A Review of New Secure Image Transmission Technique via Secret-Fragment-Visible Mosaic Images by Nearly Reversible Color

Dr. Giriraj Kumar Prajapati*
Professor, Mechatronics and Robotics Automation Department, Parul University, Vadodara, Gujarat, India
Prof. Dr. Ashok Kumar Gupta
Professor Satpuda College of Engineering & Polytechnic Balaghat, M.P., India

Abstract—

A new technique of transmitting an image securely over any channel is proposed. This technique automatically transforms a given secret image into a secret-fragment-visible mosaic image.The mosaic image, which definitely looks similar to an arbitrarily selected target image and can be used as a camouflage of the secret image. This is yielded by dividing the secret image into fragments and transforming their color characteristics to be those of the corresponding blocks of the divided target image. Highly skillful techniques are employed to conduct the color transformation process so that the secret image may be recovered nearly lossless. The information required for recovering the secret image is embedded into the created mosaic image by a nearly lossless data hiding scheme using a key. The key can be sent to the recipient in a secure manner. The experimental results on various secret and target images show that the proposed method is highly feasible. A plan of taking care of the floods/undercurrents in the changed over pixels' shade values by recording the color contrasts in the untransformed shade space is additionally proposed. The data needed for recuperating the mystery Images is inserted into the made mosaic Images by a lossless information concealing plan utilizing a key. Great exploratory results demonstrate the attainability of the proposed system.

Key Words — Data hiding, Image encryption, Key encryption, Mosaic image, Reversible color transformation, Secure image transmission, Secret image.

I.INTRODUCTION

Images from various sources are frequently used and transmitted through the internet for various applications, such as online personal photographic albums, confidential enterprise data, document storage systems, bio medical imaging systems, and military secrecy image databases. These images usually contain highly private and confidential information such that they should be protected from leakages and hacking during transmissions. Recently, several methods have been proposed for secure image transmission, for which two common techniques are encryption and data hiding. Image

encryption is a technique that makes use of the inherent natural properties 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 an entirely meaningless file, which cannot provide additional information before decryption and may arouse a hacker's attention during transmission due to its randomness in form. An alternative solution to avoid this problem is data hiding that hides a secret message into a cover image so that no one can realize, at any cost the existence of the secret data, in which the data type of the secret message is investigated in this paper is an image. The existing data hiding methods mainly utilize the techniques of LSB substitution, 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 evaluated upper bound for the distortion value is usually set on the selected cover image. For example, for a data hiding method with an embedding rate of 0.6 bits per pixel, a secret image with 8 bits per pixel must be compressed at a rate of at least 94% beforehand in order to be hidden into a cover image. But, for many applications, such as keeping or transmitting Medical, 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 [3], are not suitable for line drawings and textual graphics, in which slightly sharp contrasts between adjacent pixels are often destructed to become noticeable artifacts [1]. In this paper, a new and latest technique for secure image transmission is proposed, which transforms a selected secret image into a meaningful mosaic image with the same size and looking like a preselected target image [3]. The transformation process is controlled by a secret key, and only with the key can a person recover the secret image nearly lossless from the mosaic image. The proposed method is totally new in that a meaningful mosaic image is created, which is in contrast with the image encryption method that only creates meaningless noise images. Also, the proposed method can transform totally a secret image into a totally disguising mosaic image without compression, while a data hiding or encryption method must hide a highly compressed version of the secret image into a cover image when the secret image and the cover image have nearly the same data volume.

II. PROPOSED METHODOLOGY

It involves two main phases. 1) Mosaic Image Creation, 2) Secret Image Recovery. The Proposed Method In the first step, a new mosaic image is yielded, which consists of the fragments of an input secret image with color transformation according to a similarity condition based on color variations. The step includes four stages: 1) fitting the tile images of the secret image into the target blocks of a preselected target

image; 2) transforming the color characteristic of each square shaped tile image in the secret image to become that of the corresponding target block in the target image; 3) embedding sufficient information into the created mosaic image for future recovery of the secret image. In the next phase, the embedded information is extracted to recover nearly losslessly the secret image from the generated mosaic image. The step includes two stages: 1) extracting the embedded information for secret image recovery from the selected mosaic image, and 2) successfully recovering the secret image using the extracted information.

