ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

A Secure Image Transmission Technique via Mosaic Image Using HSV Colour Converted Target Image anda Reversible Data Hiding Method

Nithya Susan Abraham, Annie George

Post Graduate Student, Dept. of CSE, Sree Buddha College of Engineering for Women, Elavumthitta, Pathanamthitta, Kerala, India

Assistant Professor, Dept. of CSE, Sree Buddha College of Engineering for Women, Elavumthitta, Pathanamthitta, Kerala, India

ABSTRACT: A secure image transmission technique via mosaic image using HSV converted target image and reversible data hiding method is a new type of image protection method. It can transmit a secret image by converting it into secret fragment mosaic image and hidden inside a target image with the help of a reversible data hiding technique. Mosaic image are generated by converting secret image color to those of target image color and then diving it into small fragments. Color transformation is done based on a skillful method so that original image can be losslessly recovered. Inoder to reduce recovered image distortion and increase its security, before color transformation, target image are converted to its HSV color model. Underflow and overflow problem are solved by recording pixel value in untransformed color space. To increase security, mosaic image along with encrypted information that is required to recover original image are hidden inside target image by using a reversible data hiding technique.

KEYWORDS: data hiding; secret fragment mosaic image; underflow; overflow;color transformation

I. INTRODUCTION

Information transfer through internet is limited due to various attacks present in it. Areas like medical imaging, military, telemedicine etc. transfer different type of confidential images and data through internet. So it is very important to protect this type of images from different security problems. Two commonly used methods are data hiding and encryption, decryption method. Information hiding includes watermarking, anonymity and steganography. Here, data or images are securely hided inside an image so that no one can easily identify the presence other images or data. Image encryption and decryption method include conventional encryption and others such as chaotic encryption methods. Here, images are securely transfer by encrypting the whole image with a secret key. It is very difficult for an attacker to decrypt without the secret key. Due to some disadvantages of data hiding and encryption method, a new method called secret fragment visible mosaic images are developed. Mosaic image is a one type of art in which it is manufactured by generating small pieces of materials like stone, glass, tile etc. Based on this concept secret fragment visible mosaic image [1] are created. Here, images are divided into small pieces and convert its colour based on its target image and then combine these small pieces to form a mosaic image. One of the disadvantages of this method is that, even if tiles are random in position, sometimes one can guess what the image is. And also tiles are composed of different colour values, so during the data hiding time there is a chance for loss of some of the information.

To avoid this problem, a secure image transmission technique via mosaic image using HSV colour converted target image and a reversible data hiding method are proposed. Here, firstly source image colour is transformed to its corresponding colour of its HSV converted target image. Then source image and target image are tiled equally based on a particular block size. After that, based on the mean and standard deviation of each secret and target tiled image,

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

similar images are find out. Then each colour transformed tiles are rotated in different directions and its root mean square error is found out with respect to its target image. Angle with minimum root mean square error is set as its final position. All rotated tiles are then combine together to form a mosaic image and save all details such as mean, standard deviation quotient, rotation angle, index of original image. Secure transmission of mosaic image is done by hiding each pixel in last two bit of target image. Data that needed to recover original image are encrypted with AES encryption algorithm. This encrypted data are reversibly hidden at the one of the bit position of target image. In order to recover original image, residual value generated during colour transformation are also hidden at the fifth and sixth bit position of the target image. This data hidden target image is transmitted to the receiver.

The remainder of this paper is organized as follows. Related works of this paper is described in Section II. Proposed method along with a detailed explanation of each stage is given in section III. Detailed algorithms are explained in Section IV. Section V discusses the experimental setup and the results, followed by conclusion and future research directions in section VI.

