INTERNATIONAL JOURNAL OF RESEARCH
In Advanced Engineering Technologies

Volume 4, Issue 4 AUG 2015

A ROBUST APPROACH TO SECURELY TRANSFER A SECRET IMAGE USING REVERSIBLE COLOR TRANSFORMATIONS FOR CONFIDENTIALITY

D. SHAFRUNALI[1] MR. K. MANJUNATH[2]

Department of ECE (DECS) [1] Assistant PROFESSOR[2]

SREE RAMA ENGINEERING COLLEGE, Tirupati, Andhra Pradesh, INDIA

Abstract

Hiding the data in digital images has been area of interest in the digital image processing domain. Although so much work has been carried out in the literature to resolve the issues like increasing the data capacity, creating the secret image alike of target image but most of the works fails to meet the practical requirements. This paper presents an approach where mosaic image generation has done by dividing the secret image into fragments and transforming their respective color characteristics into corresponding blocks of the target image. Usage of the Pixel color transformations helps to yield the lossless recovered image based on the untransformed color space values. Generation of the key plays an important role to recover the data from the secret image in lossless manner. Finally the same approach can be performed on videos also which helps to eliminate the flickering artifact to achieve the lossless data recovery in motion related videos. The experimental results shows good robust behavior against all incidental and accidental attacks and compare to the conventional algorithms performance evaluation has been increased in an significant way.

KEYWORDS: Color transformation, mosaic image, secure image transmission

1. INTRODUCTION

Recently, many methods have been proposed for securing image transmission, for which two common approaches are image encryption and data hiding. Image encryption is a technique that makes use of the natural property of an image, such as high redundancy and strong spatial correlation, to get an encrypted image based on Shannon's confusion and diffusion properties. 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 a meaningless file, which cannot provide additional information before decryption and may arouse an attacker's attention during transmission due to its randomness in form. An alternative to avoid this problem is data hiding that hides a secret message into a cover image so that no one can realize the existence of the secret data, in which the data type of the secret message investigated in this paper is an image. Existing data hiding methods mainly utilize the techniques of LSB sub situation, histogram shifting, difference expansion, prediction-error expansion, recursive histogram modification, and discrete cosine/wavelet transformations. However, in order to reduce the distortion of the resulting image, an upper bound for the distortion value is usually set on the payload of the cover image.

A discussion on this rate distortion issue can be found in . Thus, a main issue of the methods for hiding data in images is the difficulty to embed a large amount of message data into a single image. Specifically, if one wants to hide a secret image into a cover image with the same size, the secret image

must be highly compressed in advance. For example, for a data hiding method with an embedding rate of 0.5 bits per pixel, a secret image with 8 bits per pixel must be compressed at a rate of at least 93.75% beforehand in order to be hidden into a cover image. But, for many applications, such as keeping or transmitting medical pictures, military images, legal documents, etc., that are valuable with no allowance of serious distortions, such data compression operations are usually impractical. Moreover, most image compression methods, such as JPEG compression, are not suitable for line drawings and textual graphics, in which sharp contrasts between adjacent pixels are often destructed to become noticeable artifacts. In this paper, a new 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 process is controlled by a secret key, and only with the key can a person recover the secret image nearly losslessly from the mosaic image. The proposed method is inspired by Lai and Tsai, in which a new type of computer art image, called secret-fragment-visible mosaic image, was proposed. The mosaic image is the result of rearrangement of the fragments of a secret image in disguise of another image called the target image preselected from a database. But an obvious weakness of Lai and Tsai is the requirement of a large image database so that the generated mosaic image can be sufficiently similar to the selected target image. 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 weakness of the method while keeping its merit, that is, it is aimed to design a new method that can transform a secret image into a secret fragment visible mosaic image of the same size that has the visual appearance of any freely selected target image without the need of a database.

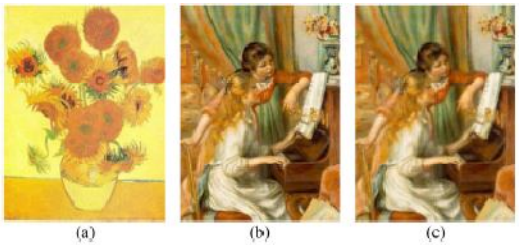


Figure 1: Result yielded by the proposed method. (a) Secret image. (b) Target image. (c) Secret-fragment-visible mosaic image created from (a) and (b) by the proposed method.

