Volume-4, Issue-5, May Special Issue-2015 • ISSN No 2277 - 8160

Research Paper

Engineering

A SECRET SHARING METHOD VIA SECRET-FRAGMENT-VISIBLE-MOSAIC IMAGE

N.Sumedha Sherly

Department of Electronics and Communication Engineering
Narayana Engineering College,Nellore-524003, A.P, India

P.Sindhuri

Department of Electronics and Communication Engineering
Narayana Engineering College,Nellore-524003, A.P, India

ABSTRACT

A new secret sharing based method is future which transforms a secret picture into secret fragment visible mosaic ize and looking like a preselected target picture. The mosaic image which looks as target picture and used as a disguise of a secret picture is afforded by isolating the secret picture into shards and transform the color characteristics to be that of corresponding target lumps of the target image.

In color transformation process, skillful schemes are used, so that of the secret picture may be improved nearly losslessly. The scheme of usage the overflows/underflows in the renewed pixels by coping the color difference in the untransformed color space is proposed. The information which is used to recover the secret picture is embedded into the mixture image by a lossless data hitting technique using a key. The results show the possibility of the proposed method.

KEYWORDS : Image encryption, data hiding, color transformation, mosaic image, secret figure recovery.

I.INTRODUCTION

Images from various sources are frequently utilized and transmit through the internet for a range of applications, such as confidential enterprise documents, medical imaging systems for electronic patient record (EPRs), and military image databases. These images frequently include personal or confidential information. So they should be limited from leakages while transmitting.

In this proposal, a secret sharing method is proposed, which transforms a secret figure into a mosaic image with equal size and appears like a preselected target figure. This process is controlled by a secret key; with that key only a man recover the secret figure from the mosaic image. The mosaic image is the result of the relocation of the fragments of a secret figure in cover of another image called the target image which is preselected.

II.LITERATURE SURVEY

In recent years, many techniques were proposed to increase the safety of the secret, for which two common approaches are image encryption and data hiding.

Encryption is the method of encoding messages or information in a way that only official parties can read it, to get an encrypted image based on Shannon's confusion and diffusion properties[1]-[3]. The ciphered figure is a noisy figure, so that no one can gain the secret image unless he/she knows the correct key. Data hiding embeds the secret data in the cover image so that no one can recognize the being of the secret data. At present in data hiding the techniques used are LSB substitution[4], histogram shifting[5], difference expansion[6], prediction-error expansion[7]-[8], recursive histogram shifting[9], and discrete cosine/wavelet transformations[11].

In data hiding method there is a disadvantage, of which it will be highly compressed when the secret image and the cover image are of same volume,

(a) With permutation-diffusion architecture this is planned to improve a bit-level permutation advance for chaos-based image cipher[10].

(b)The redundancy in the digital capacity to get reversibility. Performance of a reversible data-embedding algorithm are Payload capacity limit, Visual quality, and Complexity[12].

(c)The threshold is given based on computing weighted -within class variance through considering probability density function of significant difference[13].

(d)Hybrid data embedding scheme offering both reversibility and high hiding capacity properties while maintaining acceptable image quality of stego-image about 30 dB[14].

III.PROPOSED METHOD

The proposed method consist of two main parts
1) Mosaic image creation.
2) Secret figure recovery.
It describe in the algorithms.

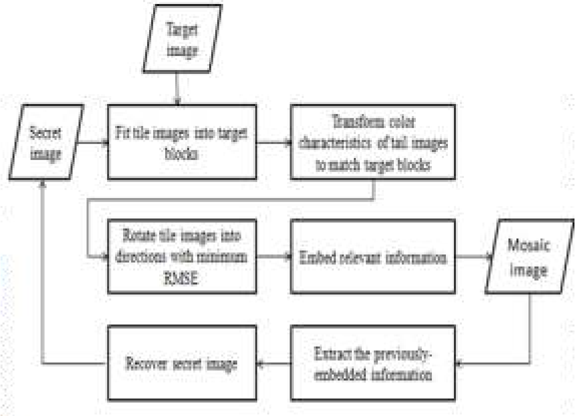
Target image
Secret image
Fit tile images into target blocks
Transform color characteristics of tail images to match target blocks
Rotate tile images into directions with minimum RMSE
Embed relevant information
Mosaic Image
Recover secret image
Extract the previously-embedded information

Fig.1: Flow diagram of proposed method

CREATION OF A MOSAIC IMAGE

(1)Transforming color between Blocks.