II. RELATED WORK

Fast, reliable and robust, security systems is needed to store and transmit digital images used in the application like military image databases, medical imaging, confidential video conferencing, online personal photograph albums, cable TV, etc. [2]. Bulk data capacity, High Redundancy and high correlation among pixels, are the factors that differentiate Image Encryption from text Encryption. Because of the development in theory and application of chaos, now a day's many chaos algorithms have been proposed. Properties of chaotic systems are sensitively depend on initial conditions and system parameters, the density of the set of all periodic points and topological transitivity, etc. Most properties are related to requirements such as diffusion and mixing in the sense of cryptography. Therefore, chaotic cryptosystems has different useful and practical applications [3]. To improve the properties of confusion and diffusion in terms of discrete exponential chaotic maps, a paper called Image Encryption Approach Based on Chaotic Maps [3] is introduced. In this paper, it designs a key scheme for the resistance to statistic attack, grey code attack and differential attack. A novel algorithm for image encryption based on mixture of chaotic maps [4], focus on the chaotic digital encryption techniques. Symmetric key chaotic cryptography is used here. To enhance future security high-dimensional chaotic systems such as a coupled map are used. Another paper called A Symmetric Chaos-Based Image Cipher with an Improved Bit-Level Permutation Strategy [5]a symmetric chaos- based image cipher with a 3D cat map-based on spatial bit-level permutation is used. Diffusion effect of this method is high because its bits are shuffled in different planes rather than within the same bit plane. Now a day's different encryption method are present and it is good in different areas. But the main disadvantage of encryption-decryption method is that, during the recovery stage original image is not recovered. And also, due to its randomness form causes the attackers attention [1]

Another method to solve disadvantage of encryption method is data hiding technique. It hides a secret message into a cover image so that no one can easily identify the presence of message. One of the main advantages of data hiding over cryptography is that it does not attract the attention of attackers themselves. Data hiding can be used in various areas like tamper proofing, ownership identification, data transmission etc. Mainly data hiding are classified as watermarking and image hiding. Watermarking is a method used to embed a distinguishable symbol into a host image to authorize the ownership of the image. Image hiding is the method that embeds one image into the other image so that no one can easily identify the hidden image easily. Existing data hiding methods use different techniques. One of the common techniques used for data hiding is Image hiding by optimal LSB substitution and genetic algorithm [6]. In this method, data are embedding at the LSB position of the image. To increase security and obtain better embedding result an optimal LSB substitution and randomized embedding process along with data hiding by human perception model are used. Another technique is hiding data in images by simple LSB substitution [7]. Advantage of simple LSB over optimal LSB is that the WMSE between the cover image and embedded image of optimal LSB is 1/2 that of obtained by the simple LSB. Computational cost is also low with respect to optimal LSB because optimal LSB requires huge computation cost for genetic algorithm to find an optimal substitution matrix.In general, data hiding causes distortion in the host image. Such distortion may be very small but it is not acceptable to some application. To solve this problem, reversible data hiding method is used. Here, secret information is embedded in reversible manner so that original information can be perfectly recovered.Different reversible data hiding techniques are present; one type is Reversible Data Embedding Using a Difference Expansion [8]. It is a reversible data embedding method in which high quality and

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

high capacity are present. Another Reversible data hiding technique is, RCM [9] - is a simple integer transform which is applies to pairs of pixels. Even if the LSB is lost, some pair of the RCM can be invertible. One of the problems in data hiding method is that if the embedded data is larger than the image size then the information should be compressed and then embeds into it. This may cause distortion to the images.

Another new technique for secure image transmission is Secret-Fragment-Visible Mosaic Image [10] is a new type of image which is created automatically by composing small fragments of a given image to become a target image. Here secret image are divided into small fragments and they are embedded inside a target image visibly. Fragments are so tiny and random in position so that no one can easily identify the original image. Information needed to recover original image are embedded into the mosaic image with a secret key and the method used is a lossless LSB scheme. Fast greedy search algorithm is used to find the similar target block to fit the secret tiled image.One of the disadvantages of Secret-Fragment-Visible Mosaic Image [10] is the requirement of a large image database so that the generated mosaic image can be sufficiently similar to the selected target image. By removing this weakness and keeping its merit, a new method called A New Secure Image Transmission Technique via Secret-Fragment-Visible Mosaic Images by Nearly Reversible Color Transformations [1] is developed. It 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. Information needed to recover secret image are encrypted with a secret key and then embedded inside the mosaic image with the help of RCM method [9].