As an illustration, Fig. 1 shows a result yielded by the proposed method. Specifically, after a target image is selected arbitrarily, the given secret image is first divided into rectangular fragments called tile images, which then are fit into similar blocks in the target image, called target blocks, according to a similarity criterion based on color variations. Next, the color characteristic of each tile image is transformed to be that of the corresponding target block in the target image, resulting 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 new in that a meaningful mosaic image is created, in contrast with the image encryption method that only creates meaningless noise images. Also, the proposed method can transform a secret image into a disguising mosaic image without compression, while a data hiding method must hide a highly compressed version of the secret image into a cover image when the secret image and the cover image have the same data volume.

2. PROPOSED METHOD

Color Transformations between Blocks In the initial part of the planned technique, every tile image T within the given secret image is match into a target block B in a preselected target image. Since the color characteristics of T and Bare totally different from one another, the way to amendment their color distributions to form them look alike is that the main issue here color transfer theme in this face t, that converts the color characteristic of an image to be that of another within the l αβ color area. This idea is a solution to the difficulty and is adopted during this paper, except that the RGB color area rather than the l αβ one is employed to reduce the amount of the desired data for recovery of the original secret image. More specifically, let and B be described as 2 pixel sets{p1,p2 ,p3,…….. p_n}and{p_1', p_2' ……p_n'} severally. Let the color of every pi be denoted by ((r_i, g_i, b_i). which of everyp_1' by (r_i', g_i', b_i'). At first, we tend to work out the means and standard deviations of T and B, severally; in every of the 3 color channels R, G, and B by the subsequent formulas:

$$\mu_c = \frac{1}{n}\sum_{i=1}^{n} ci$$

$$\mu_c = \frac{1}{n}\sum_{i=1}^{n} c_i' i \text{.....(1)}$$

$$\sigma_c = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(c_{i-}\mu_c)^2}$$

$$\sigma_c' = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(c_i' - \mu_c')^2} \text{.....(2)}$$

$$c_i^n = q_c(c_i - \mu_c) + \mu_c' \text{.....(3)}$$

in $q_c = \sigma_c / \sigma_c'$ is the standard deviation quotient and c=(r,g,orb). It can be verified easily that the new color mean and variance of the resulting tile image T' are equal to those of B, respectively. To compute the original color values ((r_i, g_i, b_i) of p_i from the new ones (r_i', g_i', b_i'), we use the following formula which is the inverse of (3)

$$c_i = \frac{1}{q_c}(c_i^n - \mu_c') + \mu_{.c.} \text{ ..... (4)}$$

Furthermore, we've to embed into the created mosaic image sufficient data concerning the new tile image T' foruse within the later stage of convalescent the initial secret image. For this, theoretically we will use (4) to compute the initial pixel price of p_i However, the concerned mean and normal deviation values within the formula area unit all real numbers, and it is impractical to embed real numbers, every with several digits, in the generated mosaic image. Therefore, we limit the numbers of bits wont to represent relevant parameter values in (3) and (4). Specifically, every |for every} color channel we tend to enable each of the means of T and B to have 8 bits with its worth within the vary of 0 to 255, and also the standard deviation quotient qc in (3) to have seven bits with its worth within the vary of 0.1 to 12.8. That is, each mean is modified to be the closest value within the range of0 to 255, and each qc is modified to be the closest value in the range of 0.1 to 12.8. We don't enable qc to be zero 0otherwise the first picture element worth cannot be recovered back by (4) for the reason that 1/qc in (4) isn't outlined once qc=0

2.1 Choosing Appropriate Target Blocks and Rotating Blocks to Fit Better with Smaller RMSE Value

In transforming the colour characteristic of a tile image T to be that of a corresponding target block

Bas represented higher than, how to choose an appropriate B for every T is a problem. For this, we use the standard deviation of the colors within the block as a live to pick out the foremost similar for each T. Specially, we type all the tile pictures to make a sequence ,Stile, and every one the target blocks to make another, S target, consistent with the typical l values of the quality deviations of the 3 color channels. Then, we work the primary in S tile into the primary in S target, fit the second in S tile into the second in S target, and so on.

