
R.V. Ramana Kumar1, S. Narayana Reddy2

1 PG Scholar, Dept of ECE, S.V. University College of Engineering, Tirupati, AP, India, E-mail: rvrkumar63@gmail.com.
2 Professor, Dept of ECE, S.V. University College of Engineering, Tirupati, AP, India, E-mail: snreddysvu@yahoo.com.

Abstract: Another secure picture transmission strategy is proposed, which changes naturally a given substantial volume mystery picture into a supposed mystery piece noticeable mosaic picture of the same size. The mosaic picture, which appears to be like an discretionally chose target picture and may be utilized as a cover of the mystery picture, is yielded by partitioning the mystery picture into pieces and changing their shading qualities to be those of the comparing squares of the objective picture. Able strategies are intended to lead the shading change process so that the mystery picture may be recuperated almost losslessly. A plan of taking care of the floods/undercurrents in the changed over pixels' shading values by recording the shading contrasts in the untransformed shading space is additionally proposed. The data needed for recuperating the mystery picture is installed into the made mosaic picture by a lossless information concealing plan utilizing a key. Great exploratory results demonstrate the practicality of the proposed strategy.

Keywords: Load Balancing Model; Public Cloud; Cloud Partition; Game Theory.

I. INTRODUCTION

At present, pictures from different sources are as often as possible used and transmitted through the web for different applications, for example, online individual photo collections, private endeavor chronicles, archive stockpiling frameworks, restorative imaging frameworks, and military picture databases. These pictures generally contain private or secret data so that they ought to be shielded from spillages amid transmissions. As of late, numerous strategies have been proposed for securing picture transmission, for which two regular methodologies are picture encryption and information stowing away. Picture encryption is a strategy that makes utilization of the common property of a picture, for example, high excess and solid spatial relationship, to get a scrambled picture based on Shannon's disarray and dispersion properties. The scrambled picture is a commotion picture so that nobody can get Composition got May 9, 2013; reexamined July 21, 2013; acknowledged September 16, 2013. Date of distribution September 25, 2013; date of current adaptation April 2, 2014. This exploration was upheld to some degree by the NSC, Taiwan, under Grants 101-3113-P-009-006 and 102-2218-E-009-003, and to some extent by the Ministry of Education, Taiwan, under the five-year Project of "Going for the Top University" from 2011 through 2015. This paper was prescribed by Associate Editor W. Zhu. the mystery picture from it unless he/she has the right key.

On the other hand, the scrambled picture is an inane record, which can't give extra data before decoding and may excite an aggressor's consideration amid transmission because of its arbitrariness in structure. A distinct option for stay away from this issue is information concealing that conceals a mystery message into a spread picture so that nobody can understand the presence of the mystery information, in which the information sort of the mystery message researched in this paper is a picture. Existing information concealing strategies mostly use the methods of LSB substitution, histogram moving, contrast development, forecast blunder extension, recursive histogram adjustment, also, discrete cosine/wavelet changes. Be that as it may, keeping in mind the end goal to lessen the contortion of the subsequent picture, an upper headed for the bending quality is normally situated on the payload of the spread picture. An examination on this rate distortion issue can be found. In this way, a principle issue of the strategies for concealing information in pictures is the trouble to insert a lot of message information into a solitary picture.

In particular, if one needs to shroud a mystery picture into a spread picture with the same size, the mystery picture must be very compacted ahead of time. Case in point, for an information concealing system with an implanting rate of 0.5 bits per pixel, a mystery picture with 8 bits per pixel must be compacted at a rate of in any event 93.75% in advance keeping in mind the end goal to be covered up into a spread picture. Yet, for some applications, for example, keeping or transmitting medicinal pictures, military pictures, authoritative reports, and so forth, that are profitable with no remittance of genuine contortions, such information pressure operations are generally unfeasible. Also, most picture pressure techniques, for example, JPEG pressure, are not suitable for line drawings and printed illustrations, in which sharp differentiations between nearby pixels are frequently destructed to end up observable antiques. In this paper,
another method for secure picture transmission is proposed, which changes a mystery picture into an important mosaic picture with the same size and resembling a preselected target picture. The change procedure is controlled by a mystery key, and just with the key can a man recoup the mystery picture about losslessly from the mosaic picture. The proposed strategy is enlivened by Lai and Tsai, in which a new sort of PC workmanship picture, called mystery piece obvious mosaic picture, was proposed. The mosaic picture is the after effect of reworking of the pieces of a mystery picture in mask of another picture called the objective picture pre select 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. 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 characterization 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.

