International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

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

[1]M.Kiranmai
M.Tech., Department Of Ece, Sree Shiridi Sai Institute Of Science And Engineering Anantapur.
[2]Y.Raghuram Prasad
Associate Professor And Hod, Department Of Ece, Sree Shiridi Sai Institute Of Science And Engineering Anantapur.

Abstract

A new secure image transmission technique is proposed, which transforms automatically a given large-volume secret image into a so-called secret-fragment-visible mosaic image of the same size. The mosaic image, which looks similar to an arbitrarily selected target image and may be used as a camouflage of the secret image, is yielded by dividing the secret image into fragments and transforming their color characteristics to be those of the corresponding blocks of the target image. Skillful techniques are designed to conduct the color transformation process so that the secret image may be recovered nearly loss less. A scheme of handling the overflows/underflows in the converted pixels' color values by recording the color differences in the untransformed color space is also proposed. The information required for recovering the secret image is embedded into the created mosaic image by a lossless data hiding scheme using a key. Good experimental results show the feasibility of the proposed method.

Index Terms—Color transformation; data hiding; image encryption; mosaic image; secure image transmission

INTRODUCTION

Today, images from various sources are frequently utilized and transmitted through the internet for various applications, such as online personal photograph albums, confidential enterprise archives, document storage systems, medical imaging systems, and military image databases. These images usually contain private or confidential information so that they should be protected from leakages during transmissions. Now a day, many methods have been proposed for securing image transmission, for which two common approaches are image encryption and data hiding.

Encryption of an image is a procedure which use the natural properties of images, such as redundancy and spatial correlation, to get an image already encrypted which use the Shannon's confusion and diffusion properties. The image that is encrypted becomes an image with noise so that no one can obtain the transmitted secret image from it unless having the correct key. But, the encrypted image still is a meaningless document, which cannot give more information before the decryption is done. Thus, this may evoke an attacker's attention during the transmission of the image because of it arbitrary in nature.

Another possibility to avoid this problem is hiding of data that conceals a secret message into another image so that noon can anticipate the survival of the secret text, in which the type of data of the secret message that is examined in this paper is an image. The methods of data hiding already known mostly use the techniques such as LSB substitution, histogram shifting, recursive histogram modification, discrete cosine/wavelet transformations etc. However, in order to reduce the distortion of the resulting image, an upper bound forth distortion value is usually set on the payload of the cover image.

Thus, the main limitation of them methods for data hiding in images is the difficulty in embedding a huge amount of message data into on image. Specifically, if one wants to hide a secret image into another image with the same size, the secret image must be highly compress Edina dance. For example, foradatahidingmethodwithanembeddingrateof0.5bits per pixel, a secret image with 8bits per pixel must be compress data rate of atleast93.75%before hand 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.

REVIEWOFLITERATURE

This section describes the various existing schemes which are compared in this paper.

Color Model In this paper, Ya-Lin Lee shows a technique for the transmission of the secret image securely and lossless. This method transforms the secret image into a mosaic tile image having the same size like than to the target image which is preselected from a data base. This color transformation is controlled and the secret image is recovered lossless from the mosaic tile image with the help of the extracted relevant information generated for their covey of the image. Images from various sources are frequently used and are transmitted through the internet for various applications, such as confidential enterprise archives, document storage systems, medical imaging systems, and military image databases. These images may contain private or confidential information so that they should be protected from leakages during transmissions is needed, to transform a secret image in toone meaningful Mosaic tile image with size almost the same and looking like one target image. The mosaic image is the outcome of arranging of the tile fragments of a secret image indifferent way so as to disguise the other image called the target image which is already selected from a database.

The mosaic image, which looks similar to a randomly selected target image, which is used for hiding of the secret image by color transforming their characteristics similar to the tile fragments of the target image. Such technique is necessary so for the lossless recovery of the transmitted secret image. The relevant information embedded into the mosaic image is required for the recovery of the transmitted secret image.

Flow Diagram of securely Transfer a Secret Image

The embedding of text into secret image by Data Hiding, the embedding of secret image into the target image in tile form and maintaining the visibility of the original target image. The proposed method includes

1) Mosaic tile image creation

2) Secret image and secret text recovery

The result is the mosaic tile image, which consists of the tile fragments of an input secret image which has color characteristics same as that of another target image selected from the database.