Additionally, after a target block B is chosen to fit a tile image T and after the color characteristic of T is transformed, we conduct a further improvement on the color similarity between the resulting tile imageT' and the target blockBby rotating T' into one of the four directions, 0 o ,90 o , 180 o , and 270 o , which yields a rotated version of T' with the minimum root mean square error (RMSE) value with respect to B among the four directions for final use to fit T into B.

2.2 Embedding Information for Secret Image Recovery

In order to recover the secret image from the mosaic image, we have to embed relevant recovery information into the mosaic image. In order to recover the secret image from the mosaic image, we've to embed relevant recovery info into the mosaic image. For this, we adopt a way planned by Coltuc and Chassery and apply it to the smallest amount vital bits of the pixels within the created mosaic image to conduct information embedding. not like the classical LSB replacement strategies, that substitute LSBs with message bits directly, the reversible distinction mapping technique applies simple integer transformations to pairs of pixel values. Specifically, the method conducts forward and backward integer transformations as follows, respectively, in which (x, y) are a pair of pixel values and (x', y') are the transformed ones

$$x' = 2x - y, \qquad y' = 2y - x$$

$$X=\left[\frac{2}{3}x' + \frac{1}{3}y'\right] \qquad Y=\left[\frac{1}{3}x' + \frac{2}{3}y'\right]$$

The method yields high data embedding capacities close to the highest bit rates and has the lowest complexity reported so far The information required to recover a tile image T which is mapped to a target block B includes: 1) the index of B;2)the optimal rotation angle of T; 3) the truncated means of T and Band the standard deviation quotients, of all color channels; and 4) the overflow/underflow residuals. These data items for recovering a tile image Tare integrated as a five-component bit stream of the form

M=t1t2...tmr1r2m1m2...m48q1q2...q21d1d2...d

In more detail, the numbers of required bits for the five data items in Mare discussed below: 1) the index of B need sm bits to represent, with m computed by

M=[log [(Ws×Hs)]/N_T]

4. ALGORITHMIC FLOW

In this proposed method it contains mainly in the two phases they are one is mosaic image creation and second one is secret image recovery process.

PHASE 1

Stage 1: Fitting the tile images into the target blocks.

Step 1: here first we need to compare the sizes of the target and secret image sizes if they are not equal then we need to resize and equalize them and divide the secret image into tile images$\{T_1.T_2, T_3 \dots \dots \dots T_n\}$ and also the target image as$\{B_1, B_2 B_3 \dots \dots \dots . B_N\}$ and with each T_i , B_j belongs to size of N_t.

Step 2: then calculate the both mean and standard deviation from the above equations are (3),(4) for each tile image T_i and target image B_j respectively for i,j=1 …n.

Step 3: now we have the set of tile images as $S_{title} = \{T_1.T_2, T_3 \dots \dots \dots T_n\}$ and target blocks are $S_{target} = \{B_1, B_2 B_3 \dots \dots \dots . B_N\}$ then by sorting of this two according to the mean and standard deviation values we need to map the two tile image set to the target blocks in 1-to-1 manner then resulting mapping sequence L of the form $T_1 \quad B_{J1} \dots\dots\dots T_N \quad B_{Jn}$