2.1 Color transformations

Color can be described by its red (R), green (G) and blue (B) coordinates (the well-known RGB system), or by some its linear transformation as XYZ, CMY, YUV, IQ, among others. The CIE adopted systems CIELAB and CIELUV, in which, to a good approximation, equal changes in the coordinates result in equal changes in perception of the color. Nevertheless, sometimes it is useful to describe the colors in an image by some type of cylindrical-like coordinate system, it means by its hue, saturation and some value representing brightness. If the RGB coordinates are in the interval from 0 to 1, each color can be represented by the point in the cube in the RGB space.

2.2 **Image Encryption Techniques**

Due to the rapid growth of digital communication and multimedia application, security becomes an important issue of communication and storage of images. Encryption is one of the ways to ensure high security images are used in many fields such as medical science, military.Modern cryptography provides essential techniques for securing information and protecting multimedia data. In recent years, encryption technology has been developed quickly and many image encryption methods have been used to protect confidential image data from unauthorized access .In this paper survey of different image encryption techniques have been discussed from which researchers can get an idea for efficient techniques to be used.With the ever-increasing growth of multimedia applications, security is an important issue in communication and storage of images, and Encryption is a common technique to uphold image security. Image encryption techniques try to convert original image to another image that is hard to understand; to keep the image confidential between users, in other word, it is essential that nobody could get to know the content without a key for decryption.

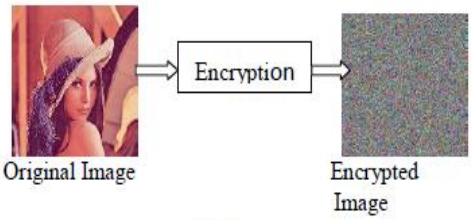


Fig.1

2.3 Techniques for data Hiding

Data hiding, a form of steganography, embedsdata into digital media for the purpose ofidentification, annotation, and copyright. Severalconstraints affect this process: the quantity ofdata to be hidden, the

need for invariance of thesedata under conditions where a “host” signal issubject to distortions, e.g., lossy compression,and the degree to which the data must be immuneto interception, modification, or removal by a thirdparty. We explore both traditional and noveltechniques for addressing the data-hiding processand evaluate these techniques in light of three
applications: copyright protection, tamperproofing,and augmentation data embedding.

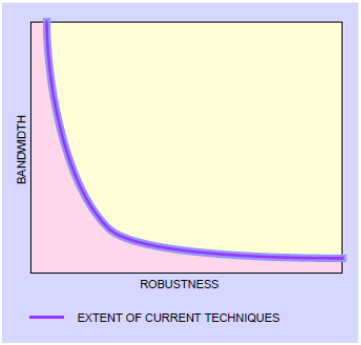


Figure 2 Conceptual data-hiding problem space

2.5 Data hiding in still images

Data hiding in still images presents a variety of challengesthat arise due to the way the human visual system(HVS) works and the typical modifications thatimages undergo. Additionally, still images provide arelatively small host signal in which to hide data. Afairly typical 8-bit Images of 200 ´ 200 pixels providesapproximately 40 kilobytes (kB) of data spacein which to work. This is equivalent to only around 5seconds of telephone-quality audio or less than a single frame of NTSC television.

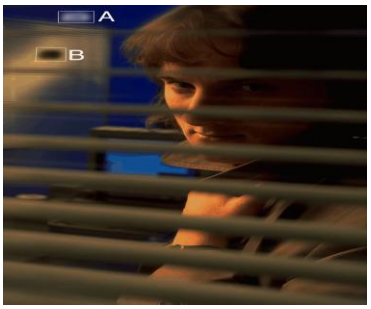


Figure 3A single iteration in the Patchwork method (photograph courtesy of Webb Chapel

Table 1 Degree of certainty of encoding given deviation from that expected in a Gaussian distribution ($\delta = 2$)

Standard Deviations Away	Certainty	n
0	50.00%	0
1	84.13%	679
2	97.87%	2713
3	99.87%	6104

III. MOSAIC IMAGE GENERATION

Some of the ideas of mosaic image generation are discussed here.