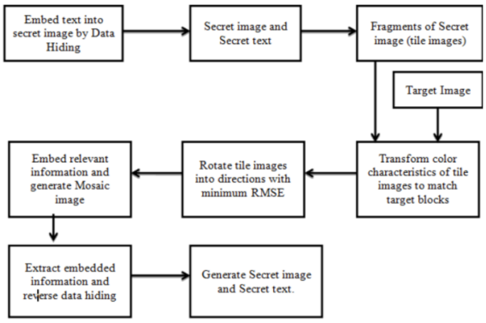

Embed text into secret image by Data Hiding
Secret image and Secret text
Fragments of Secret image (tile images)
Target Image
Transform color characteristics of tile images to match target blocks
Rotate tile images into directions with minimum RMSE
Embed relevant information and generate Mosaic image
Extract embedded information and reverse data hiding
Generate Secret image and Secret text.

Fig : Flow Diagram

Hyper-chaos Based Image Encryption Algorithm

In the proper, Chen zaiping, Li haifen, Dong enzeng, Du yang developed A Hyper-chaos Based Image Encryption Algorithm developed in 2010. Inside this paper present a new image encryption algorithm, within this algorithm, shuffling matrix and diffusing matrix are generate. This is based on Chen‟s hyper-chaotic system. Firstly, the Chen‟s hyper-chaotic system is use to shuffle the position of the image pixels, and then use Chen‟s hyper-chaotic system to confuse the relationship between the original image and the cipher image. Within this paper, a new image encryption algorithm based on hyper-chaos is proposed, it uses an image shuffling matrix to shuffle the pixel positions of the plainimage and then the states combination of hyper-chaos is used to change the grey values of the shuffled-image. Some security analysis such as key space analysis, key sensitivity analysis, and correlation analysis of two adjacent pixels is given to show that the proposed cryptosystem has a high security level.

Secret sharing technique

A Novel Image Secret Sharing Scheme, Prabir Kr. Naskar, AyanChaudhuri, DebaratiBasu, AtalChaudhuri, [3] Secret sharing is a technique for protecting sensitive data, such as cryptographic keys, precisely during transmission over internet. Secret sharing is a technique for protecting sensitive data, such as cryptographic keys, precisely during transmission over internet. Leading to high computational complexity during both sharing and reconstructing phase and most of the popular secret sharing schemes are based on above schemes. Apart from those secret sharing technique, we are suggesting a scheme which deploys simple graphical masking, done by simple ANDing for share generation and reconstruction can be done by simple ORing the qualified set of shares. Not only that, it generates compressed shares that lead to strong protection of the secret image. Nevertheless it confirms confidentiality and integrity as well. This scheme is highly useful where low end processors are used but security is a major challenge.

Image Cryptography

The Genetic Algorithm Approach, Sandeep Bhowmik, SriyankarAcharyya, to protect our data against unauthorized access, from the time immemorial the first choice has always been to use cryptography. The effectiveness of the protection through encryption depends on the algorithm applied and as well as on the quality of the „key‟ used. If a „key‟ is badly designed or haphazardly selected, obviously the protection fails to provide proper security and improper access can be gained on the secured information. The first algorithm in cryptographic system design is the algorithm to generate „key‟. It specifies the manner in which the „key‟ is to be chosen. This work focuses on a totally new approach towards the „key‟ generation for encryption algorithms. Here, Genetic Algorithm (GA), an important method of artificial intelligence has been applied to generate encryption „key‟, which plays a vital role in any type of encryption. In our work, a hybridized technique called BlowGA is also proposed which is a combination of Blowfish and GA. Blowfish Algorithm is a conventional method of encryption. Our experimental observations show that the newly-proposed hybridized method BlowGA outperforms both GA and Blowfish Algorithm.

EXISTING SYSTEM

3.1 EXISTING SYSTEM

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.

