IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 11, November 2015

A New Secure Image Transmission Technique via Mosaic Images Using Genetic Algorithm

Surya .T.S[1], Deepthy Mathews[2]

PG Student, Dept of Computer Science & Engineering, Christ Knowledge City, Ernakulam, India[1]

Assistant Professor, Dept of CSE, Christ Knowledge City, Ernakulam, India[2]

Abstract: A new secure image transmission method is proposed in which it transforms the secret image into secret-fragment-visible mosaic image. The size of the mosaic image is same as that of secret image. Mosaic image is created by dividing the secret image and target image into fragments of equal size and fitting these secret tile blocks into target blocks. For tile image hiding, a mapping sequence is generated using Genetic Algorithm (GA). This provides better clarity in the retrieved secret image. It also reduces the computational complexity. The quality of the original target image remains preserved while embedding the secret image. Therefore better security and robustness is assured. Embed these tile fragments into the target image based on the mapping sequence by genetic algorithm and permuted the sequence again by KBRP with a key. Color transformations are performed to make the mosaic image similar to the target image. After color transformation rotation is performed. Rotating each tile block into an optimal rotation angle with minimum root mean square error value with respect to its corresponding target blocks. For the recovery of the secret image from the mosaic image embed relevant information into the created mosaic image. Overflows/underflows in the transformed color values can also be handled by using this method. By using the same key and the mapping sequence, the secret image can be recovered.

Keywords: Image hiding, Mosaic image, Genetic Algorithm, Key Based Random Permutation, Color Transformation.

I. INTRODUCTION

Images from different sources are utilized and transmitted through the internet for variety of applications. These applications include confidential enterprise archives, military image databases, document storage systems, online personal photograph albums and medical imaging systems. These images contain confidential or private information. Therefore, such information should be protected from leakages while transmitting through internet.

Now a day, different methods have been proposed for secure image transmission. The two common approaches are image encryption and data hiding. Image encryption is the process of encoding secret images in such a way that only authorized parties can view it. Data hiding is the process of embedding the secret data into the cover images. The Image encryption technique is based on the natural property of an image like high redundancy and strong spatial correlation. By using these properties, the encrypted image is obtained. The encrypted image is a noise image, so without the correct key the secret image cannot be decrypted. The encrypted image is a meaningless file that cannot provide additional information before decryption. It also makes an attacker's attention to the encrypted image during transmission because of its randomness in form.

An alternative method to avoid this problem is data hiding that hides a secret data into a cover images. So, no one can recognize the existence of the secret data. In this method, the data type of the secret message investigated is an image. 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. On the payload of the cover image, an upper bound for the distortion value is usually set, in order to reduce the distortion of the resulting image.

The main drawback of the data hiding method is that, difficulty to embed a large amount of message data into a single image. The secret image must be highly compressed in advance, in order to hide a secret image into a cover image with the same size. Data compression operations are usually impractical for many applications like keeping or transmitting legal documents, military images, medical pictures, etc.

In this method, a mosaic image steganography is used to hide the secret image based on Genetic algorithm (GA) and Key based random permutation (KBRP). Genetic algorithm (GA) is used to generate a mapping sequence for tile image hiding. Genetic algorithm (GA) provides better clarity in the retrieved secret image and reduces the computational complexity. The quality of original cover image remains same after embedding the secret image. So better security and robustness is assured.

The mosaic image is created by dividing the secret image and target image into equal number of fragments and fitting these secret tile blocks into corresponding target blocks according to the mapping sequence generated by Genetic Algorithm (GA). The mapping sequence is again permuted using Key based random permutation (KBRP) with a key to improve the security. Using the same key and the mapping sequence, the secret image can be recovered. Fig. 1 shows an illustration of creation of mosaic image using the proposed method.

DOI 10.17148/IJARCCE.2015.41168

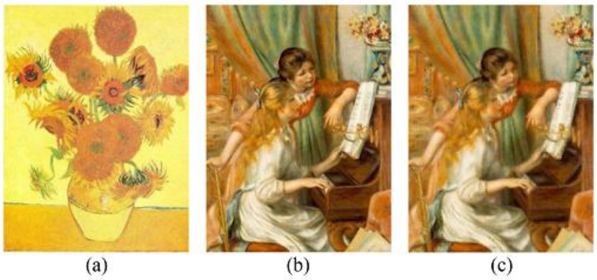


Fig.1. Result yielded by the proposed method. (a)) Secret image. (b) Target image. (c) Mosaic image

II. RELATED WORKS

Lin-Yu Tseng et.al proposed an image hiding technique using Genetic Algorithm (GA) and an Optimal Pixel Adjustment Process (OPAP) [10] in the year 2008. In the image hiding methods, a secret image is embedded into a cover image. The fusion of the two images, called a stego-image, fools the attackers who cannot be aware of the differences between the cover image and the stego-image. Secret image can be transmitted securely using this method. In this method, each pixel in the secret image is disarranged and adjust them to make a suitable string of bits that could be embedded. Then these string of bits are embedded into the cover image in corresponding locations, and resulting image would become a stego-image that hides secret data. This method proposes a new image disarranging technique. It employs an improved Genetic Algorithm (GA) and an Optimal Pixel Adjustment Process (OPAP), to improve the quality of the stego-image.

Zahra Toony et.al proposed a novel steganography method based on content aware seam carving [9] in the year 2010. In this method, an image hiding technique is proposed in which, the secret image is classified based on image complexity measure. Then the secret image is resized to an appropriate smaller size, by preserving the important objects of the image in resized image using seam carving method. Seam carving technique resizes an image by preserving the important content of the secret image. After applying the seam carving method, an image that is smaller than the original one, hide it in a cover image. Less distortion is caused in the stego-image while hiding a smaller secret image, hence high quality stego-image is obtained. This method provides more embedding rate and more security is enhanced.