A. Applying Color Transformations In the first stage of the proposed method, each of the tile image T in the given/selected secret image is fit into a target block B in a preselected target image. Since the color characteristics of target T and block B are different from each other, how to change their color characteristics distributions such that to make them look alike is the main issue here. Reinhard et al. proposed a color transfer scheme in this aspect, which converts the color characteristic of a selected image to be that of the one in the lαβ color space. This idea is an answer to the issue and has been adopted in this paper, except that the RGB color space instead of the lαβ

one is used to reduce the volume of the required information for recovery of the original secret image.

B. Choosing Appropriate Target Blocks In transforming the color characteristic of a tile image T to be that of a corresponding target block B as described above, how to choose an appropriate B for each T is a problem. Specially, we sort all the tile images to form a sequence, S_tile, and all the target blocks to form another, S_target. Then, we fit the first in S_tile into the first in S_target, fit the second in S_tile into the second in S_target, and so on.

C. Embedding Information In order to successfully recover the secret image from the selected mosaic image, we have to embed relevant necessary recovery information into the mosaic image. For this, we implement a unique technique proposed by Cultic and Chassery [3] and apply it to the least significant bits of the pixels in the created mosaic image to conduct data embedding. Highly unlike the classical LSB replacement methods, which substitute LSBs with message bits directly, the reversible contrast mapping method applies simple integer transformations to pairs of pixel values. Specifically and iteratively, the method conducts forward and reverse integer transformation as follows, respectively, in which (x, y) are a pair of pixel values and (x', y') are the transformed ones.

IV. ALGORITHM

The detailed algorithms for creation of mosaic images and the recovery of secret images are given below. They are treated as Algorithm 1 and Algorithm 2. A. Algorithm1: Creation of Mosaic Image: Input: A selected secret image S, a selected target image T, and a secret key K. Output: a secret- mosaic image F. Steps:

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

Step 1: If the size of the target image T is different from that of the secret image S, change such that the size of T to be identical to that of S; and divide the secret image S into n tile images {T1, T2, . . . , Tn} as well as the target image T into n target blocks {B1, B2, . . . , Bn} with each Ti or Bi being of size NT.

Step 2: Evaluate the means and the standard deviations of each tile image Ti and each target block Bj for the three color channels; and evaluate accordingly the average standard deviations for Ti and Bj , respectively, for i = 1 through n and j = 1 through n.

Step 3: Sort the tile images in the set S_tile = {T1, T2, . . . ,Tn} and the target blocks in the set S_target = {B1, B2, . . . , Bn} map in order the blocks in the sorted Stile to those in the sorted S_target in a 1-to-1 manner; and if necessary reorder the mappings according to the indices of the tile images, resulting in a mapping sequence L of the form: T1 → Bj1 , T2 → Bj2 , . . . , Tn → Bjn .

Step 4: Now create a mosaic image F by fitting all the tile images into the corresponding target blocks. Stage 2. Performing color conversions between the tile images and the target blocks.

Step 5. Create a new table with 256 entries, each of which with an index corresponding to a listed residual value, and assign an initial value zero to each of the entry.

Step 6. For each mapping Ti →Bji in a sequence L, represent the means of Ti and Bji, respectively, by eight bits; and represent the standard deviation quotient by seven bits, where c = r, g, or b.

Step 7. For each pixel pi in each tile image Ti of mosaic image F with color value ci where c = r, g, or b, transform ci into a new value cii; if cii is not smaller than 255 or if it is not larger than 0, then change cii to be either 255 or 0; Stage 3. Embedding the secret image recovery information.

Step 8. Construct a table HT using the content of the counting table TB to encode all the values computed previously.