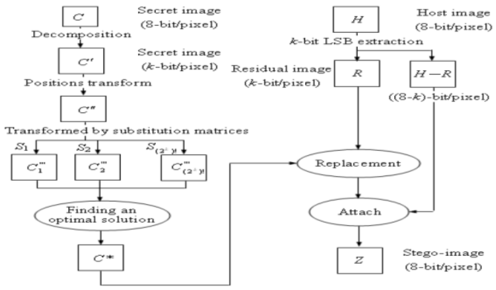
An alternative to avoid this problem is data hiding that hides a secret message into a cover image so that no one can realize the existence of the secret data, in which the data type of the secret message investigated in this paper is an image. Existing data hiding methods mainly utilize the techniques of

- LSB substitution,
- Histogram shifting,
- Difference expansion,
- Prediction-error expansion,
- Recursive histogram modification
- Discrete cosine/wavelet transformations.

LSB SUBSTITUTION

LSB Substitution Scheme

Using simple LSB substitution, the rightmost k least significant bits of H will be replaced by C. k is denoted as the length of LSB, i.e., |LSB| = k. C′ is defined by decomposing the bit streams of C into several k-bit units and treating each unit as a single pixel. Also, let R be the k-bit residual image, which is derived by extracting the rightmost k least significant bits from eachpixel in the host image H. To increase security, the pixel location of C′ is randomized bya bijection (i.e., one-to-one and onto) mapping function into a meaningless image C″. In order to achieve a good embedding result, an N × N substitution matrix S = {sij} is defined by where *N* = 2*k*. The substitution matrix *S* is used to replace each pixel with gray value *i* in Here *zl*, *hl*, , *l c'''* and *rl* represent the pixel gray values of the stego-image *Z*, host image \result (*i.e.*, the result with the minimum *MSE*) in their scheme.



A data hiding scheme by simple LSB substitution

A data hiding scheme by simple LSB substitution is proposed. By applying an optimal pixel adjustment process to the stego-image obtained by the simple LSB substitution method, the image quality of the stego-image can be greatly improved with low extra computational complexity.

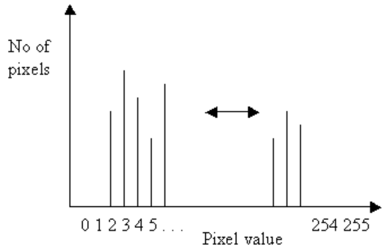
Further proposed a data hiding scheme by optimal LSB substitution and genetic algorithm. Using the proposed algorithm, the worst mean-square-error(WMSE) between the cover-image and the stego-image is shown to be 12of that obtained by the simple LSB substitution method. In this paper, a data hiding scheme by simple LSB substitution with an optimal pixel adjustment process (OPAP)is proposed.

The Transforming LSB Substitution Scheme

In this redefine the LSB substitution scheme proposed by Wang *et al.* [8] in a more general situation. Let the secret image *C* form a bit string *S* = *s*0*s*1…*sn*-1, where *n* is the number of secret bits and *s*i represents a bit, for *i* = 0, 1, 2, …,*n* − 1. For the *k*-bit simple LSB substitution approach, the bits in host image *H*, which will be replaced by the bit string *S*, form a bit string *R* = *r*0*r*1…*rn*-1. We will refer to the bit string *S* as the secret string and to the bit string *R* as the replaced string. Each bit *si*in *S* will replace the bit *ri*in *R*. The value of *k* is usually equal to 1, 2, 3, or, 4 and each of the *k* adjacent bits of *R* in come from the same pixel of the host image. The idea of Wang *et al.*'s LSB substitution scheme is that each *k*-bit string of *S* is transformed into another *k*-bit string before replacing *R*. Then we extend the *k*-bit string to the *l*-bit string, denoted as the matching string, where *l* ≥ *k*. *l* is the length of a matching string. As shown in Fig. 2, each *l*-bit string of *S* will be transformed into another *l*-bit string before replacing *R*, therefore we call our new scheme as the *l*-bit transforming LSB substitution scheme. Note that the LSB substitution scheme proposed by Wang *et al.* is a special case of our new scheme with *l* = *k*.

HISTOGRAM SHIFTING

Each pixel contained in a digital photograph can have a value between 0 and 255. When the number of pixels having a value of 0, 1, 2 …. 255, are plotted against the pixel value, we get the histogram as shown below:



Pixels on the left of the graph represent the dark areas in the photograph, whilst the pixels on the right side of the graph represent the bright areas in the photograph.