CHEN Yuefen et.al proposed an image hiding method based on intensity quantization based on Genetic Algorithm (GA) [8] in the year 2010.In this method, an image hiding method is proposed based on intensity quantization and is optimized using Genetic Algorithm (GA). The secret image is transformed into 16-grayscale from 256-grayscale, by using the quantization parameters obtained from genetic optimization. Before embedding the secret image into the host image in space domain, the secret image is scrambled based on blocks. Information hiding technology has been a great interest to many researchers, which refers to hiding the secret information into a public media and is transformed in a public channel. In this method, space domain algorithm is used to change the intensity value to embed the secret image.

YongHong Zhang proposed an image hiding technique using curvelet transform [7] in the year 2011. Embedding images into other images has wide variety of applications in data hiding and digital watermarking. In this method, an extended image encryption algorithm is applied. For image encryption, curvelet transform and extended discrete chaotic dynamic system is used. Curvelet transform is defined as a multiscale transform with frame elements indexed by location and scale parameters. It has directional parameters. Fusion rule and Arnold transform are also used in this technique. Compared to wavelet transform, it contains directional parameters, and the curvelet pyramid, which contains elements with very high degree of directional specificity. In addition to wavelets, the curvelet transform is based on a certain anisotropic scaling principle which is different from that of isotropic scaling of wavelets.

Cheng-Hsiang Yeh et.al proposed an image hiding method based on multilevel histogram modification and halftoning technique [6] in the year 2011. Digital image can be widely and easily distributed by unauthorized copy, which is harmful to content owners. The data hiding method is the process of embedding secret messages into a cover media. Data hiding can be considered as a good solution to protect the secret information. For example, military images and medical images or data can be embedded into the digital images from the huge data storage.

The main requirements of digital image are authentication, High quality, frequent insertions and high capacity. In this method, multilevel histogram modification is applied to complete the data embedding process and data extracting process. The halftone data is extracted from the stego-image and the secret image is obtained using LUT inverse halfton method. This method provides high embedding capacity at low distortion level.

Manoj Sharma et.al proposed an image hiding technique using unitary similarity transformation [5] in the year 2011. In this technique, an efficient and different method of image hiding is proposed. This method is based on unitary similarity transformation, which involves eigen value calculations and determining eigen vectors of a matrix, and transforming into a diagonal matrix. Here, only the secret image needs to be transformed into diagonal matrix and embedded to the cover image. Inorder to recover the secret image from the stego-image inverse transformation is applied. The decryption key in this is the eigen vector matrix. This hiding algorithm is simple and can be easily implemented. This method can greatly improve robustness of image-hiding and the security of the system. The quality of the recovered secret image and stego-image can be improved by using this method.

I-Jen Lai et.al proposed a new type of computer art image called secret-fragment-visible mosaic image [4] in the year 2011. This art image is created by composing small fragments of a secret image to become a target image in a mosaic form. This method provides an effect of embedding the secret image in the resulting mosaic image and the mosaic image will look similar to the target image.

DOI 10.17148/IJARCCE.2015.41168

This type of information hiding is helpful for secure keeping of secret images and covert communication.

In order to create this type of a mosaic image from a secret image, firstly transform the 3-D color space into a new 1-D color scale based on the similarity measure. In this method, the target image database is created for selecting the target image which is most similar to the secret image using the similarity measure. Here, a fast greedy search algorithm is used to determine similar tile image in the secret image to fit into corresponding block in the target image. Tile image fitting sequence is embedded into randomly-selected pixels in the created mosaic image. The information is embedded into the pixels by LSB replacement scheme using a secret key. The secret image cannot be recovered without the secret key. This method is designed for dealing with color images and is extended to create grayscale mosaic images that are useful for hiding text-type grayscale document images.

Yongjian Hu et.al proposed an Image Hiding Scheme Based on 3D Skew Tent Map and Discrete Wavelet Transform [3] in the year 2012. Various data in digital form is transmitted over the Internet network due to the rapid developments of multimedia and network technology. The transmitted data can be a digital representation of text, image, audio and video. The digital images has more security issues, hence it require more attentions. Data encryption and data hiding are two widely used approaches for ensuring the security of the data transmission over the internet. Data encryption is a technique to protect data from unauthorized access by transforming the secret data into meaningless code. Data hiding is a technique in which the secret data is hide into a meaningful host data to make distraction to the observer's attention.

In this method, an image hiding scheme is proposed based on 3D skew tent map and wavelet transform. To encrypt the secret image, one coupled map lattice and one 3D skew tent map with three control parameters are used. This encrypted secret image is embedded in one host image. In order to scramble the pixel positions, generate a chaotic orbit by the skew tent map. A random gray value sequence by the coupled map lattice is yielded to change the gray values. Then, the encrypted secret image and the host image are transformed using the wavelet transform and merged in the frequency domain.

Sara Sajasi et.al proposed a high quality image hiding scheme based upon Noise Visibility Function and an optimal chaotic based encryption method [2] in the year 2013. Information security is plays a major role in multimedia communication due to the rapid growth of transmitting data through public channels such as internet. Steganography is an effective method for securing the systems by embedding secret data in multimedia like images, audios or videos. Cover image is the image in which the secret image is embedded and image which contains the secret image is known as stego-image.

This method improves visual quality of the stego-image and also the security of the secret image by using an image steganographic approach for hiding a secret image in the cover image. This method also provides high embedding capacity. In this method, firstly determine the payload of each region of the cover image to improve the visual quality of the image and to preserve the embedding capacity at an acceptable level. Based on Noise Visibility Function (NVF), the payload is determined. Then, an optimal chaotic based encryption method is used to convert the secret image into an encrypted image. The encryption is performed to ensure the security of the secret image. By using GA/PSO algorithm, the optimal chaotic based encryption method is obtained to find an optimal secret key. Using the, optimal secret key, encrypt the secret image. Such encryption reduces the rate of changes in the stego-image while embedding the secret image which increases the quality of the stego-image.