III. PROPOSED METHOD

Proposed system is based on the secure transmission of a source image based on secret fragment mosaic image, reversible data hiding and HSV color converted target image. Skillful techniques are used to conduct the color transformation process so that the secret image may be recovered nearly losslessly. A scheme of handling the overflow/underflow in the converted pixels color values by recording the color differences in the untransformed color space is also used here. In addition to RGB color space, HSV color space [11] is also used in color transformation process. RGB color transformation method successfully transfer image fast and it also efficiently generates a convincing result. However, the result is not quite reliable if an image contains many colors or wide chromatic regions since they define the color characteristics of an image with only one mean and standard deviation values for each RGB color channel. Also RGB value will vary a lot depending on strong or dim lighting conditions and shadows etc. Due to this reason visibility of secret image is high in mosaic image and an observer can easily identify some of the part very clearly and he can guess the image. If HSV is used instead of RGB then color transformation is based on color, greyness and brightness so that it is much better at handling lighting difference. Inoder to improve the security, mosaic image along with residual value are hidden inside the target image. The information required for recovering the secret image is embedded into the new target image by a lossless data hiding scheme using a key. This is a new technique of information hiding, which solves some disadvantages of existing data hiding techniques. It is useful for the application of covert communication or secure keeping of secret images.
The overall architecture of proposed system at sender side and receiver side are shown in the Figure 3.1 and Figure 3.2.

A. Color Transformation Between Tiles:

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. To solve this problem, RGB color space is used [1]. Since RGB value will vary a lot depending on strong or dim lighting conditions and shadows, color conversion is not done correctly. So that an attacker can identifies some portion of the image correctly. So to avoid this in addition to RGB, HSV color space are be used for color transformation. For that firstly convert RGB target image to HSV.

Let T and B be two pixel sets $\{p_1, p_2 \ldots p_n\}$ and $\{p'_1, p'_2, \ldots\ldots, p'_n\}$. Let the color of each p_i be denoted by r_i, g_i, b_i and that of each p'_i by r'_i, g'_i, b'_i. At first, the means and standard deviations of T and B are found out, for each of the three color channels R, G, and B

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

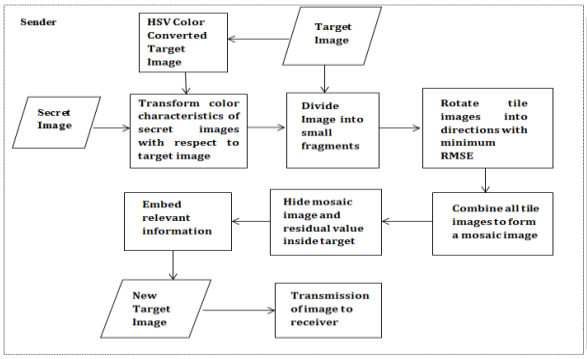

Figure 3.1: Flow diagram of the secret fragment mosaic image creation at sender side

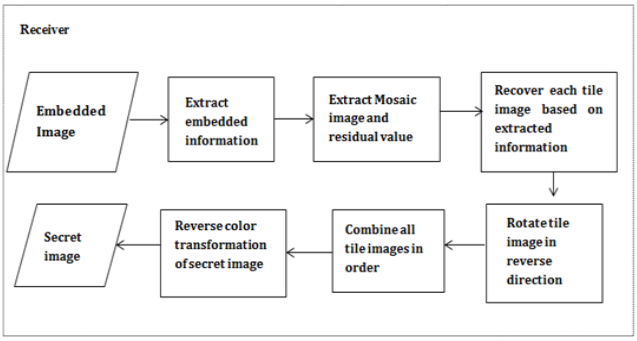

Figure 3.2: Flow diagram of the secret fragment image recovery at receiver side

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

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

in which c_i and c_i' denote the C-channel values of pixels p_i and p'_i, respectively, with c = r, g, or b and C = R, G, or B. Next, compute new color values (r_i'', g_i'', b_i'') for each p_i in T by

