An Algorithm Based On Secret-Fragment-Visible Mosaic Images For Secure Image Transmission Using Pixel Color Transformations

K.NAGA JYOTHI (PG Scholar)¹

J.S.S.RAMA RAJU (M.Tech)²

¹Department of ECE, Bhimavaram institute of Engineering and technology, JNTU (KKD)

²Assistant Professor, Department of ECE, Bhimavaram institute of Engineering and technology, JNTU (KKD)

Abstract

Digital image processing is the domain to hide the data in digital images. Recently, so many data hiding techniques have been used. But most of the techniques failed to meet the major requirements. This paper presents an approach to meet the major requirement and for that the secret image is generated as the mosaic image. Here the secret image is divided into fragment tiles and the target image is divided into blocks. Secret image fragments are transforming their respective color characteristics into corresponding blocks of the target image. By using this pixel color transformation helps to get the lossless recovered image based on the untransformed color space values. Key generated in the code also helps to get the lossless data from the secret image. This same approach is performed on the videos to get the lossless data from the motion related videos.

INTRODUCTION

These days’ images are more frequently transmitted through the internet from one source to other, as a purpose of online photograph, documents storage, medical images, some confidential data and mainly military information. There is no security for this to protect them from leakage or data damage. To secure this data loss there are two proposed image transmission methods, image encryption and data hiding. Image encryption is a technique 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 they have the correct key. But, the encrypted image is a meaningless file, which cannot provide any information before decryption. To avoid this problem is data hiding that hides a secret message into a cover image so that no one can know the existence of the secret data.
This method causes the distortion of the result image causing the payload of the cover image.

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. 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. This process is controlled by a secret key, and only with the key a person can recover the secret image without any loss of data from the mosaic image. The mosaic image is the result of rearrangement of the fragments of a secret image in disguise of another image called the target image.

![Fig.1. Result of the proposed method. (a) Secret image. (b) Target image. (c) Secret-fragment-visible mosaic image created from (a) and (b) by the proposed method.](image)

Here, Fig. 1 shows a result of the proposed method. Once a target image is selected arbitrarily, the given secret image is first divided into rectangular fragments called tile images, which are then 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. 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.

**PROPOSED METHOD**

First we need to match the color transformations, for that initially the secret image is divided into tile image is match into a target image target blocks. Since the color characteristics of tile image and target block are totally different from one another, we need to make them look alike, for that converts the color characteristic of an image. Target blocks and tile images are described as 2 pixel sets, and the color of every pixel is denoted by RGB. First we need to find the mean and standard deviation of this tile
image and target block. Next, we compute the new color values for these pixels. Here it will be verified that the new color mean and variance of the resulting tile image is equal to that of target block.

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

In transforming the color characteristic of a tile image $T$ to be that of a corresponding target block $B$ as 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, $S_{tile}$, 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 image $T$ and the target block $B$ by rotating $T$ into one of the four directions, $0^\circ$, $90^\circ$, $180^\circ$, and $270^\circ$, 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 $B$.

**Extracting 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. Specifically, the method conducts forward and backward integer transformations.

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 $B$ and the standard deviation quotients, of all color channels; and 4) the overflow/underflow residuals.
FLOW DIAGRAM

In this proposed method it contains two phases they are mosaic image creation and secret image recovery process.

PHASE 1 Mosaic image creation

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

Step 1: here first we need to divide the secret image into tile images T and also the target image as target blocks B and with each T B belongs to size of N.

Step 2: then calculate the both mean and standard deviation for each tile image T and target image B.

Step 3: now we have the set of tile images as $S_{tile}$ and target blocks are $S_{target}$ 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.

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 calculate the RMSE values in F with respected to corresponding target block B after rotating T into directions 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.

Step 2: repeat the above step to extract the number of iterations embedded $M_i$.

Step 3: and decrypt the bit stream $M_i$ by the use of key K.

Step 4: Decompose $M_i$ 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 $M_i$ for each tile image T to obtain the index, mean, standard deviation values.

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

RESULTS

Figure 1: Original image

Figure 2: Secret image

Figure 3: before embedding mosaic image

Figure 4: after embedding mosaic image
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 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.
CONCLUSION

A new method for secure image transmission has been proposed which creates meaningful mosaic images and transforms a secret image into a mosaic one with the same data size. With the help of pixel color transformation as well as a skilful scheme for handling overflows and underflows in the converted values of the pixel color, secret-fragment visible mosaic images with very high visual similarities to arbitrarily-selected target images can be created without the need of a target image database. The experimental results have shown the feasibility of the proposed method. Finally the same approach can be performed on videos which help to eliminate the flickering to achieve the lossless data recovery in motion related videos.

REFERENCES