This simulation program allows the user to shift the value of all the pixels to the right or left on the histogram graph. It is done by using the slider or by pointing to any position on the graph and dragging it to the left or to the right. The brightness of the image will change accordingly.

Histogram-Shifting-Based Reversible Data Hiding

Histogram shifting (HS) is a useful technique of reversible data hiding (RDH). With HS-based RDH, high capacity and low distortion can be achieved efficiently. In this paper, we revisit the HS technique and present a general framework to construct HS-based RDH. By the proposed framework, one can get a RDH algorithm by simply designing the so-called shifting and embedding functions.

The modified histogram shifting method proposed best method of reversible watermarking. The shifting of pixels are more in method. Even method of modified histogram shifting has less embedding capacity and do not provide enough quality for general purpose image. Our forward modified histogram shifting method overcomes all. Generally PSNR decreases when embedding capacity increases and shifting pixels also increases. But our modified histogram shifting method optimizes all these factors.

Our forward modified histogram shifting method shifts required pixel values to right by 'n-1' numbers. 'n-1' may be 1,2,3 and so on. This also increases embedding capacity approximately to (n-1) time's maximum number of pixels in the histogram. The complexity of our forward modified histogram shifting method is same as that of Hong et. al. (2010) modified histogram shifting method as both scans image twice during processing.

PREDICTION-ERROR EXPANSION

In prediction-error expansion (PEE) based reversible data hiding, better exploiting image redundancy usually leads to a superior performance. However, the correlations among prediction-errors are not considered and utilized in current PEE based methods. Specifically, in PEE, the prediction-errors are modified individually in data embedding. In this paper, to better exploit these correlations, instead of utilizing prediction-errors individually, we propose to consider every two adjacent prediction-errors jointly to generate a sequence consisting of prediction-error pairs. Then, based on the sequence and the resulting 2D prediction-error histogram, a more efficient embedding strategy, namely, pairwise PEE, can be designed to achieve an improved performance. The superiority of our method is verified through extensive experiments.

Unlike conventional PEE which embeds data uniformly, we propose to adaptively embed 1 or 2 bits into expandable pixel according to the local complexity. This avoids expanding pixels with large prediction-errors, and thus, it reduces embedding impact by decreasing the maximum modification to pixel values. Meanwhile, adaptive PEE allows very large payload in a single embedding pass, and it improves the capacity limit of conventional PEE. We also propose to select pixels of smooth area for data embedding and leave rough pixels unchanged.

Reversible Watermarking Based on Prediction Error Expansion and Pixel Selection on Color Image

Reversible watermarking enables embedding of valuable information in a host signal with no loss of host information. The conventional PEE exploit the similar inherent in the neighborhood of pixel that the difference expansion scheme. In our proposed system, the PEE technique is further investigated and an resourceful reversible watermarking scheme is deduced by incorporating in PEE two new techniques, namely, adaptive embedding and pixel selection. PEE technique embeds data consistently, using Embedded Zerotree Wavelet (EZW), Bit-plan Complexity Segmentation (BPCS) based embedding is applied to embed on natural images. This avoids expanding pixels with huge prediction errors likewise it also reduces embedding impact by diminishing the maximum modification to pixel values. We as well put forward to selecting pixels of smooth area for data embedding and leave the rough pixels unchanged. In our method a more penetratingly effective method for data embedding and a better visual quality of watermarked image is observed.

It is used for copyright protection, authentication. In application reversible watermarking is used in military, medical and source tracking. This enable the decoder extract the watermarking image and reconstruct the original host image from the watermarked image. In our proposed method the image is divided into two parts called flat region and rough region by selecting the region of interest. The selected region was grown according to the adaptive threshold value then the grown region was masked with the original image to identify the flat region then the flat region was cropped to embed the watermark. Finally the watermark signal was generate by using the two techniques called Bit-plane Complex Segmentation (BPCS) and Embedded Zerotree Wavelet (EZW).