$$c_i'' = q_c(c_i - \mu_c) + \mu_c' \quad (3)$$

In which $q_c = \sigma_c' / \sigma_c$ is the standard deviation quotient and c = r, g, or b. It can be verified easily that the new color mean and variance of the resulting tile image T are equal to those of B, respectively. 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, limit the numbers of bits used to represent relevant parameter values in (3). Specifically, for each color channel 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 q_c in (3) to have 7 bits with its value in the range of 0.1 to 12.8. That is, each mean is changed to be the closest value in the range of 0 to 255, and each q_c is changed to be the closest value in the range of 0.1 to 12.8. Do not allow q_c being 0 because otherwise the original pixel value cannot be recovered back [1].

B. Selecting Appropriate Target Blocks And Rotating Blocks To Better Fit With Smaller RMSE Value:

To choose an appropriate block B for each tile T, use the standard deviation of the colors in the block as a measure to select the most similar B for each T. Mainly, sort all the tile images to form a sequence, S_{tile} and all the target blocks to form another S_{target}, according to the average values of the standard deviations of the three color channels. Then, fit the first tile in S_{tile} into the first block position in S_{target}, fit the second tile in S_{tile} into the second block position in S_{target}, and so on[1]. To improve color similarity between the resulting tile image T' and the target block B, rotate T' into one of the four directions, $0°, 90°, 180° and 270°$ and find its root mean square error (RMSE) value for each angle with respect to B. Then find minimum RMSE value among the four directions. Angle with minimum RMSE value direction will be set as final rotation direction of tile image [1].

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

C. Overflow, Underflow Handling in color Transformation:

After color transformation, overflow or underflow of pixel values may occur in T'. To solve this problem, such values are convert into non overflow or non-underflow ones and record the value difference as residuals. Pixel value not smaller than 255 is converted to 255 and those not larger than 0 to 0. In [1], residual values are calculated by computing the difference between the original pixel values and the converted one as the residual and record it as a part of the information associated with T'. But here, residual values are calculated only for the pixel value, which has occurred overflows and underflows. So that during recovering stage, it can be easily identify which pixel values are converted to 255 and 0 due to overflow and underflow. These residual values are embedded along with the mosaic image inside the target image and transmitted to the receiver side.

D. Hiding Mosaic Image And Residual Value losslessly

After color conversion and rotation of each tile image of the secret image, they are combined together to form a mosaic image. Since the tile images are placed in random position with different angle, one can't identify the original image very easily. And due to the color conversion each pixel value range is very much different from the original image. So during the data embedding stage, some of the pixel value may change and so that during recovery stage original color conversion is not possible. To avoid this problem, mosaic image are hidden inside the target image and one can recover this mosaic image without any loss [12].To hide mosaic image, first target image is resized as double of the mosaic image size. Then divide each pixel value of mosaic image into a four two-bit value. Let d1, d2, d3, d4, d5, d6, d7, d8 are the bit value of one pixel of mosaic image. Then divide the new resized target image into four quadrants. Replace last two bit of first quadrant value with d7 and d8 bit values. d5 and d6 bit are replaced last two bit of fourth quadrant. d3 and d4 are replaced last two bit of second quadrant value. And d1, d2 bit are replaced with last two bit of third quadrant value. Thus the last two bit of target image is replaced with mosaic image value. It is very difficult to identify that an image is hidden inside it. Here mosaic image are hidden at the 7th and 8th bit position of target image in different positions. To recover the original image it is very important to hide the residual value also. So at 5th and 6th bit position of target image are replaced with the residual value as the same order done for mosaic image hiding. This target image with mosaic image and residual value, let it be T'' are used for further process.