I-Jen Lai et.al proposed a new type of computer art image called secret-fragment-visible mosaic image [1] in the year 2014. This art image is created by composing small fragments of a secret image to become a target image in a mosaic form. Images contain confidential or private information, hence they should be protected from leakages during transmissions. Many methods have been proposed for secure image transmission. Two common approaches are image encryption and data hiding. Image encryption is the process of encoding secret images in such a way that only authorized parties can view it. The encrypted image is a noise image, so without the correct key the secret image cannot be decrypted. Data hiding is the process of embedding the secret data into the cover images.

The mosaic image is the result of rearrangement of the fragments of a secret image and the preselected target image. No database is required for selecting the target images. After a target image is selected arbitrarily, the given secret image is first divided into rectangular fragments called tile images, which then are fit into similar blocks in the target image, called target blocks, according to a similarity criterion based on color variations. Next, the color characteristic of each tile image is transformed to be that of the corresponding target block in the target image, resulting in a mosaic image which looks like the target image. The proposed method is new in that a meaningful mosaic image is created, in contrast with the image encryption method that only creates meaningless noise images. Also, the proposed method can transform a secret image into a disguising mosaic image without compression.

III. PROPOSED METHOD

The proposed method includes two main phases, mosaic image creation and secret image recovery. In the first phase, mosaic image is created by fitting the secret tile blocks to the corresponding target blocks. Mosaic image contains fragments of secret image with color corrections based on the similarity of the target image. The mosaic image creation includes four stages: fitting the tile images of the secret image into the target blocks of a target image, transformation of the color characteristics of each tile blocks in the secret image to that of the corresponding target block in the target image, based on the minimum RMSE value, rotate each tile images into a direction with respect to corresponding target block, and embeddingthe

DOI 10.17148/IJARCCE.2015.41168

relevant secret information into the mosaic image for the further recovery of the secret image. In the second phase, the secret image is recovered from the secret image by extracting the secret information embedded in the mosaic image. This phase includes two stages: extracting the embedded information from the mosaic image for secret image recovery and recovering the secret image using the extracted information.

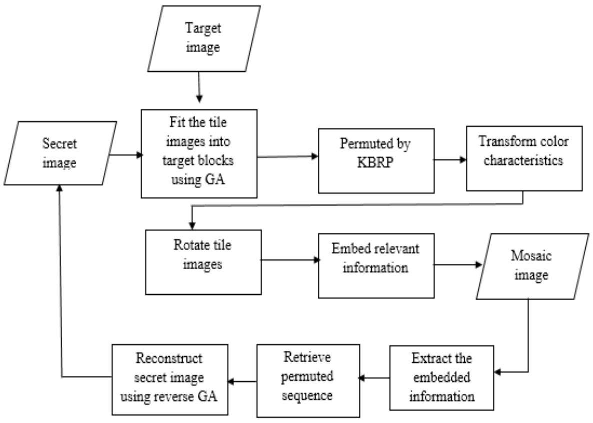

Target image
Secret image
Fit the tile images into target blocks using GA
Permuted by KBRP
Transform color characteristics
Rotate tile images
Embed relevant information
Mosaic image
Reconstruct secret image using reverse GA
Retrieve permuted sequence
Extract the embedded information

Fig.2. Flowchart of the proposed method

IV. MOSAIC IMAGE CREATION USING GA

Steps involved in the creation of the mosaic image are discussed in this section.

A. Color Transformation between Blocks

In the first phase, both the secret image and the selected target image is divided into equal number of blocks. Then, each tile image T in the secret image is fit into the corresponding target block B of the target image. The color characteristics of secret tile blocks and target tile blocks are different from each other. In order to make the mosaic image similar to the target image, color transformation is performed. For color transformation, color scheme is applied which converts the color characteristic of an image to be that of another in the lαβ color space. This technique is applied in this method, 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.

Let T and B be two pixel sets of secret image and target image, $\{P_1, P_2,\ldots, P_n\}$ and $\{P_1', P_2',\ldots, P_n'\}$, respectively. 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'). Firstly, calculate the means and standard deviations of T and B in each of the three color channels R, G, and B by the following formulas.

$$\mu_c = \frac{1}{n}\sum_{i=1}^{n} C_i \qquad (1)$$

$$\mu_c' = \frac{1}{n}\sum_{i=1}^{n} C_i' \qquad (2)$$

$$\sigma_c = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(C_i - \mu_c)^2} \qquad (3)$$

$$\sigma_c' = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(C_i' - \mu_c')^2} \qquad (4)$$

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

$$C_i'' = q_c\left(C_i - \mu_c\right) + \mu_c' \qquad (5)$$

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. To compute the original color values (r_i, g_i, b_i) from the new ones (r''_i, g''_i, b''_i), use the following formula which is the inverse of (eq. [5]):

$$C_i = (1/q_c)\left(C_i'' - \mu_c'\right) + \mu_c \qquad (6)$$

In order to recover the original secret image, sufficient information about the new tile image T' have to embed into the created mosaic image. For this, use (eq. [6]) to compute the original pixel value of p_i.

However, the mean and standard deviation values in the equation are all real numbers. It is impractical to embed real numbers, each with many digits, in the generated mosaic image. So, limit the numbers of bits used to represent relevant parameter values in (eq. [5]) and (eq. [6]). 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 (eq. [5]) to have 7 bits with its value in the range of 0.1 to 12.8. That is, each mean value should change to the value in the range of 0 to 255, and each q_c is changed to value in the range of 0.1 to 12.8. Do not allow q_c to be 0 because otherwise the original pixel value cannot be recovered by using (eq. [6]) for the reason that $1/q_c$ in (eq. [6]) is not defined when q_c=0.