Step 9. For each tile image Ti in mosaic image F, construct a bit stream Mi for recovering Ti including the bit-segments which encode the data items of: 1) the index of the corresponding target block Bji; 2) the optimal rotation angle θ° of Ti; 3) the means of Ti and Bji and the related standard deviation quotients of all three color channels;

Step 10. Concatenate the bit streams Mi of all Ti in F in a raster-scan order to form a total bit stream Mt; use the secret key K to encrypt Mt into another bit stream Mti

Step 11. Construct a bit stream I including: 1) the number of conducted iterations Ni for embedding Mt; 2) the number of pixel pairs Npair used in the last iteration; and 3) The table HT constructed for the residuals; and embed the bit stream I into mosaic image. Stage 3. Embedding the secret image recovery information

Step 12: Embedded sufficient information into the target block. Then generate a key based on any of the properties of the image. The key can be based on the rmse value, mean or standard deviation of the embedded blocks. B. Recovery of the secret image Input: A mosaic image F with n tile images {T1, T2, . . ., Tn} and the secret key K. Output: The secret image S. Stage 1. Extracting the secret image from the mosaic image. Step 1: For the selected mosaic image, the first step is to extract the bit stream I by a reverse version of the scheme proposed in [14] and decode them to obtain the following: 1) the number of iterations Ni for embedding Mt; 2) the total number of used pixel pairs Npair in the last iteration; and 3) the table HT for encoding the values of the residuals of the overflows or underflows. Step 2. Extract the bit stream Mt using the values of Ni and Npair by the same scheme used in the last step. Step 3. Decrypt the bit stream Mt into Mt by K. Step 4. Decompose Mt into n bit streams M1 through Mn for the n to-be-constructed tile images T1 through Tn in S, respectively. Step 5. Decode Mi for each tile image Ti to obtain the following:

V. SECURITY ISSUES

In order to increase the security of the proposed system, the embedded information for later recovery is encrypted with a secret key as given in the Algorithm 1 and only the receiver who has the key can decode the secret image. However, a hacker who does not have the key may still try to find all

possible permutations of the tile images in the mosaic image to get the original secret image back. The number of all possible permutations is n!, and hence the probability for the hacker to correctly guess the permutation is p=1/n! which is very small in value. For e, for the typical case in which we divide a secret image of size 1024×768 into tile images with block size 8×8, the value n is (1024×768)/(8×8) = 12,288. So the probability to guess the permutation correctly without the key is 1/n! = 1/ (12,288!). Hence breaking away the system by this way of guessing is computationally infeasible... In order to increase the security of the proposed method against this type of attack, one of the possible ways is to use the key to randomize [2] important information of a selected secret image, such as the actual positions of the pixels in the secret image, before transforming the selected secret image into a new mosaic image by the proposed method. As a result of this, only authorized users with the key can know the correct secret image while a hacker cannot at any cost.

VI. RESULTS ANALYSIS

Experimental results on various randomly selected secret and target images have shown the accuracy of the proposed method.Another secure Images transmission technique has been proposed, which not just can make genuine mosaic Imagess at the same time likewise can change a mystery Images into a mosaic one with the same information size for utilization as a disguise of the mystery Images. By the utilization of fitting pixel color changes and an adroit plan for taking care of floods and undercurrents in the changed over estimations of the pixels' colors, mystery fragment visible mosaic Imagess with high visual similitude's to subjectively chose target Imagess can be made with no need of a target Imagesdatabase. Likewise, the first mystery Images can be recouped about losslessly from the made mosaic Imagess

Figure 3 As δ or n increases, the distribution of S'_n shifts further to the right.

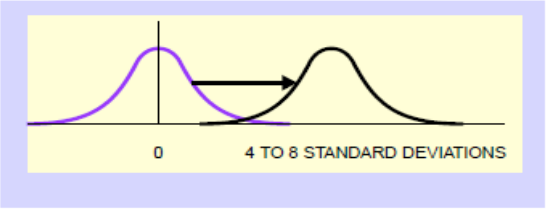


Figure 4 The contour of a patch largely determines which frequencies will be modified by the application of Patchwork.