E. Information Embedding For Secret Image Recovery:

In order to recover the secret image from the mosaic image, embed relevant recovery information into the mosaic image. The information required to recover a tile image T which is mapped to a target block B includes: Index of B, Optimal rotation angle of T , Truncated means of T and B and the standard deviation quotients, of all color channels, Total number of tiles. These data items for recovering a tile image T are integrated as a five-component bit stream of the form $M = t_1 t_2 \ldots\ldots t_m r_1 r_2 m_1 m_2 \ldots\ldots m_{48} q_1 q_2 \ldots q_{21} k$ in which the bit segments $t_1 t_2 \ldots\ldots t_m, r_1 r_2, m_1 m_2 \ldots\ldots m_{48}, q_1 q_2 \ldots q_{21}, k$ represent the values of the index of B, the rotation angle of T , the means of T and B, the standard deviation quotients, and total number of tiles, respectively. In more detail, the numbers of required bits for the five data items in M are: The index of B needs m bits to represent, with m computed by $m = \lceil \log[(W_s \times H_s)/N_T] \rceil$ in which W_s and H_s [1] are respectively the width and height of the secret image S, and N_T is the size of the target image T , It needs two bits to represent the rotation angle of T because there are four possible rotation directions; 48 bits are required to represent the means of T and B because eight bits are used to represent a mean value in each color channel, It needs 21 bits to represent the quotients of T over B in the three color channels with each channel requiring 7 bits, Total number of tiles "k" is required to separate each set of value from other. Then, the above-defined bit streams of all the tile images are concatenated further into a total bit stream M_t for the entire secret image. Moreover, in order to protect M_t from being attacked, encrypt it with a secret key to obtain an encrypted bit stream M_t' . For that AES encryption is used. After AES encryption, M_t' will embed at the fourth bit position of T''. Some related information about the mosaic image generation process into the mosaic image for use in the secret image recovery process are also embed at the last fourth bit position of T''. Such information, described as a bit stream I like M, includes the following data items: 1) encryption key; and 2) total length of M_t before encryption. After all this process Target image T'' with mosaic image, residual value and all information that required recovering original image are transmitted to receiver side.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

IV. ALGORITHM

ALGORITHM 1: MOSAIC IMAGE CREATION AND HIDING

Step 1**:** Select secret image S and target image T. If the size of the target image T is different from that of the secret image S, change the size of T to be identical to that of S

Step 2**:** Convert target image into HSV image by using the equation (1) to form new target image T

Step 3: For performing color conversion, first means μ_c and μ_c' of S and T are find out and then find standard deviation quotient q_c from equation (3) for each color channel

Step 4: Limit mean value by eight bits and standard deviation quotient to seven bits

Step 5: Based on this value, for each pixel p_i in each secret image S_i with color value c_i where c = r, g, or b, transform c_i into a new value c_i'' by (3)

Step 6: if c_i'' is not smaller than 255 or if it is not larger than 0, then change c_i'' to be 255 or 0, respectively; compute a residual value R_i for pixel p_i

Step 7: Divide the color converted secret image S into n tile images $T_1, T_{2,\ldots\ldots} T_n$ as well as the target image T into n target blocks $B_1, B_{2,\ldots\ldots} B_n$

Step 8: Compute the means and the standard deviations of each tile image T_i and each target block B_j for the three color channels according to equations (1) and (2).

Step 9: Compute accordingly the average standard deviations for T_i and B_j, respectively, for i = 1 through n and j = 1 through n.

Step 10: Sort the tile images in the set $S_{tile} = T_1, T_{2,\ldots\ldots} T_n$ and the target blocks in the set $S_{target} = B_1, B_{2,\ldots\ldots} B_n$ according to the computed average standard deviation values of the blocks; map in order the blocks in the sorted S tile to those in the sorted S target in a 1-to-1 manner; and reorder the mappings according to the indices of the tile images, resulting in a mapping sequence L of the form $T_1 \to B_{j1}, T_2 \to B_{j2,\ldots\ldots,} T_n \to B_{jn}$.

Step 11: Compute the RMSE values of each color transformed tile image T_i with respect to its corresponding target block B_j after rotating T_i into each of the directions $\theta = 0°, 90°, 180° and 270°$

Step 12: Rotate T_i into the optimal direction θ° with the smallest RMSE value and form T'

Step 13: Create a mosaic image F by fitting the tile images T' into the corresponding target blocks positions.