II. EXISTING METHOD

Data hiding is a method of hiding secret messages into a cover-media such that an unintended observer will not be aware of the existence of the hidden messages. In this paper, 8-bit grayscale images are selected as the cover media. These images are called cover-images. Cover-images with the secret messages embedded in them are called stego-images. For data hiding methods, the image quality refers to the quality of the stego-images. In the literature, many techniques about data hiding have been proposed. One of the common techniques is based on manipulating the least-significant-bit (LSB) planes by directly replacing the LSBs of the cover-image with the message bits. LSB methods typically achieve high capacity. Wang, proposed to embed secret messages in the moderately significant bit of the cover-image. A genetic algorithm is developed to find an optimal substitution matrix for the embedding of the secret messages. They also proposed to use a local pixel adjustment process (LPAP) to improve the image quality of the stego-image. Unfortunately, Corresponding author, since the local pixel adjustment process only considers the last three least significant bits and the fourth bit but not on all bits, the local pixel adjustment process is obviously not optimal. The weakness of the local pixel adjustment process is pointed out. As the local pixel adjustment process modifies the LSBs, the technique cannot be applied to data hiding schemes based on simple LSB Substitution.

Recently, further proposed a data hiding scheme by optimal LSB substitution and genetic algorithm. Using the proposed algorithm, the worst mean-square-error (WMSE) between the cover-image and the stego-image is shown to be that obtained by the simple LSB substitution method. In this paper, a data hiding scheme by simple LSB substitution with an optimal pixel adjustment process (OPAP) is proposed. The basic concept of the OPAP is based on the technique proposed. The operations of the OPAP is generalized. The WMSE between the cover-image and the stego-image is derived. It is shown that the WMSE obtained by the OPAP could be less than that obtained by the simple LSB substitution method. Experimental results demonstrate that enhanced image quality can be obtained with low extra computational complexity. The results obtained also show better performance than the optimal substitution method, the optimal pixel adjustment process is described and the performance is analyzed. Experimental results are given data hiding by simple LSB substitution. In this section, the general operations of data hiding by simple LSB substitution method is described.

III. PROPOSED MITIGATION SCHEME

In this paper, another procedure for secure picture transmission is proposed, which changes a mystery picture into an important mosaic picture with the same size and resembling a preselected target picture. The change procedure is controlled by a mystery key, and just with the key can a man recoup the mystery picture almost losslessly from the mosaic picture. The proposed technique is enlivened by Lai and Tsai in which a new kind of PC workmanship picture, called mystery piece noticeable mosaic picture, was proposed. The mosaic picture is the consequence of the pieces of a mystery picture in mask of another picture called the objective picture preselected from a database. In any case, a conspicuous shortcoming of Lai and Tsai is the prerequisite of an extensive picture database so that the created mosaic picture can be adequately like the chose target picture. Utilizing their technique, the client is not permitted to choose unreservedly his/her most loved picture for utilization at this very moment picture. It is hence fancied in this study to evacuate this shortcoming of the technique while keeping its legitimacy, that is, it is meant to outline another technique that can change a mystery picture into a secret fragment- unmistakable mosaic picture of the same size that has the visual appearance of any unreservedly chose target picture without the need of a database.