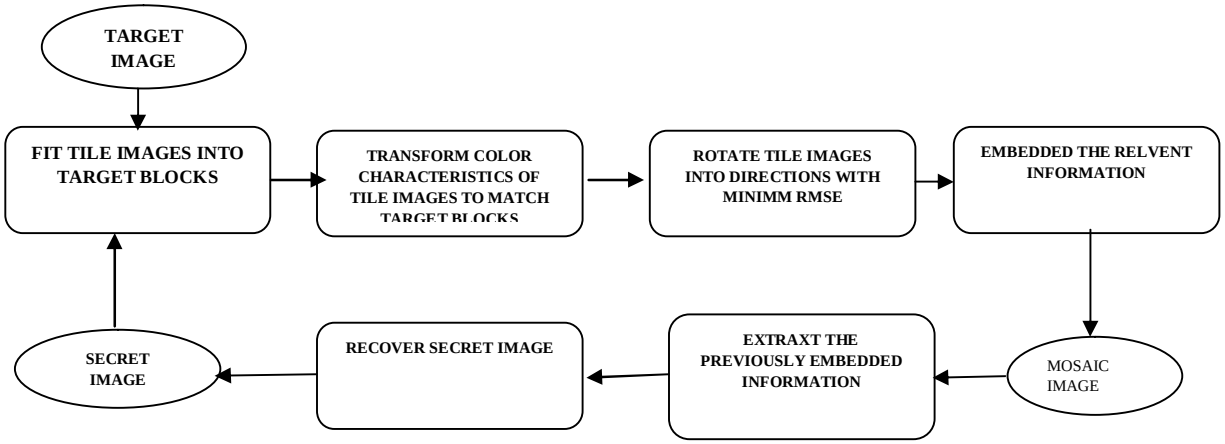


Figure 2: Algorithmic flow

Step 4: so create the mosaic image F by fitting the tile images into the corresponding blocks according to L .

Stage 2: Rotating Images

For each colored transformed tile image T_1 calculate the RMSE values in F with respected to corresponding target block B_{Ji} after rotating T_i into directios of $\theta = 0,90,180,270,360$ respectively.

PHASE 2: secret image retrieval

Stage1: extracting the secret image recovery information.

Step 1: extract the bit stream I from the F by reversion scheme and decode them to get the below items1) the number of iterations N_i for embedding $M_i^{'}$ the total number of used pixel pairs N_{pair} in the last iteration.

Step 2: repeat the above step to extract the $M_i^{'}$.

Step 3: and decrypt the bit stream $M_i^{'}$ into M_i by the using of key K.

Step 4: DecomposeM_t into n bit streamsM_1 through $M_n$for the n to-be-constructed tile images T_1 through T_n in S, respectively .

Step 5: Decode M_i for each tile image T_1 to obtain the following data items: 1) the index ji of the block B_{ij} in F corresponding to T_i2) the optimal rotation angle θ° of T_i; 3) the means of $T_i$and B_{ij} and the related standard deviation quotients of all color channels.

Step 6: Recover one by one in a raster-scan order the tile images T_i, i= 1 throughn, of the desired secret image S by the following steps: 1) rotate in the reverse direction the block indexed by j i, namely B_{ij}, in F through the optimal angle θ° and fit the resulting block content into T_i to form an initial tile image T_i 2) use the extracted means and related 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 cS and cL;4) scan T_i to find out pixels with values 255 or 0 which indicate that overflows or underflows, respectively, have occurred there; 5) add respectively the values cS orcLto the corresponding residual values of the found pixels; and 6) take the results as the final pixelvalues, resulting in afinaltile image T_i.

Step 7: combine the all final tile images to get desired secret image T.