Step 14: Re-size target image as double size of its mosaic image F.

Step 15: Divide resized target image into four quadrants.

Step 16: Hide mosaic image F at the 7th and 8th bit position of target image four quadrant to form T''

Step 17: Hide residual value R_i at the 5th and 6th bit position of target image four quadrant to form T''

Step 18: For each tile image T_i in mosaic image F, construct a bit stream M_i for recovering T_i in the way as described in Section 3.3.6, including the bit segments which encode the data items of: 1) the index of the corresponding target block B_{ji}; 2) the optimal rotation angle θ° of T_i; 3) the means of T_i and B_{ji} and the related standard deviation quotients of all three color channels; and 4) total number of tiles present in mosaic image creation.

Step 19: Concatenate the bit streams M_i of all T_i in F in a raster-scan order to form a total bit stream M_t; use the secret key K to encrypt M_t into another bit stream M_t' by using AES encryption; and embed M_t' into T'' by replacing fourth bit position.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

Step 20: Construct a bit stream I including: 1) encryption key; and 2) total length of M_t before encryption and embed the bit stream I at the end of the $T^{"}$ by the same scheme used in Step 19.
Step 21: Send embedded target image to receiver side.

ALGORITHM 2: SECRET IMAGE RECOVERY

Step 1: Select the image $T^{"}$.

Step 2: The bit stream I are extracting from $T^{"}$ and decode them to obtain the following data items: 1) encryption key K; and 2) total length of encrypted input.

Step 3: Extract the bit stream $M_t^{'}$ from the fourth bit of the image by using length of encrypted input and decrypt the bit stream $M_t^{'}$ into M_t by K using AES decryption algorithm.

Step 4: Decompose M_t 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: Extract mosaic image bit stream and residual value bit stream from $T^{"}$

Step 6: Decode M_i for each tile image T_i to obtain the following data items: (1). the index ji of the block B_{ji} in F corresponding to T_i. (2). the optimal rotation angle θ° of T_i. (3). the means of T_i and B_{ji} and the related standard deviation quotients of all color channels. (4). total number of tiles.

Step 7: Divide mosaic image into tiles with the help of total number of tiles that extracted from step 6.

Step 8: Recover one by one in a raster-scan order the tile images T_i, i = 1 through n, of the desired secret image S by, (1).Rotate in the reverse direction the block indexed by ji, namely B_{ji}, in F through the optimal angle θ° and fit the resulting block content into T_i to form an initial tile image T_i. (2). compose all the tile images T_i to form the desired secret image

Step 9: Use the extracted means, related standard deviation quotients and residual values to recover the original pixel values in T_i according to the equation: $c_i = \frac{1}{q_c}(c_i^{"} - \mu_c^{'}) + \mu_c$

Step 10: Desired secret image S is recovered with less distortion

V. SIMULATION RESULTS

Experimental results of the proposed technique for secure transmission of an image by using HSV colour conversion and reversible data hiding technique, is discussed in this section. The proposed algorithm is implemented with MATLAB.To show that the retrieved image that depends on HSV colour converted target image is more similar to secret image than RGB colour converted image and also show that target image with hidden data are more secure, a quality metric of root mean square error is utilized.

A. Results:

The proposed method are tested using many secret and target images with sizes 96×96, 960×960, 100×100 in jpg format and 928×1024, 288×175, 512×512 in tiff format. JPG images are tested with JPG target images, tiff images are tested with tiff and jpg format target images. Tiling of image is done by 20×20 and 100×100 block sizes. From the Figure 6.1 to 6.3, (a) is the secret image; (b) is the target image. (c) is the target image with relevant information and mosaic image with RGB color conversion hidden in it, (d) is target image with relevant information and mosaic image with HSV color conversion hidden in it, (e) shows the retrieved secret image from RGB color converted mosaic image and (f) shows the retrieved secret image from HSV color converted mosaic image. Target image with all information hidden are compared with original secret image and also extracted secret image are compared with original image by using RMSE value. The Root Mean Square Error (RMSE) calculates the difference between original image and image result from proposed method. Low RMSE value has less error when compare to original image. Experimental results are shown in table 5.1 and 5.2.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