Each tile image T in the given secret figure is fit to the corresponding target block B in target figure. The color characteristics of T and B are different to each other. RGB color space is used because it decreases the size of the necessary information for recovery of the secret figure. Let T and B be represented the pixel sets {p1, p2, . . . , pn} and {p1', p2', . . . , pn'}.

Let the color of each pi be denoted by (ri, gi, bi) and that of each Pi' by (ri', gi', bi'). Calculate the means and standard deviations of T and B, respectively,

$$\mu c=1/n.\sum_{i=1}^{n} ci, \quad \mu c'=1/n.\sum_{i=1}^{n} ci' \qquad (1)$$

$$\sigma c=\sqrt{\frac{1}{n}.\sum_{i=1}^{n}(ci-\mu c)^2},$$

$$\sigma c'=\sqrt{\frac{1}{n}.\sum_{i=1}^{n}(ci'-\mu c')^2} \qquad (2)$$

in which ci and ci' denote the C-channel values of pixels pi and pi', where c = r, g, or b and c' = r', g', or b'.

Next, we calculate new color values (ri'', gi'', bi'') for each pi in T by,

$$ci''=qc(ci-\mu c)+\mu c' \qquad (3)$$

in which qc = σc'/σc is the standard deviation quotient and it verified as new color mean and variance of the resultant tile image T' are equal to that of B. To compute the original color values (ri, gi, bi) of pi from the modern ones (ri'', gi'', bi''), we use the following equation which is the inverse of (3)

$$ci=(1/qc)(ci''-\mu c')+\mu c \qquad (4)$$

Specifically, for each color channel we allow means of T and B to have 8 bits, range (0-255), and the standard deviation quotient qc to have 7 bits, range (0.1-12.8). We do not allow qc to be 0 because the pixel value cannot recovered back because 1/qc in (4) is not clear.

(2)Rotating Blocks with Smaller RMSE Value.
To choose appropriate B for each T we use average standard deviations to measure. We sort all the tile images to Stile, and all the target blocks to Starget, according to the average standard deviations of the three color channels, fit the Stile to Starget in 1-to-1 manner. Color similarity between the resulting tile image T' and the target block B of turning T' into one of four directions, 0º, 90º, 180º, and 270º, with the minimum root mean square error (RMSE) value with respect to B for final use to fit T into B.

(3)Overflows/Underflows in Color Transformation.
After the color transformation is carried, some pixel values of new tile image T' may have overflows/underflows. The residual values in the untransformed color space quite than in transformed one. Where we compute the smallest possible color value cs (with c = r, g, or b) in T that becomes larger than 255, and the largest possible value cl in T that becomes smaller than 0 since the color shift process has been conducted:

$$cs=[(1/qc)(255-\mu c')+\mu c];$$
$$cl=[(1/qc)(0-\mu c')+\mu c]. \qquad (5)$$

ci which gives an overflow after the color transformation, we compute its residual as |ci - cs|; and for ci which gives an underflow, we compute its residual as |cl - ci|. Then, the possible values of the residuals of ci will all lie in the range of 0 to 255. Huffman encoding scheme to encode the residuals in order to reduce the number of required bits to represent them.

(4)Information Embedding for Secret figure Recovery.
A technique[15] used apply for embedding information to the least significant bits of the pixels, with message bits directly. The method conducts forward and backward integer transformations[15], in which (x, y) are a pair of pixel values and (x', y') are the transformed ones,

$$x'=2x-y, \quad y'=2y-x \qquad (6)$$

$$x=[\tfrac{2}{3}x'+\tfrac{1}{3}y'] \quad y=[\tfrac{1}{3}x'+\tfrac{2}{3}y'] \qquad (7)$$

Information contains: 1)Index of B; 2)Rotation angle of T; 3) Means of T and B and standard deviation quotients of all color channels; 4) overflow/underflow residuals. Information for recovering tile image T included five-component bit stream
M = t1t2…tmr1r2m1m2…m48q1q2…q21d1d2…dk