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

Choosing an appropriate B for each T is an important issue while transforming the color characteristic of a tile image T similar to the target block B. In order to solve this issue, use the Genetic Algorithm (GA) for selecting the most similar B for each T. Here, PSNR value is taken as the fitness function. Mutation and crossover operations are performed and the optimal mapping sequence is generated. By using that sequence fitting is performed such that, 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.

After fitting the target blocks into the secret tile blocks according to the sequence generated using Genetic Algorithm (GA) and also after the color transformation process, perform the rotation. Rotation is performed in order to improve the similarity between the resulting mosaic image and the target image by rotating T' into one of the four directions, 0°, 90°, 180°, and 270°, which results a rotated version of T'. Rotation is performed according to the minimum root mean square error (RMSE) value with respect to B among the four directions.

C. Handling Overflows/Underflow

After the color transformation process is performed, overflows or underflows will happened to some pixel values in the new tile image T'. In order to solve this problem, convert overflow or underflow values to be non-overflow or non- underflow and compute the value differences as residuals for future recovery of the secret image. That is, convert all the transformed pixel values in T' greater than 255 to be 255, and all those smaller than 0 to be 0. Then, determine the residuals by calculating the differences between the original pixel values and the converted ones and saved as a part of the information associated with T'.

If the pixel values are in between the range 0 to 255, it cannot be distinguished from those with overflow/underflow values during later recovery since all the pixel values with overflows/underflows are converted to be 255 or 0 now. To remedy this, define the residuals of those pixel values which are on the bound to be 0 and record them as well.

From (eq. [5]), if the ranges of residual values are unknown, it causes a problem of deciding how many bits should be required to store a residual. To solve this issue, the residual values are recoded in the untransformed color space instead of the transformed color space. That is, by using the following two formulas, compute first the smallest possible color value C_S in T that becomes larger than 255, as well as the largest possible value C_S in T that becomes smaller than 0, respectively, after the color transformation process has been conducted:

$$C_S = \lceil (1/q_c)(255 - \mu_c{}') + \mu_c \rceil \qquad (7)$$

$$C_L = \lfloor (1/q_c)(0 - \mu_c{}') + \mu_c \rfloor \qquad (8)$$

ext, for an untransformed value c_i which yields an overflow after the color transformation, compute its residual as $|C_i - C_S|$; and for c_i which yields an underflow, compute its residual as $|C_L - C_i|$. Then, the possible values of the residuals of c_i will all lie in the range of 0 to 255 as can be verified. Consequently, simply record each of them with 8 bits.

Algorithm 1 Mosaic image creation

Input: a secret image S, a target image T, and a secret key K.

Output: a secret-fragment-visible mosaic image F.

Step 1: Divide the secret image S and target image T into n tiles.

Step 2: Compute the means and standard deviations of each tile image and each target block for the three color channels.

Step 3: Map the images using a mapping sequence L generated using Genetic Algorithm.

Step 4: Create a mosaic image F by fitting the tile images into the corresponding target blocks according to L.

Step 5: Generate permutation using KBRP

Step 6: Create a counting table with 256 entries.

Step 7: For each pixel in each tile image of mosaic image with color value is transform into new color values.

Step 8: Compute the RMSE values of each color transformed tile image with respect to its corresponding target block after rotating the tile image into each of the directions, 0^o, 90^o, 180^o, and 270^o and select the optimal direction with minimum RMSE value.

Step 9: For each tile image, construct a bit stream Mi for recovering tile image. The data items included in the bit stream are the index of the corresponding target block, the optimal rotation angle, the mean and standard deviation quotients overflows/underflows residuals.

Step 10: Concatenate the bit streams of all tile images to form total bit stream Mt. Use a secret key to encrypt the bit stream Mt into another bit stream Mt' and embed into the mosaic image.

Step 11: Construct a bit stream I including the number of iterations Ni for embedding Mt' and the number of pixel pairs Npair used in last iteration.

D. Genetic Algorithm

In this method, Genetic Algorithm (GA) is used for achieving additional security, robustness and also to improve the clarity of the image. Here, mosaic image is created by hiding the tiles of secret image into the arbitrarily selected target by using GA. In this method, GA is used to generate a mapping sequence for fitting the tiles of the secret image into the target blocks. Genetic Algorithms are an optimization techniques and adaptive heuristic search techniques that imitate the process of natural evolution. GA is an effective stochastic search method, for robust problem solving which results better than random results. The algorithm involves a predetermined number of generations. Each generation is populated with a predetermined number of fixed length binary strings. Then these binary strings are converted into suitable format that represents parameters as output. One of the major advantage of using Genetic Algorithm (GA) is that the problem solving strategy involves strings to direct the search. So, they can operate well on search spaces that have gaps, jumps, or noise and also they do not require any problem-specific knowledge of the search space.

Genetic Algorithm (GA) operations are based on the population size and the number of generations. If the number of generation in GA increases, the time required to achieve the optimal result will also increases. Another advantage of GA is that if the inputs varied slightly or reasonable noise is present, it does not affect the result to a great extent. The algorithm begins with the initial population which contains a set of solutions. The new population is formed by taking the solutions from one population. The solutions are selected according to their fitness value to form new solutions. This iterations are is repeated until some condition is satisfied.

In this method, firstly determine the population size and the maximum generation size. Then, create an initial population. A random permutation sequence is generated for each individual. In this method, PSNR value is taken as the fitness value. So, calculate the PSNR values of each block. Based on the PSNR value of each block, determine the fitness value and select the fittest individuals. Generic operations such as mutation and crossover are performed and replace the population with a new one.