Embedding Architecture of Reversible Watermarking Based on Prediction Error Expansion

In the proposed system the PEE technique is further investigated and an efficient reversible watermarking is produced by incorporating PEE in two new strategies, namely, adaptive embedding and pixel selection. Our proposed method has two stages of embedding they are EZW (Embedded Zerotree Wavelet), BPCS

(Bit-Plane Complexity Segmentation). Before embedding the image was firs split into two regions namely flat region and rough region. Then the flat region was chose to embed the watermark signal. For select the flat region and rough region we use the ROI. The region was grown according to the adaptive threshold value. Then the grown region was masked with the original image to indentify flat region then the flat region was cropped for used for the further operations. Then apply the BPCS and EZW techniques were used to embed the water mark. Then the histogram was calculated for both the original image and Embedded image to identify the distortion between them.

Embedding procedure

Before embedding the watermark into an we define region of interest (ROI) by taking the smallest area around an image. This border will be used for our watermark embedding later. The watermark generated from hashing the area of interest. The embedding region is measured to be outside the region of interest as to preserve the area for distortion as a result from watermarking. In an image, the embedding region's pixel value is 0. This feature will be exploited to create a reversible or invertible watermarking.

PROPOSED SYSTEM

To securely transmit a secret image and recover it lossless by method of creating a mosaic image using HSV color model. Embedding text into the secret image to be transmitted by data hiding and to implement key less approach for secret image transmission.

PROPOSEDSCHEME

In this project, 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..

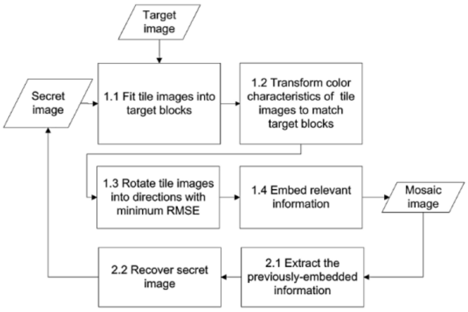

Target image
Secret image
1.1 Fit tile images into target blocks
1.2 Transform color characteristics of tile images to match target blocks
1.3 Rotate tile images into directions with minimum RMSE
1.4 Embed relevant information
Mosaic image
2.2 Recover secret image
2.1 Extract the previously-embedded information

Fig : FlowDiagram of proposed system

The embedding of text into secret image by Data Hiding, the embedding of secret image into the target image in tile form and maintaining the visibility of the original target image. The proposed method includes.

There suit is the mosaic tile image, which consists of the tile fragments of an input secret image which has color characteristics same as that of another target image selected from the database.

SECRET IMAGE SELECTION

A Secret image is selected from the system and is uploaded to the database. And this secret image is divided into 9 fragments. The color transformation function, h and y is applied to each of the fragments of the image and is saved in the database. the value 1, is assigned to the blue channel value b'. This way of weight assignment is based on the fact that the human eye is the most sensitive to the green color and the least sensitive to the blue one, leading to a larger emphasis on the intensity of the resulting mosaic image.

Fitting tile images into target blocks

Calculate the h-feature values of all the tile images from the secret image and take out the h-feature values of all the target blocks of Do from DB. In a raster-scan order of the target blocks in Do, perform the greedy search process to find the most similar tile images s1,s2,…s9 in S and corresponding to the N target blocks d1,d2,…d9 in Do , respectively, to construct the secret recoverysequence LR=0,1,..9 Using the h-feature values. And finally, fit the tile images s1, s2…s9 into the corresponding target blocksd1, d2…d9 respectively, to generate a preliminary secret-fragment- visible mosaic image U. Key Generation: Fitting tile images into target blocks: Calculate the h-feature values of all the tile images from the secret image and take out the h-feature values of all the target blocks of Do from DB. In a raster-scan order of the target blocks in Do, perform the greedy search process to find the most similar tile images s1,s2,…s9 in S and corresponding to the N target blocks d1,d2,…d9 in Do , respectively, to construct the secret recovery sequence LR=0,1,..9 Using the h-feature values. And finally, fit the tile images s1, s2…s9 into the corresponding target blocksd1, d2…d9 respectively, to generate a preliminary secret-fragment- visible mosaic image U.

Key Generation

A secret key is generated randomly in each of the fragments of the images using a random class. This secret key is used for recovering the secret image from the mosaic image. Without this key secret image cannot be recovered.