B. *Discussion:*

These results proves that the proposed data hiding technique is totally revertible, and the original mosaic image can be retrieved at the receiver side without any distortion and by using HSV color transformation, secret image can be retrieved with less distortion than RGB color conversion method. In [1], mosaic image are yield by dividing the secret image into tile images and then transforming their color characteristics to be those of the corresponding target blocks, one problem arise here is that during color transforming, edge distortion may occur and during the recovery stage, low similar secret image is recovered. But in this method, first color conversion of secret image is done then tiling of both images is take place. So that edge distortion can be reduced and maximum similar image can be recovered. In RGB color conversion method, mean and standard deviation quotient method of target image are taken from its 3 channel and based on this value secret image color are converted. Here, Inoder to increase the security level, first target image color is converted to HSV and based on this H, S, V value; mean and standard deviation quotient value are calculated and then convert secret image color based on it. By this method, difference between target image and mosaic image can be reduced and after hiding of this mosaic image, visual distortion of target image can also reduce. Thus an intruder can't easily identify that inside this image some other values are present. From the table 5.1 it is clear that target image with HSV hidden image has low RMSE value so it has less distortion when compared to RGB image. And from table 5.2, it is clear that recovered image after HSV color converted image has less distortion with respect to its original image than RGB color converted image. And also it is clear that secret image with tiff format hidden inside target image in jpg format has less RMSE value than other target images.To increase the security of the proposed method, the embedded information is encrypted with a secret key and also mosaic images are hidden inside the target image in different bit positions. Only the receiver who has the key and correct order in which mosaic image hidden can decode the secret image.

Figure 5.1: a) Secret image. (b) Target image. (c) Target image with RGB colour converted mosaic image and relevant information hidden in it with RMSE=13.7701. (d)Target image with HSV colour converted mosaic image and relevant information hidden in it with RMSE=8.74512. (e) Recovered RGB colour converted secret image with RMSE=2.30285. (f) Recovered HSV colour converted secret image with RMSE=2.12203

Figure 5.2: (a) Secret image. (b) Target image. (c) Target image with RGB colour converted mosaic image and relevant information hidden in it with RMSE=15.2158. (d)Target image with HSV colour converted mosaic image and relevant information hidden in it with RMSE=8.20475. (e) Recovered RGB colour converted secret image with RMSE=7.41801. (f) Recovered HSV colour converted secret image with RMSE=6.9818

Figure 5.3: (a) Secret image. (b) Target image. (c) Target image with RGB colour converted mosaic image and relevant information hidden in it with RMSE=9.65088. (d)Target image with HSV colour converted mosaic image and relevant information hidden in it with RMSE=8.73098. (e) Recovered RGB colour converted secret image with RMSE=4.06874. (f) Recovered HSV colour converted secret image with RMSE=4.14801

Table 5.1: RMSE value of target image with all data hidden in it (sender side)

Source Image	Target Image	RMSE(RGB)	RMSE(HSV)
Images1.jpg	Imaget1.jpg	2.30285	2.12203
Images2.jpg	Imaget2.jpg	7.41801	6.9818
Images3.jpg	Imaget3.jpg	4.06874	4.14801
Images4.tiff	Imaget4.tiff	7.3292	6.21591
Images5.tiff	Imaget5.tiff	2.26917	2.20167
Images6.tiff	Imaget6.tiff	5.10793	4.64609
Images4.tiff	Imaget7.jpg	1.70805	1.61682
Images6.tiff	Imaget1.jpg	5.0642	5.05809
Images7.tiff	Imaget2.jpg	4.72588	2.92436