DOI 10.17148/IJARCCE.2015.41168

The Genetic Algorithm (GA) optimizes the image quality and improves security of the data. In this method, each pixel in a block is considered as a chromosome. In genetic algorithm an initial population of the first generation is generated by taking some chromosomes of a block. In order to select the best chromosomes, several generations of chromosomes are created by using the fitness function to replace the original chromosomes. By flipping the second or third lowest bit in the chromosomes, reproduction randomly duplicates some chromosomes. After the first generation, several second generation chromosomes are generated. Crossover operation is performed by randomly selecting two chromosomes. By combining these two chromosomes, new chromosomes are generated. Crossover is performed in order to eliminate duplication in the generations. Mutation operation changes the bit values and exchanges any two genes to generate new chromosome. If once the selection, reproduction and mutation is completed, the next block is evaluated. Several iterations are performed in order to optimize the value using the fitness function.

Algorithm 2 Creating the mapping sequence

```
Input: Target image, Secret image.
Output: Mapping sequence.
Step 1: Determine the population size and maximum generation size.
Step 2: [Start] Generate initial population of n chromosomes. A pixel in each block is the chromosome.
Step 3: [Fitness] Evaluate the PSNR value of each block and set as the fitness function f(x).
Step 4: [New Population] Create a new population by repeating the following steps until the new population is complete.
Step 5: [Selection] Select two parent chromosomes from a population according to their fitness.
Step 6: [Crossover] With a crossover probability, crossover the parents to form a new offspring. If no crossover is performed offsprings is the exact copy of the parents.
Step 7: [Mutation]With a mutation probability, mutate new offspring at each locus.
Step 8: [Accepting] Place new offspring in the new Population.
Step 9: [Replace] Use new generated population for a further run of the algorithm.
Step 10: [Test] If the end condition is satisfied, stop, and return the best solution in current population.
Step11: [Loop] Go to step 2.
```

E. Key Based Random Permutation

Key Based Random Permutation (KBRP) is a permutation method that can generate one permutation of size N out of N! permutations. The permutation is generated from a key, which is an alphanumeric string by considering all the elements of the key in the permutation generation process. The generated permutation is stored in one dimensional array. The size of the array is same as that of the permutation size (N). The KBRP process three consecutive steps: init(), eliminate(), and fill().

Algorithm 3 Key Based Random Permutation

```
Input: Key K.
Output: An array that contain modified ASCII value of input key K.
Step 1: Store the ASCII value of key in an array A.
Step 2: Do step 3 until length of key.
Step 3: Add P[i] and P[i+1].
Step 4: Keep the value at first location of A to P[S].
Step 5: Repeat step 6 to 9 until S is greater than N.
Step 6: Increment value of S and store it.
Step 7: Repeat step 8 and 9 for i starting from 1 to S-1.
Step 8: Repeat step 9 for K starting from i to S-1 and the values of j less than or equal to N.
Step 9: Add P[i] and P[k+1] and increment value of j.
Step 10: Compute P[i]mod N and store result in P[i].
Step 11: Initialize left with 1 and right with size of array.
Step 12: Repeat steps 3 to 5 until left less than right.
Step 13: If P[left]==P[i], set P[i] to zero.
Step 14: If P[right]==P[j], set P[j] to zero.
Step 15: Increment left by 1 and decrement j by 1.
Step 16: Let m be the number of missing values in array A.
Step 17: Initialize i to 0.
Step 18: Repeat the following steps until i is greater than m.
Step 19: Store the value of N to j.
Step 20: Decrement value of j until P[i] becomes 0 and j less than 0.
Step 21: If j greater than 0, store value of A[i] to P[i] and increment value of i.
Step 22: Initialize K to 1.
Step 23: Increment value of K until P[K] becomes 0 and K greater than N.
Step 24: If K less than or equal to N, store value of A[i] to P[K] and increment value of i.
```

In the first step, init(),initialize array of size N with elements from the given key. Then store the element in the key in the array consecutively by taking the ASCII code of the elements in the key. To complete the elements of the array, add consecutive values of the array and the result is add into the array. This process will continue until all the elements of the array are set to values. By applying the mode operation, all values are set to the range 1 to N.

In the second step, eliminate(), eliminate the repeated values by replacing them with value of zero and keep only the value that is not repeated. In the last step, fill(),replace all zero values with nonzero values in the range 1 to N which are not exist in the array. Now the resulted array represents the permutation.

E. Embedding Information for Secret Image Recovery

After mosaic image is created, embed some secret relevant recovery information into the mosaic image in order to recover the secret image from the mosaic image. For embedding the recovery information, a technique proposed by Coltuc and Chassery [11] is adopted and apply it to the least significant bits (LSB) of the pixels in the mosaic image to perform data embedding. In this method, instead of using classical LSB replacement methods, the reversible contrast mapping method [11] is used for data embedding. Reversible Contrast Mapping (RCM) method applies simple integer transformations to pairs of pixel values. The RCM method performs forward and backward integer transformations, in which (x, y) are a pair of pixel values and (x', y') are the transformed ones.

$$x'=2x-y,\ y'=2y-x \qquad (9)$$

$$x=\left\lceil \frac{2}{3}x' + \frac{1}{3}y' \right\rceil, y=\left\lceil \frac{1}{3}x' + \frac{2}{3}y' \right\rceil \qquad (10)$$

```
Algorithm 4 Secret information embedding
Input: mosaic image, secret bit streams.
Output: Secret information embedded mosaic image.
Step 1: Partition the image into pairs of pixels.
Step 2: For each pair(x,y), perform the following step according to the conditions.
Step 3: If (x,y) ϵ Dc and are not both odd pixel values, transform the pair by the forward RCM.
Step 4: Set LSB of x' to 1 and embed data into the LSB of y'.
Step 5: If (x,y) ϵ Dc and are both odd pixel values, transform the pair by the forward RCM.
Step 6: Set LSB of x' to 0 and embed data into the LSB of y'.
Step 7: If (x,y) not belongs to Dc, set the LSB of x to 0 and save the true value.
```

```
Algorithm 5 Secret information recovery
Input: mosaic image.
Output: Secret information.
Step 1: Partition the image into pairs of pixels.
Step 2: For each pair (x', y'), perform the following step according to the conditions.
Step 3: If the LSB of x' is 1, perform step 4 to 6.
Step 4: Extract the LSB of y'.
Step 5: Set LSBs of (x', y') to 0 and transform by inverse RCM.
Step 6: If the LSB of x' is 0 and ϵ Dc perform step 7 and 8.
Step 7: Extract the LSB of y'.
Step 8: Set LSBs of (x', y') to 1 and transform by inverse RCM.
Step 9: If the LSB of x' is 0 and (x', y') with the LSBs set to 1 does not belong to Dc, perform step 10.
Step 10: Replace LSB of x' with the corresponding true value.
```