5. RESULTS

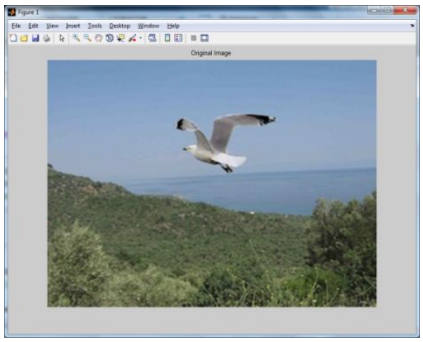


Figure 1: Original image

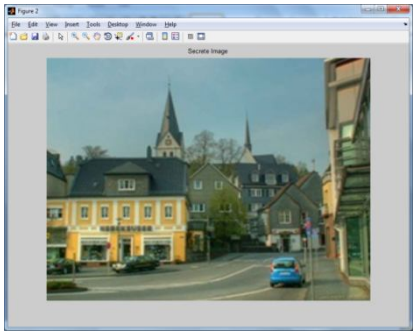


Figure 2: Secret image

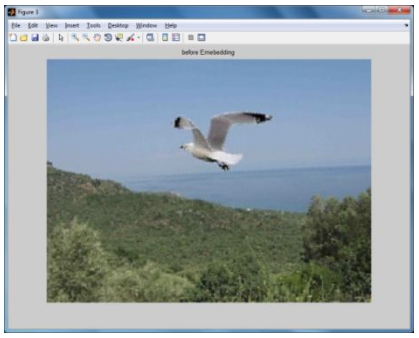


Figure 3: before embedding mosaic image

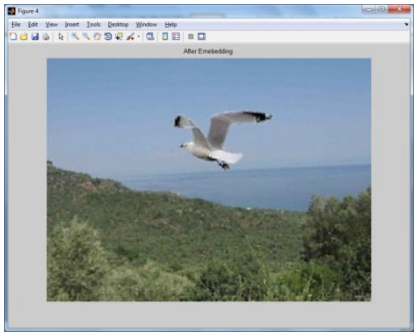


Figure 4: after embedding mosaic image

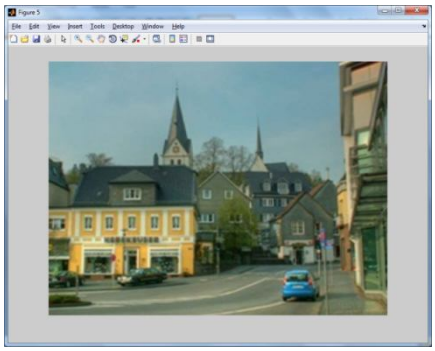
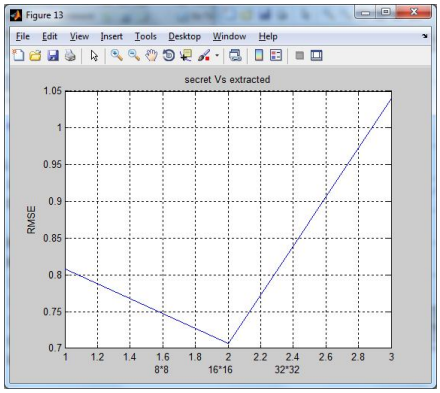
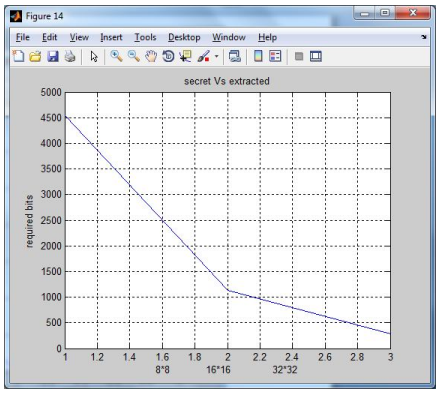


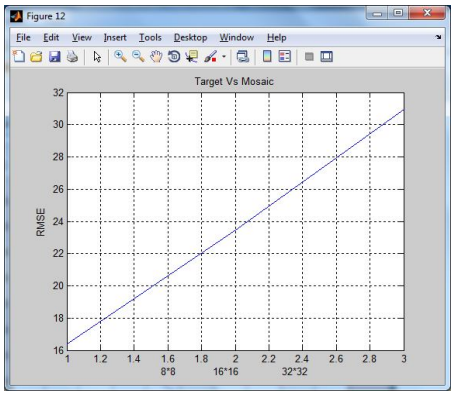
Figure 5: Extracted image



Graph 1: Secret vs Extracted (RMSE)



Graph 2: Secret vs Extracted (Required bits)



Graph 3: Target vs Mosaic (RMSE)

EXTENSION

The proposed method has been written on the digital images, in this work images are used as media to hide the secret image by using the an approach where mosaic image generation has done by dividing the secret image into fragments and transforming their respective color characteristics into corresponding blocks of the target image. Usage of the Pixel color transformations helps to yield the lossless recovered image based on the untransformed color space values. So in extension work we did the same algorithm on the digital videos. The approach towards videos is totally different from the images, so algorithm on videos is the contribution to the proposed work.

6. CONCLUSION

Hiding the data in digital images has been area of interest in the digital image processing domain. Although so much work has been carried out in the literature to resolve the issues like increasing the data capacity, creating the secret image alike of target image but most of the works fails to meet the practical requirements. This paper presents an approach where mosaic image generation has done by dividing the secret image into fragments and transforming their respective color characteristics into corresponding blocks of the target image. Usage of the Pixel color transformations helps to yield the lossless recovered image based on the untransformed color space values. Generation of the key plays an important role to recover the data from the secret image in lossless manner. Finally the same approach can be performed on videos also which helps to eliminate the flickering artifact to achieve the lossless data recovery in motion related videos. The experimental results shows good robust behavior against all incidental and accidental attacks and

compare to the conventional algorithms performance evaluation has been increased in a significant way.

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.