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

Table 5.2: RMSE value of recovered image at receiver side

Source Image	Target Image	RMSE(RGB)	RMSE(HSV)
Images1.jpg	Imaget1.jpg	13.7701	8.74512
Images2.jpg	Imaget2.jpg	15.2158	8.20475
Images3.jpg	Imaget3.jpg	9.65088	8.73098
Images4.tiff	Imaget4.tiff	10.1595	8.79745
Images5.tiff	Imaget5.tiff	15.9159	8.24918
Images6.tiff	Imaget6.tiff	15.169	5.87793
Images4.tiff	Imaget7.jpg	9.04397	6.88208
Images6.tiff	Imaget1.jpg	14..6729	9.65885
Images7.tiff	Imaget2.jpg	15.2348	6.54405

VI. CONCLUSION AND FUTURE WORK

A secure image transmission technique via secret fragment mosaic image using HSV color converted target image and a reversible data hiding method is a new image transmission method. In this method, sender can transmit his secret image by converting it into a mosaic image and hidden securely inside the target image. By the use of proper pixel color transformation as well as a skillful scheme for handling overflows and underflow in the converted values of the pixel colors, mosaic image with high visual similarity to target image can be created without need of a target image database. Inoder to avoid the identification of tile images, mosaic images are hidden inside the target image in a secure manner. In addition to that, all relevant data are also hidden inside the target image after an encryption method so that during the recovery stage, mosaic image will be retrieved without any distortion. From experiment results it is clear that, the original image can be recovered nearly losslessly. In future, image can be retrieved more accurately by using other color models and color transfer between secret and target image can also be improved.

REFERENCES

1. Ya-Lin Lee, Wen-Hsiang Tsai, 'A New Secure Image Transmission Technique via Secret-Fragment-Visible Mosaic Images by Nearly Reversible Color Transformations', IEEE transactions on circuits and systems for video technology, vol. 24, no. 4, April 2014.
2. 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.
3. Jianjiang CUI1, Siyuan LI2 and Dingyu Xue3, 'A Novel Color Image Cryptosystem Using Chaotic Cat and Chebyshev Map', IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 3, No 2, May 2013.
4. 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.
5. Chong Fu, Jun-Bin Huang,Ning-NingWang, Qi-Bin Hou and Wei-Min Lei, 'A Symmetric Chaos-Based Image Cipher with an Improved Bit-Level Permutation Strategy', Entropy 2014, 16, 770-788.
6. R. Z. Wang, C. F. Lin, and J. C. Lin, 'Image hiding by optimal LSB substitution and genetic algorithm', Pattern Recog., vol. 34, no. 3, pp. 671–683, 2001.
7. K. Chan and L. M. Cheng, 'Hiding data in images by simple LSB substitution', Pattern Recognit.., vol. 37, pp. 469–474, Mar. 2004.
8. N. Ansari, and W. Su, Y. Q. Shi and Z. Ni,'Reversible data hiding', IEEE Trans. Circuits Syst. Video Technol, 2006.
9. Coltuc and J.-M. Chassery, 'Very fast watermarking by re- versible contrast mapping', IEEE Signal Process. Lett., vol. 14, no. 4, pp. 255–258,Apr.2007.
10. I. J. Lai and W. H. Tsai, 'Secret-fragment-visible mosaic image—A new computer art and its application to information hiding', IEEE Trans. Inf. Forens. Secure. vol. 6, no. 3, pp. 936–945, Sep. 2011.
11. GauriDeshpande, and MeghaBorse,'Image Retrieval with the use of Colour and Texture Feature', (IJCSIT) International Journal of Computer Science and Information Technologies, 2011.
12. http://matlabsproj.blogspot.in/2012/06/image-hider-using-matlab.html.

BIOGRAPHY

Nithya Susan Abrahamis a Post Graduate student in Department of Computer Science & Engineering, Sree Buddha College of Engineering for Women, Mahatma Gandhi University. She received Bachelor of Technology (B.Tech) degree in 2013 from Mahatma Gandhi University, Kottayam, Kerala, India. Her research interests are Image Processing, Networking etc.