At this very moment, Fig. 1 demonstrates an outcome yielded by the proposed strategy. In particular, after an objective picture is chosen discretionarily, the given mystery picture is initially partitioned into rectangular sections called tile pictures, which then are fit into comparable pieces in the objective picture, called target squares, as indicated by a comparability foundation taking into account shading varieties. Next, the shading normal for every tile picture is

changed to be that of the comparing target obstruct in the objective picture, coming about in a mosaic picture which resembles the objective picture. Applicable plans are additionally proposed to lead about lossless recuperation of the first mystery picture from the subsequent mosaic picture. The proposed system is new in that a significant mosaic picture is made, conversely with the picture encryption strategy that just makes aimless commotion pictures. Additionally, the proposed system can change a mystery picture into a camouflaging mosaic picture without pressure, while an information concealing strategy must shroud a profoundly compacted rendition of the mystery picture into a spread picture when the mystery picture and the spread picture have the same information volume.

The proposed strategy incorporates two primary stages presently by the stream chart of Fig.1. 1) mosaic picture creation and 2) mystery picture recuperation. In the first stage, a mosaic picture is yielded, which comprises of the sections of a data mystery picture with shading revisions as per a comparability model taking into account shading varieties. The stage incorporates four stages: 1) fitting the tile pictures of the mystery picture into the objective pieces of a preselected target picture. 2) changing the shading normal for every tile picture in the mystery picture to turn into that of the comparing target obstruct in the objective picture. 3) pivoting every tile picture into a bearing with the base RMSE esteem with deference to its comparing target piece, and 4) implanting important data into the made mosaic picture for future recuperation of the mystery picture.

Fig1. Flow diagram of the proposed method.

Issues experienced in creating mosaic pictures are talked about in this segment with answers for them proposed. Shading Transformations between Blocks In the first period of the proposed strategy, every tile picture T in the given mystery picture is fit into an objective piece B in a preselected target picture. Since the shading attributes of T and B are not the same as one another, how to change their shading circulations to make them resemble the other alike is the primary issue here. Reinhard et al. proposed a shading exchange plan in this angle, which changes over the shading normal for an picture to be that of another in the lαβ shading space. This thought is a response to the issue and is received in this paper, aside from that the RGB shading space rather than the lαβ one is utilized to diminish the volume of the obliged data for recuperation of the first mystery picture.

Picking Appropriate Target Blocks and Rotating Blocks to Fit Better with Smaller RMSE Value In changing the shading normal for a tile picture T to be that of a relating target square B right now, step by step instructions to pick a fitting B for every T is an issue. For this, we utilize the standard deviation of the hues in the square as a measure to choose the most comparable B for every T. Exceptionally, we sort all the tile pictures to frame an arrangement, Stile, and all the target squares to frame another, Starget, as indicated by the normal estimations of the standard deviations of the three shading channels. At that point, we fit the first in Stile into the first in Starget, fit the second in Stile into the second in Starget, etc. Taking care of Overflows/Underflows in Color Transformation After the shading change procedure is led right now portrayed already, some pixel values in the new tile picture may have floods or sub-currents. To manage this issue, we change over such values to be non-flood or non underflow ones and record the worth contrasts presently for utilization in later recuperation. In particular, we change over all the changed pixel values in To not littler than 255 to 255, and each one of those not bigger than 0 to 0. Next, we process the contrasts between the first pixel values and the changed over ones right now and record them presently the data connected with to. As needs be, the pixel values, which are just on the bound of 255 or 0, in any case, can't be recognized from those with flood/undercurrent qualities amid later recuperation since all the pixel values with floods/undercurrents are changed over to be 255 or 0 now.

To cure this, we characterize the residuals of those pixel values which are on the certain to be 0 and record them too. Taking care of Overflows/Underflows in Color Transformation. After the shading change procedure is directed presently portrayed already, some pixel values in the new tile picture may have floods or sub-currents. To manage this issue, we change over such values to be non-flood or non underflow ones and record the worth contrasts presently for utilization in later recuperation. In particular, we change over all the changed pixel values in To not littler than 255 to 255, and every one of those not bigger than 0 to 0. Next, we figure the contrasts between the first pixel values and the changed over ones right now and record them at this very moment the data connected with To. Likewise, the pixel values, which are just on the bound of 255 or 0, nonetheless, can’t be recognized from those with flood/undercurrent qualities amid later recuperation since all the pixel values with floods/undercurrents are changed over to be 255 or 0 now.
mosaic picture, we need to implant important recuperation data into the mosaic picture. For this, we receive a strategy proposed by Coltuc and Chassery and apply it to the minimum huge bits of the pixels in the made mosaic picture to direct information installing.