The Reversible Contrast Mapping (RCM) method provides high data embedding capacities and has lowest complexity. The information required to recover the secret image from the mosaic image includes: the index of the target block, the optimal rotation angle of target image, mean and standard deviation quotients of the secret image and the target image, and finally the overflow/underflow residuals. These recovery information for recovering the tile image are integrated a five-component bit stream of the form

$$M=t_1t_2\ldots t_mr_1r_2m_1m_2\ldots m_{48}q_1q_2\ldots q_{21}d_1d_2\ldots d_k$$

the bit streams $t_1t_2\ldots t_m$, r_1r_2 , $m_1m_2\ldots m_{48}$, $q_1q_2\ldots q_{21}$ and $d_1d_2\ldots d_k$ represent the values of the index of B, the rotation angle of T, the means of T and B, the standard deviation quotients, and the residuals, respectively. The index of B needs m bits to represent and m is computed by

$$m=\lceil\log[(W_S\times H_S)/N_T]\rceil$$

$W_S$and $H_S$are respectively the width and height of the secret image S, and N_T is the size of the target image T. Two bits are required to represent the rotation angle of the target image because there are four possible rotation directions. 48 bits are required to represent the means of secret image and the target image because it use 8 bits to represent a mean value in each color channel. 21 bits are required to represent the standard deviation quotients of the secret image and the target image because it use 7 bits to represent a mean value in each color channel. The total number k of required bits for representing all the residuals depends on the number of overflows or underflows in T'.

Then, concatenate all the above-defined bit streams of all the tile images in the same order into a total bit stream M_t for the entire secret image. In order to protect the concatenated bit steam M_t from attacks, encrypt the concatenated bit stream with a secret key to obtain an encrypted bit stream M'_t. This encrypted bit stream is embedded into the pixel pairs in the mosaic image using the method of Coltuc and Chassery [11]. Embedding the bit stream require more than one iteration in the encoding process since the length of M'_t may be larger than the number of pixel pairs available in an iteration.

In the secret image recovery process some other related information about the mosaic image generation process have to embed into the mosaic image. Such information is denoted as as a bit stream I. The bit stream I includes the data items such as the number of iterations performed for embedding the bit stream M'_t, and the total number of pixel pairs used in the last iteration for embedding M'_t.

By using the the bit stream M'_t embedded into the mosaic image, the secret image can be recovered from the mosaic image. It is noted that some loss will be incurred in the recovered secret image, or more specifically, in the color transformation process using (eq. [5]), where each pixel's color value c_i is multiplied by the standard deviation quotient q_c, and the resulting real value c_i'' is truncated to be an integer in the range of 0 through 255.

However, because each truncated part is smaller than the value of 1, the recovered value of c_i using (eq. [6]) is still precise enough to yield a color nearly identical to its original one. Even when overflows/underflows occur at some pixels in the color transformation process, record their residual values as described previously and after using (eq. [6]) to recover the pixel value c_i, add the residual values back to the computed pixel values c_i to get the original pixel data, yielding a nearly losslessly recovered secret image.

```
Algorithm 6 Secret image recovery
Input: a mosaic image F with n tile images and the secret key K.
Output: the secret image S.
Step 1: Extract the bit stream I from the mosaic image using the reverse RCM to obtain the number of iterations for embedding Mt' and the total number of pixel pairs
```

used in the last iteration.

Step 2: Extract the bit stream Mt’ using the values of Ni and Npair.

Step 3: Decrypt the bit stream Mt’ into Mt by K.

Step 4: Decompose Mt into n bit streams.

Step 5: Decode Mi for each tile image to obtain the index of the target blocks, the optimal rotation angle, the means and standard deviation quotients and the overflow/underflow residual values.

Step 6: Recover one by one in a raster-scan order the tile images by the following steps:

1) Rotate the block in the reverse optimal angle,

2) recover the original pixel values using the extracted mean and standard deviation quotients,

3) compute C_S and C_L,

4) find out the pixels with values 255 or 0 which indicate overflow/underflow

5) add respectively the values C_S and C_L to the corresponding residual values of the found pixels and 6) take the results as the final pixel values, resulting in a final tile image.

Step 7: Compose all the final tile images to form the desired secret image S as output.

V. EXPERIMENTAL RESULTS

The output is tested with various inputs. Test is conducted using many secret and target images. The analysis of various parameters is performed with respect to the tile image sizes. The different sizes used for analysis are 4X4, 8X8, 16X16 and 24X24. A comparison with various tile image sizes was done and checks the PSNR, RMSE values and number of bits required for embedding of each one.

The PSNR and the RMSE values of the mosaic image is checked and it is above 30 and RMSE is approximately equal to one indicates that the created mosaic image is similar to the target image.