1) The index of B needs m bits to represent,

$$m= [log[(Ws.Hs)/Nt]]$$

Where Ws and Hs are width and height of secret image, Nt is the size of target image;

2) Needs two bits to represent rotation angle of T for four rotation directions;

3) 48 bits required to represent the means of T and B because we use eight bits to represent a mean value in each color channel; 4) needs 21 bits to represent the quotients of T over B in the three color channels with each channel requiring 7 bits; 5) total number k of required bits for represent the residuals depends on the number of overflows/underflows in T'. Bit streams of all the tile images are chained in order into a total bit stream Mt for entire secret image. To protect Mt from being attacked, we encrypt it with a secret key to obtain an encrypted bit stream M't, which is finally embedded into the pixel pairs in the mosaic image. Where, we have to embed some related information about the mosaic image generation in the mosaic image for recovery process. The information, described as bit stream I, which consists of : 1) how many iterations perform in the process of embedding the bit stream M't ; 2) number of pixel pairs are used in the last iteration for embedding M't; 3) Huffman table for encoding the residuals. It indicates that some loss will be occurred in the recovery of the secret image, mainly in the color transformation process using(3), where each pixel's color value ci is multiplied by the standard deviation quotient qc, and the resulting real value ci'' is truncated to be an integer in the range of 0 to 255. However, because each truncated part is smaller than the value of 1, the recovered value of ci using (4) is still precise enough to gives a color nearly identical to its original one. Even when overflows/underflows occur at some pixels in the color transformation process, we record their residual values as discovered previously and after using (4) to recover the pixel value ci, we add the residual values back to the computed pixel values ci to get the original pixel data giving up nearly losslessly recovered secret image. Recovered secret figure has a very small RMSE value compared to the original secret figure.

IV.ALGORITHMS FOR THE PROPOSED METHOD

Algorithm 1: Mosaic Image Formation

Step 1: Divided secret image S into n tile images {T1, T2,…,Tn} and target image T into n target blocks{B1, B2,..,Bn}.

Step 2: Calculate the mean and standard deviations of each tile image Ti deviations of each tile image Ti the average standard deviation of Ti, and Bj for i=1 to n and j=1 to n.

Step 3: According to the average standard deviation values of blocks map the tile images in sorted S_{tile}, to those of sorted S_{target} in 1-to-1 manner, resulting in mapping sequence L.

Step 4: Create a counting table TB with 256 entries, each with an index corresponding to residual values and assign initial value 0 to each entry.

Step 5: Represent means μc and μc' by 8 bits and standard deviation quotient qc by 7 bits. Calculate new color value ci'' by (3), compute the residual value Ri for pixel pi and increment count by 1 in the counting table.

Step 6: Compute RMSE values for each color transformed tile image Ti in F with respect to its corresponding target block Bji, rotate Ti in optimal direction θº.

Step 7: Construct a Huffman table *HT* using the content of the counting table *TB* to encode all the residual values.

Step 8: For each tile image T_i in mosaic image F, construct a bit stream M_i consists of 1) the index of Bij; 2) rotation angle θº of Ti; 3) means of Ti and Bij and related standard deviation coefficient; 4) overflow/underflow residulesin T_i encoded in Huffman table HT.

Step 9: Construct bit streams Mi of all Ti as raster-scan order to form total bit stream Mt; use the secret key K to encrypt M_t into another bit stream M_t'; and embed M_t' into F.

Step 10: 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 Huffman table HT constructed for the residuals; and embed the bit stream I into mosaic image F.

Algorithm 2: Secret figure recovery

Step 11: Extract bit stream I form F by reverse scheme proposed in [16], to get data items represent in step (10).

Step 12: extract bit stream M't using Ni and N_{pair} by the same scheme.

Step 13: Decrypt bit stream M't into Mt by K.

Step 14: Decompose Mt into n bit streams M1-Mn as to reconstructed tile images T1-Tn.

Step 15: Decode Mi for each tile image Ti to obtain data items represent in step(8).