SECRET IMAGE RECOVERY

Retrieving tile-image fitting information

Retrieve the recovery key of the tile images from the first ten pixels in the first block of image in a raster-scan order using a reverse version of the lossless LSB replacement scheme. Repetitively select randomly an unselected block other than the first block from using the random number generator with the secret key as the seed, extract bits from all the pixels of using a reverse version of the lossless LSB replacement scheme proposed. Transform every bits of LR into an integerwhich specifies the index of a tile image in the original secreti mage (to be composed), resulting in the secret recovery sequenceLR= 0, 1…9.

COLOR IMAGE

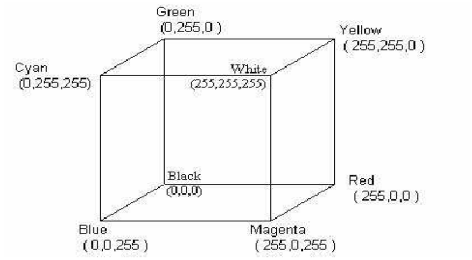


Figure: Color specification of the RGB Color Cube

PROCESSING

Any color that can be represented on a computer monitor is specified by means of the three basic colors- Red, Green and Blue called the RGB colors. By mixing appropriate percentages of these basic colors, one can design almost any color one ever imagines.The model of designing colors based on the intensities of their RGB components is called the RGB model**,** and it’s a fundamental concept in computer graphics.

Each color, therefore, is represented by a triplet (Red, Green, Blue), in which red, green and blue are three bytes that represent the basic color components. The smallest value, 0, indicates the absence of color. The largest value, 255, indicates full intensity or saturation. The triplet (0, 0, 0) is black, because all colors are missing, and the triplet(255, 255, 255) is white. Other colors have various combinations.(255,0,0) is pure red, (0,255,255) is a pure cyan (what one gets when green and blue are mixed), and (0,128,128) is a mid-cyan (a mix of mid-green and mid-blue tones). The possible combinations of the three basic color components are 256x256x256, or 16,777,216 colors

The process of generating colors with three basic components is based on the RGB Color cube as shown in the above figure. The three dimensions of the color cube correspond to the three basic colors. The cube's corners are assigned each of the three primary colors, their complements, and the colors black and white. Complementary colors are easily calculated bysubtracting the Color values from 255. For example, the color (0, 0,255) is a pure blue tone. Its complementary color is (255-0,255-0,255-255), or (255, 255, 0), which is a pure yellow tone. Blue and Yellow are complementary colors, and they are mapped to opposite corners of the cube. The same is true for red and cyan, green and magenta, and black and white. Adding a color to its complement gives white.

It is noticed that the components of the colors at the corners of the cubehave either zero or full intensity. As we move from one corner to another along the same edge of the cube, only one of its components changesvalue. For example, as we move from the Green to the Yellow corner, the Red component changes from 0 to 255. The other two components remain the same.

HSV COLOR FORMAT

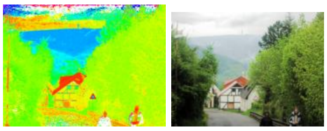
HSV color space HSL or HIS is one color space, which describes colors as perceived by human beings. HSI (or HSV) stands for hue (H),(S) saturation and intensity (I) (or value V). For example, a blue car reflects blue hue. Moreover is also attributing of the human perception. The hue which is essentially the chromatic component of our perception may again be considered as weak hue or strong hue.

The colorfulness of a color is described by the saturation component. For example, the color from a single monochromatic source of light, which produce colors of a single wavelength only , is highly saturated , while the colors comprising hues of different wavelengths have little chroma and have less saturation. The gray colors do not have any hue and hence they have less saturation or unsaturated. Saturation is thus a measure of colorfulness or whiteness in the color perceived.

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. Let us imagine the attitude of the cube, where the body diagonal linking ”black” vertex and ”white” vertex is vertical. Then the height of each point in the cube corresponds to the brightness of the color, the angle or azimuth corresponds to the hue and the relative distance from the vertical diagonal corresponds to the saturation of the color.

Optimized histogram in RGBHue with maximum saturation



Optimized histogram in YHS

The original photograph of Klínovecmountain in Bohemia was decomposed into brightness, hue and saturation by YHS model. The image "hue with maximum saturation" shows colors preserving original hue with maximum saturation. Where the original saturation was zero, the hue is not defined and white color is used. Then, the histogram was optimized in RGB coordinates, you can see the hue is distorted. When the histogram was optimized in YHS coordinates, the visibility of the foreground was enhanced without distortion of colors.