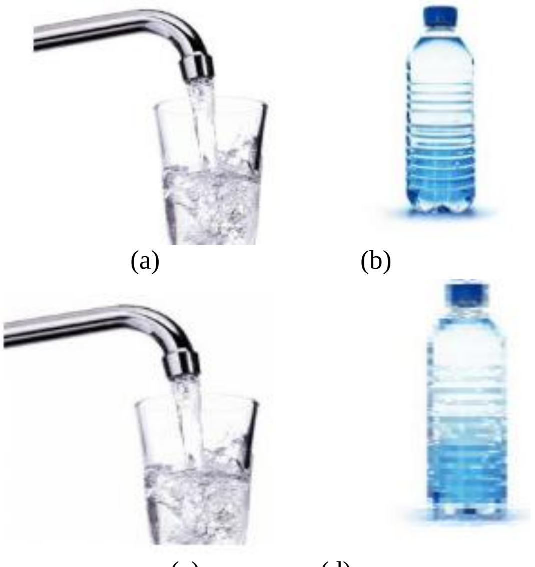

(a) (b)
(c) (d)

Fig. 3. Experimental result of mosaic image creation. (a) Target image. (b) Secret image. (c) Mosaic image created with tile image size 8×8. (d) Recovered secret image

The performance of this method is improved by using color transformations. Color transformation makes the mosaic image color values similar to the target image.

Performance of the mosaic image creation is analyzed using three parameters: Peak-Signal Noise Ratio (PSNR), Root Mean Square Error (RMSE) and numbers of required bits embedded for recovering secret images.

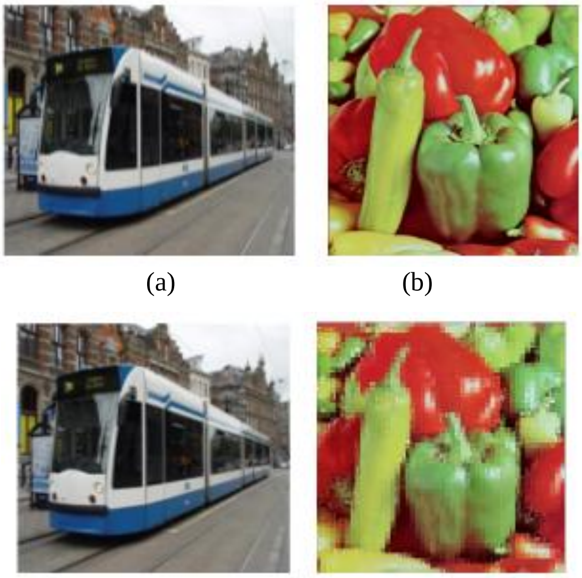

(a) (b)
(c) (d)

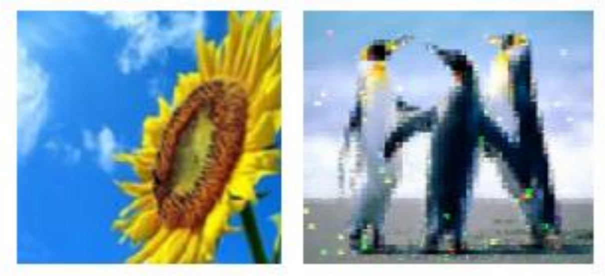
Fig. 4. Experimental result of mosaic image creation. (a) Target image. (b) Secret image. (c) Mosaic image created with tile image size 4×4. (d) Recovered secret image

Performance of the mosaic image creation is analyzed with various inputs. Test is conducted using many secret and target images. The PSNR value of the mosaic image with respect to the target image and the decrypted secret image with respect to the original secret image is evaluated. Similarly the RMSE value of the same is also evaluated.

PSNR is the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. PSNR is an approximation to human perception of reconstruction quality. A higher PSNR generally indicates that the reconstruction is of higher quality. The PSNR value of the mosaic image with respect to the target image and the decrypted secret image with respect to the original secret image are checked and it is above 30 which indicates that the mosaic image is look similar to the target image and the decrypted secret image is similar to the original secret image.

(a) (b)

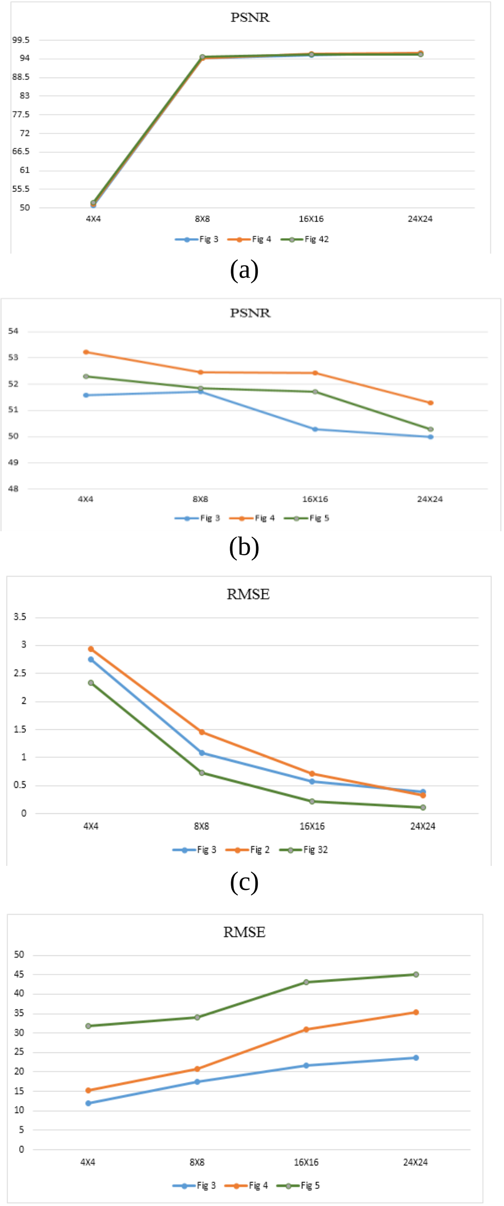
DOI 10.17148/IJARCCE.2015.41168



(c) (d)

Fig.5. Experimental result of mosaic image creation. (a) Target image. (b) Secret image. (c) Mosaic image. (d) Recovered secret image.

