frac{2}{3}p' + \frac{1}{3}q' \right\rceil \qquad (7)$$

$$q = \left\lceil \frac{1}{3}p' + \frac{2}{3}q' \right\rceil \qquad (8)$$

Where $\lceil \alpha \rceil$ is the ceil function (ceil function: the smallest integer greater than or equal to α).

B. Data Extraction

At detection, in order to extract the data and to restore the original pixels, each pair that is converted should be correctly identified. For each pair, the LSB of the first pixel is used to

indicate whether the pair was transformed or not. The LSB of the first pixel is embedded with '0' to indicate the pair (p, q) is not transformed and the LSB of the first pixel is embedded with '1' to indicate the pair (p, q) is transformed to (p', q'). In order to avoid decoding ambiguities, some odd pixel pairs should be avoided, such as those located on the borders of M. The pairs subjected to ambiguity are found by solving the equations: 2p - q = 1, 2q - p = 1, 2p - q =M, 2q - p = M. For M=255, there are only 170 such pairs. Let 'M_c' be the domain of the transform without the ambiguous odd pixel pairs.

IV. BASIC IDEA OF RECOVERING THE SECRET IMAGE

To reconstruct the original secret image, the index that forms a mapping from the secret tiles to the target blocks is required. These mappings are recorded into a sequence 'Z_R', called the secret recovery sequence. For the purpose of security, embed this sequence into randomly selected blocks in the mosaic image by using reversible contrast mapping technique [9]. The mapping can be obtained by starting from the top leftmost block s_1 in the secret image to find the most similar target block d_i in the target image to form the mapping s_1 to d_i and include it in the secret recovery sequence. Pick the next secret tiles s_2 in a raster scan order to find the most similar block d_j in the target image and form the mapping s_2 to d_j. Then proceed similarly with the third mapping s_3 to d_k, and so on. This process is continued until the last secret tiles at the bottom rightmost corner of the secret image is processed. The resulting 'Z_R' includes two block indexing sequence Z_1= 1, 2, 3,…, and Z_2 = i, j, k,…. to form the mapping 1 to i, 2 to j, 3 to k, and so on. Since 'Z_1' is an ordered sequence of 1, 2, 3,… the sequence 'Z_1' can be excluded and include the sequence 'Z_2' in 'Z_R', so as to reduce the data volume of 'Z_R'. This reduced data volume is embedded into the preliminary mosaic image. The width and height of the secret image and the size of the secret tiles are embedded into the first block of the created preliminary mosaic image.

The width and height of the secret image is denoted as 'W_S' and 'H_S' respectively and the size of the secret tiles are denoted as 'S_C'. The number of tile images 'N' in the secret image can be computed by equation (9).

$$N = \frac{W_S \times H_S}{S_C} \qquad (9)$$

The number of bits required to specify the index of a secret tile is denoted as 'N_S', which can be computed by equation (10).

$$N_s = \lfloor log_2^N + 1 \rfloor \qquad (10)$$

Where $\lfloor a \rfloor$ represents integer floor operation.

The number of bits required to represent the secret recovery sequence 'Z_R' is denoted as 'N_T' and can be computed by equation (11).

$$N_T = N \times N_s \qquad (11)$$

The receiver can compute the value of 'N_T' by extracting the data embedded into the first block of the mosaic image. Reversible contrast mapping scheme [9] requires two LSBs in an identical channel for embedding a bit. Since each color pixel has three channels, the number of bits that can be embedded into a tile image 'N_R' is computed by equation (12).

$$N_R = \frac{3 \times S_C}{2} \qquad (12)$$

V. ALGORITHM FOR THE CREATION OF SECRET FRAGMENT VISIBLE MOSAIC IMAGE AND RECOVERY OF THE ORIGINAL SECRET IMAGE

A complete algorithm for the generation of secret fragment visible mosaic image is described in the following, followed by some experimental results.

A. *Algorithm for mosaic image creation*

Step 1. Divide the secret image 'S' into blocks called secret tiles of size 'S_C'. Record the width 'W_S' and height 'H_S' of the secret image and compute the number of secret tiles in 'S' by equation (9).
Step 2. Select a target image that is slightly similar to the secret image
Step 3. Calculate the h-feature values for all the secret tiles in the secret image and target blocks in the target image.
Step 4. In a raster scan order, of the secret image find the most similar target blocks d_i, d_j, d_k,…in target image corresponding to the 'N' secret tiles s_1, s_2, s_3,… in the secret image, respectively, so as to construct the secret recovery sequence Z_R, using the h-feature calculation.
Step 5. To generate the preliminary mosaic image, fit the secret tiles s_1, s_2, s_3,… into the corresponding target blocks d_i, d_j, $d_{k,...,}$ respectively.
Step 6. Concatenate the width 'W_S' and height 'H_S' of the secret image along with the size 'S_C' of the secret tiles and convert the concatenated data into a binary string and embed these strings into the first block of the created preliminary mosaic image by using the reversible contrast mapping scheme [9].
Step 7. Convert the secret recovery sequence 'Z_R' into a binary string with its length 'N_T' computed by equations (9) to (11).
Step 8. In the created preliminary mosaic image, select the blocks in a random fashion, except the first block, to embed 'N_R' bits of 'Z_R' into all 'S_C' pixels of the preliminary mosaic image by reversible contrast mapping scheme. This process is repeated until all 'N_T' bits in 'Z_R' are exhausted, where 'N_R' is calculated using equation (12).
Step 9. The image obtained after embedding the secret recovery sequence in the preliminary mosaic image is the desired secret fragment visible mosaic image.

B. Algorithm for embedding the secret recovery sequence

Procedure for data embedding is as follows:
Step 1. Partition the entire preliminary mosaic image into pairs of pixels (p, q).
Step 2. For each pair (p, q), the following steps are computed:

a) If (p, q) ∈ M_c and if it consist of even pixel values, transform the pair (p, q) using the equations (4) and (5). Set the LSB of p' to 1, considering the LSB of q' for data embedding.

b) If (p, q) ∈ M_c and if it consist of odd pixel values, set the LSB of p to 1, considering the LSB of q for data embedding.

c) If (p, q) ∉ M_C, set the LSB of p to 0, and save the true value.

C. *Algorithm to extract the data from the mosaic image to recover the secret image.*

Steps for recovering the original data is as follows:

Step 1. Partition the entire image into pairs of pixels.

Step 2. For each pair (p', q') the following steps are computed:

a) If LSB of p' is 1, extract the LSB of q' and save it into the detected sequence. Set the LSBs of p', q' to 0, and recover the original pair (p, q) by equations (7) and (8).

b) If LSB of p' is 0, and the pair (p', q') with LSBs set to '1' ∈ M_c, extract the LSB of q'. Save the results in the detected sequence, restoring the original pair as (p', q').

c) If LSB of p' is 0, and the pair (p', q') with LSBs set to '1' ∉ M_c, then the original pair (p, q) is recovered by replacing the LSB of p' with the corresponding true value extracted from the sequence.

D. *Algorithm to recover the secret image.*

Step 1. Extract the width and height of the secret image as well as the size 'S_C' in a raster scan order from the first block of the mosaic image using the lossless LSB technique [9].

Step 2. Using the data of the width, height and size of the secret tiles, calculate the length 'N_T' of the secret recovery sequence Z_R using equations (9) to (11).

Step 3. Repeatedly select random blocks in mosaic image, except the first block with the secret key 'K' as the seed. Retrieve 'N_R' bits from all the 'S_C' pixels of the mosaic image using the reverse version of lossless LSB scheme [9]. Concatenate the bits in a sequential order, until all the 'N_T' bits of 'Z_R' are retrieved, where 'N_R' is calculated by equation (12).

Step 4. Convert all 'N_S' bits of 'Z_R' into an integer, which indicates the index of the secret tiles in the original secret image, which results in the secret recovery sequence.

Step 5. Using the secret recovery sequence, the secret tiles are arranged accordingly to obtain the original secret image.

VI. EXPERIMENTAL RESULTS

The results obtained by using one dimensional color transformation technique are shown in figure 2. The input secret image, figure 2(a) and the target image, figure 2(b) forms the preliminary mosaic image, figure 2(c). This preliminary mosaic image obtained using one - dimensional color transformation technique is quite noisy. The mosaic image obtained by using a similarity measure based on h-feature calculation is given in figure 2(d), which is clear without distortion when compared to one dimensional color transformation technique.

Experimental results obtained after implementing the algorithm for mosaic image creation is shown in figure 3. The secret image of size 240x360 is shown in figure 3(a) and the target image of size 240x360 is shown in figure 3(b).

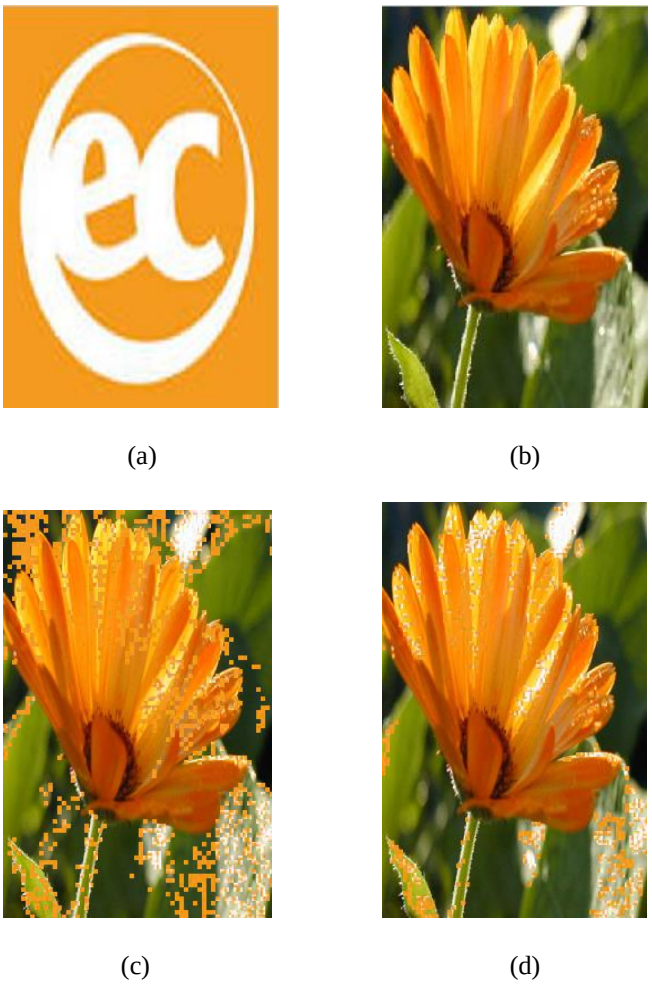


Figure 2. Effects of preliminary mosaic image creation based on image similarity measure using one-dimensional color features. (a) Secret image (b) Target image (c) Mosaic image creation based on one dimensional transformation technique (d) Mosaic image creation based on h-feature.

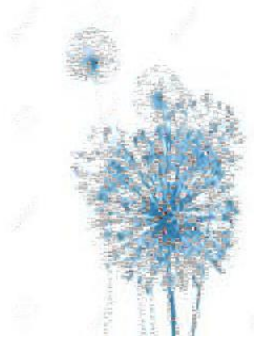
The secret and target image are divided into blocks of size 4x4. The preliminary mosaic image obtained after fitting the secret tiles into target blocks are illustrated in figure 3(c). The mosaic image obtained after the lossless LSB replacement scheme [9] is shown in figure 3(d). The implemented results show that mosaic image obtained after the data hiding technique is similar to that of preliminary mosaic image. The secret fragments are not visible in the mosaic image thus enhancing the security.

For the application in biomedical signal processing, the secret image can be selected as a medical image. Figure 4(a) illustrates the secret image. The target image of size 240x 360 is shown in figure 4(b). The preliminary mosaic image is shown in figure 4(c) and the mosaic image obtained after the lossless LSB replacement scheme is shown in figure 4(d). The results show that the mosaic image is similar to the target image and the fragments of secret image are not visible and therefore the technique of mosaic image creation can be used for medical applications.

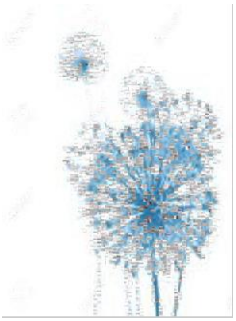
The secret fragment visible mosaic image obtained to verify the results for different tile sizes are illustrated in figure 5. The secret and target images of size 240x360 are shown in figure 5(a) and 5(b). The mosaic image obtained for the tile size of 4x4 is shown in figure 5(c) and the mosaic image obtained for the tile size of 8x8 is shown in figure 5(d). The result implies that, As the block size is increased the secret fragments are visible but they are arranged in random position that no one can identify the original secret image.

(a)

(b)



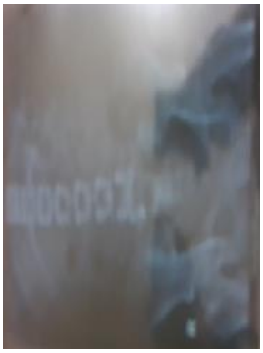
(c)



(d)

Figure 3. Results of mosaic image creation.

(a) Secret image (b) Target image (c) Preliminary mosaic image before data hiding technique (d) Mosaic image after data hiding technique.



(a)

(b)

(c)

(d)

Figure 4. Results of medical image transmission technique.

(a) Secret image (b) Target image (c) Preliminary mosaic image before data hiding technique (d) Mosaic image after data hiding technique.

(a)

(b)

(c)

(d)

Figure 5. Results of mosaic image using different tile sizes. (a) Secret image (b) Target image (c) Mosaic image created with tile image size 4x4 (d) Mosaic image created with tile image size 8x8.

VII. CONCLUSION

From the experimental results it is observed that the there is distortion in the mosaic image created using 1-D color histogram transformation technique. The mosaic image created using h-feature gives a better result.

When the secret and target image are divided into blocks of size 4x4 the mosaic image created is similar to target image. If the block size is increased to 8x8 the secret fragments are visible. As the block size increases the secret fragments are visible to the observer but they are in random position and difficult to figure out the original secret image. Thus enhancing the security features.

A large number of bits can be embedded into the preliminary mosaic image using reversible contrast mapping technique. The mosaic image obtained after the data hiding technique is similar to the preliminary mosaic image without distortion. The technique can be used for various applications where security is a major concern. As a future work the data embedded into the mosaic image has to be extracted to recover the secret image.

REFERENCES

[1] 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.

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

[3] 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.

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

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.