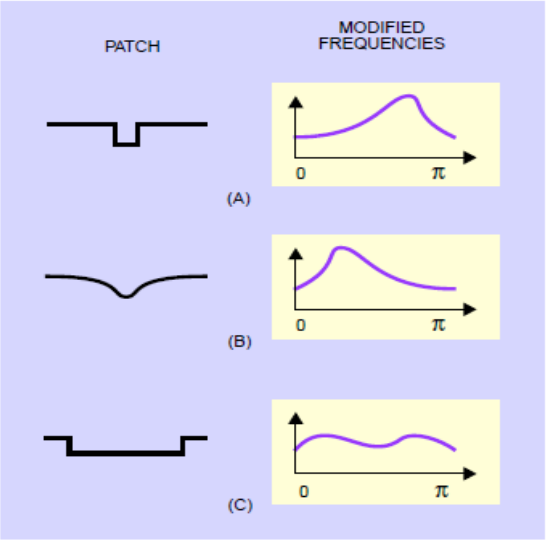


Figure 5 Patch placement affects patch visibility.

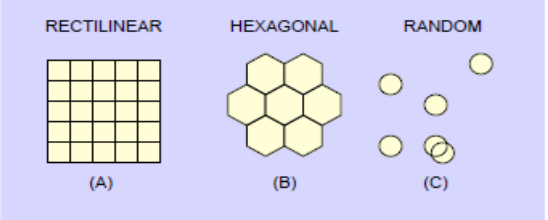


Figure 6 A histogram of Figure 2 and its autocorrelation

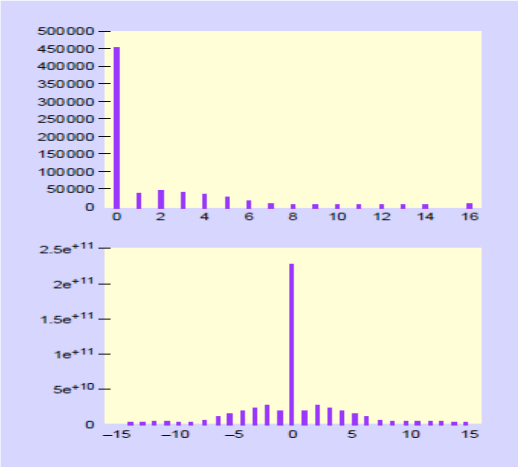
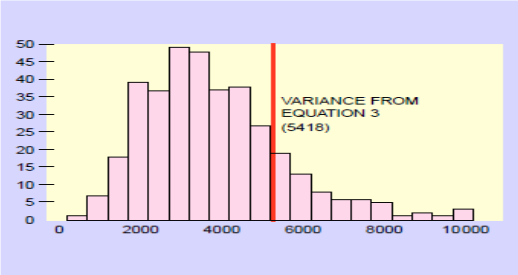


Figure 7 A histogram of the variance of the luminance of 365 Associated Press photos from March 1996



A series of experiments have been conducted to test the proposed method using many secret and target images with varying sizes. The algorithm is implemented in Matlab 2013. To show that the created mosaic image looks like the preselected target image, the quality metric of root mean square error (MSE) is utilized, which is defined as the square root of the mean square difference between the pixel values of the two images.

VII. CONCLUSIONS

In this paper a new secure image transmission method has been proposed, which not only can create mosaic images but also can transform a given secret image into a mosaic one with the same data size for use as a cover of the secret image. By the use of appropriate pixel color transformations as well as a skillful technique for embedding secret information in the converted values of the pixel intensity colors, secret and fragment visible mosaic images with very highly similar visual characteristics to arbitrarily-selected target images can be created with no need of a prior target image database. Also, the original secret image can be recovered almost nearly lossless from the mosaic images created. Great test results have demonstrated the plausibility of the proposed technique. Future studies may be guided to applying the proposed technique to Images of shade models other than the RGB.

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.