IV. RESULTS AND DISCUSSION

It can be seen from the figures:2 (a-i) that the created mosaic image retains more details of the target image when the tile image is smaller. It can also be seen that the block ness effect is visible when the image is magnified to be large; but if the image is observed as a whole, it still looks like a mosaic image with its presence similar to the target image. This fact in another way—a mosaic image created with minor tile images has a smaller RMSE value with respect to the target image. At first, we compute the means and standard deviations of T and B, respectively, in each of the three color channels R, G, and B by the following formulas:

\[ \mu_C = \frac{1}{n} \sum_{i=1}^{n} C_i, \quad \mu_C' = \frac{1}{n} \sum_{i=1}^{n} C_i' \]
\[ \sigma_C^2 = \frac{1}{n} \sum_{i=1}^{n} (C_i - \mu_C)^2 = \frac{1}{n} \sum_{i=1}^{n} (C_i' - \mu_C')^2, \]

in which \( C_i \) and \( C_i' \) denote the C-channel values of pixels \( p_i \) and \( p_i' \), respectively, with \( c=r, g, b \) or \( C=R, G, B \).

\[ \text{RMSE} = \sqrt{\text{mean}((d-d_1)^2)} \]

\( d = \text{original image} \)
\( d_1 = \text{noisy image} \)

In order to evaluate the image quality this formula is applied only on luma. The resultant SSIM index is a decimal value between -1 and 1, and value 1 is only reachable in the case of two identical sets of data.

\[ \text{MSSIM} (x,y) = \frac{(2\mu_x \mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y'^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \]

With
\[ \mu_x, \text{ the average of } x; \]
\[ \mu_y, \text{ the average of } y; \]
\[ \sigma_x^2, \text{ the variance of } x; \]
\[ \sigma_y^2, \text{ the variance of } y; \]
\[ \sigma_{xy}, \text{ the covariance of } x \text{ and } y; \]

\( C_1 = (k_1 L)^2, C_2 = (k_2 L)^2 \) two variables to stabilize the division with weak denominator; \( L \) the dynamic range of the pixel-values (typically this is \( 2^{n} \text{per pixel} - 1 \)); \( k_1 = 0.01 \) and \( k_2 = 0.03 \) by default.

Number of experiments have been conducted to test the proposed method by selecting the secret images (i) photo (ii) painting (iii) a document of 8X8, 16X16, 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) The numbers of required bits embedded for recovering the secret image. 3) The RMSE values of the recovered secret image with respect to the original ones. 4) The MSSIM values of secret mosaic images with respect to target images. It can seen from Fig.3(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 Fig.3(b). We can see from Fig.3(d) that the MSSIM value of the created mosaic image with respect to the target image varies from 0.2 to 0.8, which is not good enough, but this is not the main concern of the proposed method because our goal is to create globally visually similar mosaic image which contains a secrete image.
floods and undercurrents in the changed over estimations of the pixels’ hues, mystery fragment visible mosaic pictures with high visual similitude’s to discretionarily chose target pictures can be made with no need of an objective picture database. Additionally, the first mystery pictures can be recuperated almost losslessly from the made mosaic pictures. Great exploratory results have demonstrated the practicality of the proposed strategy. Future studies may be coordinated to applying the proposed strategy to pictures of shading models other than the RGB.

VI. REFERNCES


V. CONCLUSION

Another secure picture transmission strategy has been proposed, which not just can make significant mosaic pictures in any case, additionally can change a mystery picture into a mosaic one with the same information size for utilization as a cover of the mystery picture. By the utilization of fitting pixel shading changes and also a dexterous plan for taking care of