Step 16: Regain one by one in a raster-scan order the tile images T_i, i = 1 to *n*, by following steps: 1) rotate in the reverse direction of the block indexed by j_i, namely B_{ji}, and fit the resulting block content into T_i to form an initial tile image Ti;2) extract means and standard deviation quotients to recover the original pixel values in T_i according to (4); 3) use the extracted means, standard deviation quotients, and (5) to compute the two parameters c_S and c_L; 4) scan T_i to find out pixels with values 255 or 0 which indicate that overflows underflows; 5)add the values c_S or c_L to the corresponding residual values of the found pixels; 6) take the results as the final pixel values, resulting in a final tile image T_i.

Step 17: Create all the final tile images to form the secret figure *S* as output.

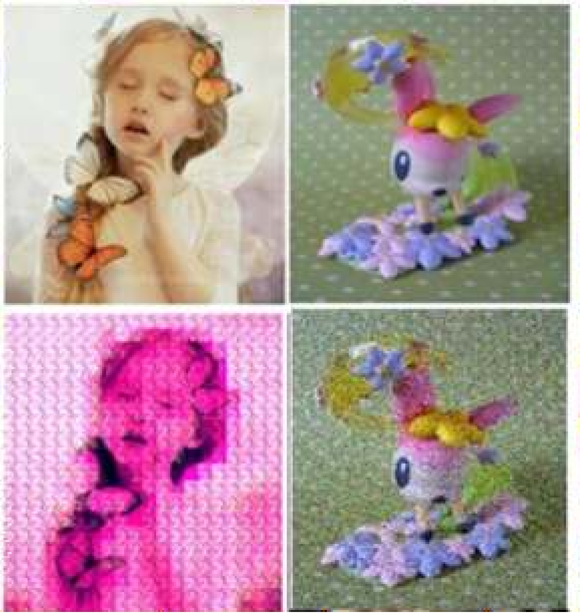

Fig 2: (a) Target figure, (b) Secret figure, (c) Mosaic image created (d) Recovered secret figure

V.RESULTS AND DISCUSSIONS

The results of the proposed method 2(a) target figure, 2(b) Secret figure and 2(c) shows the created mosaic image. Fig. 2(d) shows the recovery secret image. It can be seen in the result that the created mosaic image is clearer with smaller RMSE value.

The parameters including the mosaic image created with smaller tile images has a smaller RMSE value with respect to the target image will come correctly else the noise will increase in the created mosaic image. On the other hand, if the size of the tile image is reduce, the number of bits to embedded the mosaic image.

The sizes of target figures should match those of possible secret figures otherwise created mosaic image will become blurred.

VI.CONCLUSION

A new secret sharing method has been proposed secret-fragment visible mosaic images with very high visual similarities to arbitrarily-selected target images can be created without the need of a target figure database. The original secret figure can be obtained nearly lossless from the created mosaic images. Good results have shown the possibility for the proposed method. Future studies may be directed to applying the proposed method to images of color models other than the RGB.

REFERENCES

[1]J.Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," Int.J. Bifurcat. Chaos. | [2]L.H.Zhang, X.F.Liao, and X.B.Wang, "An image encryption approach based on chaotic maps," Chaos Solit. Fract. | [3]S.Behnia, A.Akhshani, H.Mahmodi, and A.Akhavan, "A novel algorithm for image encryption based on mixture of chaotic maps," Chaos Solit. Fract., | [4]C.K.Chan and L.M.Cheng, "Hiding data in images by simple LSB substitution," Pattern Recognit.., | [5]Z.Ni, Y.Q.Shi, N.Ansari, and W.Su, "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol. | [6] J.Tian, "Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol., | [7]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. | [8]X.Li, B.Yang, and T.Zeng, "Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection," IEEE Trans. Image Process. | [9]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. | [10]S.Lee, C.D.Yoo, and T.Kalker, "Reversible image watermarking based on integer-to-integer wavelet transform," IEEE Trans. Inf. Forens. Secur. | [11]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. | [12]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. | [13]I.J.Lai and W.H.Tsai, "Secret- fragment-visible mosaic image—A new computer art and its application to information hiding," IEEE Trans. Inf. Forens. Secur. | [14]E.Reinhard, M.Ashikhmin, B.Gooch, and P.Shirley, "Color transfer between images," IEEE Comput. Graph. | [15] 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.