Root Mean Square Error (RMSE) is defined as the square root of the mean square difference between the pixel values of the two images. The RMSE values of the mosaic image is checked and it is approximately equal to one indicates that the created mosaic image is similar to the target image.

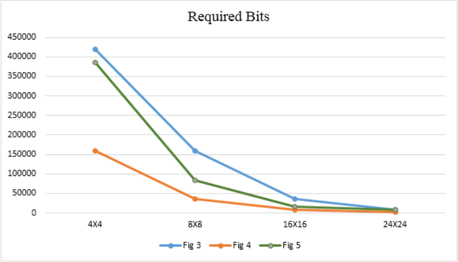


(a)

(b)

(c)

(d)



(e)

Fig. 6. Plots of trends of various parameters versus different tile image sizes (4×4, 8×8, 16×16, 24×24) (a) PSNR values of created mosaic images with respect to target images. (b) PSNR values of recovered secret images with respect to original ones. (c) RMSE values of created mosaic images with respect to target images. (d) RMSE values of recovered secret images with respect to original ones. (e) Numbers of required bits embedded for recovering secret images.

Here, for analysis, RMSE values of created mosaic images with respect to target images and RMSE values of recovered secret images with respect to original ones are calculated. For the performance analysis, the number of bits required to embed the secret data for the recovery of the secret image from the mosaic image is calculated.

Fig. 4 and 5 shows the experimental result of mosaic image creation with tile image size 4×4. Fig. 2 shows the mosaic image creation with tile image size 8×8. Fig. 6 shows the plots of trends of various parameters versus different tile image sizes. PSNR values of created mosaic images with respect to target images, PSNR values of recovered secret images with respect to original ones, RMSE values of created mosaic images with respect to target images, RMSE values of recovered secret images with respect to original ones and the numbers of required bits embedded for recovering secret images are plotted.

VI. CONCLUSION

Images from different sources are utilized and transmitted through the internet for variety of applications. These applications include confidential enterprise archives, military image databases, document storage systems, online personal photograph albums and medical imaging systems. These images contain confidential or private information. Therefore, such information should be protected from leakages while transmitting through internet. Now a days, different methods have been proposed for secure image transmission. The two common approaches are image encryption and data hiding. Image encryption is the process of encoding secret images in such a way that only authorized parties can view it. Data hiding is the process of embedding the secret data into the cover images. The Image encryption technique is based on the natural property of an image like high redundancy and strong spatial correlation. By using these properties, the encrypted image is obtained. The encrypted image is a noise image, so without the correct key the secret image cannot be decrypted. The encrypted image is a meaninglessly that cannot provide additional information

DOI 10.17148/IJARCCE.2015.41168

before decryption. It also make an attacker's attention to the encrypted image during transmission because of its randomness in form. A new secure image transmission method has been proposed using GA and KBRP, which can create meaningful mosaic images and also can transform a secret image into a mosaic image with the same size of the secret image. This method provides more clarity to the image and more security is provided. Secret-fragment-visible mosaic images with very high visual similarities to selected target images can be created by using color transformations and the scheme for handling overflows and underflows in the converted values of the pixels colors. There is no target database is required to select the target images. Also, the original secret images can be recovered nearly losslessly from the created mosaic images.

REFERENCES

[1] Ya-Lin Lee and Wen-Hsiang Tsai, “A New Secure Image Transmission Technique via Secret Fragment-Visible Mosaic Images by Nearly Reversible Color Transformations,” in IEEE, 2014

[2] Xinpeng Zhang, “A high quality image hiding scheme based upon Noise Visibility Function and an optimal chaotic based encryption method”, IEEE Trans. Inf. Forens. Secur., vol. 7, no. 2, pp. 1556-6013, Sep. 2013.

[3] I. J. Lai and W. H. Tsai, “An Image Hiding Scheme Based on 3D Skew Tent Map and Discrete Wavelet Transform,” IEEE Trans. Inf. Forens. Secur., vol. 6, no. 3, pp. 936945, Sep. 2012.

[4] I. J. Lai and W. H. Tsai, “Secret-fragment-visible mosaic image new computer art and its application to information hiding,” IEEE Trans. Inf. Forens. Secur., vol. 6, no. 3, pp. 936945, Sep. 2011.

[5] Manoj Sharma, Manoj Shukla, Amit Kaul, “Image Hiding Using Unitary Similarity Transformation”, IEEE Conference, 978-1-61284-861-7/11, 2011.

[6] Cheng-Hsiang Yeh, Ching-Tang Hsieh, Kuo-Ming Hung, Li-Ming Chen, “Reversible digital image hiding based on multilevel histogram modication and halftoning technique”, IEEE Conference, 1-4577-0653-0/11, 2011.

[7] YongHong ZHANG, “Digital Image hiding using curvelet transform”, IEEE Conference, 978-1-4244-8728-8111, 2011.

[8] Zahra Toony, Hedieh Sajedi and Mansour Jamzad, “Image Hiding Based on Intensity Quantization Using Genetic Algorithm,” IEEE Conference, 978-1-4244-4262-1, 2009.

[9] Zahra Toony Mansour Jamzad, “A novel image hiding scheme using content aware seam carving method,” IEEE Conference, 978-0-7695-3965-2/10, 2010.

[10] Lin-Yu Tseng, Yung-Kuan Chan, Yu-An Ho, Yen-Ping Chu, “Image hiding with an improved genetic algorithm and an optimal pixel adjustment process ,” IEEE Conference, 978-0-7695-3382-7/08, 2008.

[11] D. Coltuc and J.-M. Chassery, “Very fast watermarking by reversible contrast mapping,” IEEE Signal Process. Lett., vol. 14, no. 4, pp. 255258, Apr. 2007.

DOI 10.17148/IJARCCE.2015.41168