4.8 MOSAIC IMAGE CREATION

Problems encountered in generating mosaic images are discussed in this section with solutions to them proposed.

4.8.1 Color Transformations between Blocks

In the first phase of the proposed method, each tile image *T* in the given secret image is fit into a target block *B* in a preselected target image. Since the color characteristics of *T* and *B* are different from each other, how to change their color distributions 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

an image to be that of another in the l$\alpha\beta$ color space. This idea is an answer to the issue and is adopted in this paper, except that the RGB color space instead of the l$\alpha\beta$ one is used to reduce the volume of the required information for recovery of the original secret image.

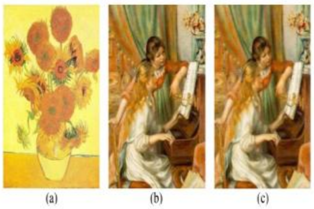


Fig: Result yielded by the proposed method. (a) Secret image. (b) Target image. (c) Secret-fragment-visible mosaic image created from (a) and (b) by the proposed method.

Furthermore, we have to embed into the created mosaic image sufficient information about the new tile image *T*_ for use in the later stage of recovering the original secret image. For this, theoretically we can use to compute the original pixel value of *pi*. However, the involved mean and standard deviation values in the formula are all real numbers, and it is impractical to embed real numbers, each with many digits, in the generated mosaic image.

Therefore, we limit the numbers of bits used to represent relevant parameter values in and . Specifically, for each color channel we allow each of the means of *T* and *B* to have 8 bits with its value in the range of 0 to 255, and the standard deviation quotient *qc* in to have 7 bits with its value in the range of 0.1 to 12.8.

4.8.2 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 described above, how to choose an appropriate *B* for each *T* is an issue. For this, we use the standard deviation of the colors in the block as a measure to select the most similar *B* for each *T*. Specially; we sort all the tile images to form a sequence, *Stile*, and all the target blocks to form another, Starget, according to the average values of the standard deviations of the three color channels.

Then, we fit the first in Stile into the first in Starget, fit the second in Stile into the second in Starget, 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, 0o, 90o, 180o, and 270o, which yields a rotated version of *T_* with the minimum root mean square error (RMSE) value with respect to *B* amongthe four directions for final use to fit *T* into *B*.

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. For this, we adopt a technique proposed by Coltuc and Chassery and apply it to the least significant bits of the pixels in the created mosaic image to conduct data embedding. Unlike the classical LSB replacement methods , which substitute LSBs with message bits directly, the reversible contrast mapping method applies simple Then, the above-defined bit streams of all the tile images are concatenated in order further into a total bit stream *Mt* for the entire secret image.

Moreover, in order 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 using the method of Coltuc and Chassery described above. It may require more than one iteration in the encoding process since the length of *M_* may be larger than the number of pixel pairs available in an iteration.

A plot of the statistics of the numbers of required bits for secret image recovery is shown in Fig. 8(b).Moreover, we have to embed as well some related information about the mosaic image generation process into the mosaic image for use in the secret image recovery process. Such information, described as a bit stream *I* like *M* mentioned previously, includes the following data items: 1) the number of iterations conducted in the process for embedding the bit stream *M_ t* ; 2) the total number of used pixel pairs in the last iteration for embedding

M_ t ; and 3) the Huffman table for encoding the residuals.

CONCLUSION:

A method is proposed to securely transmit a secret image, which can create mosaic tile images which also can transform a secret image into a mosaic tile image with the same size of data for concealing the secret image. This is done by the use of proper color transformations pixel by pixel and also using a technique for managing over flowing of the values converted for the pixels colors, in mosaic tile images with large visual similarities. The original secret image and secret text can be recovered nearly lossless from the created Mosaic images.

7.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,”ChaosSolit. 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,"ChaosSolit.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,"ChaosSolit. 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 permutationsubstitution scheme for image encryption," Opt. Commun., vol. 284, no. 19, pp. 4331–4339, 2011.

[8] C. K. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution,"PatternRecognit.., vol. 37, pp. 469–474, Mar. 2004.

[9] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, "Reversible data hiding,"IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar. 2006.

[10] J. Tian, "Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug.