ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization *Vol. 5, Special Issue 2, March 2016*

National Conference on Future Technologies in Power, Control and Communication Systems (NFTPCOS-16)

on 10, 11 and 12th March 2016

Organised by

Dept. of EEE, College of Engineering Perumon, Kollam, Kerala – 691601, India

A Loss-Less Data Hiding Scheme Using Mosaic Images

Angitha.G.A [1], Maneesha Mohan M[2]

Assistant Professor, Dept. of ECE, Sivaji College of Engineering and Technology, Manivila, Tamilnadu, India[1]

PG Student [Applied Electronics], Sivaji College of Engineering and Technology, Manivila, Tamilnadu, India [2]

ABSTRACT: Very recent communication system resourcing images from various sources are frequently utilized and transmitted through the internet. The online albums confidential archives, document storage system, medical imaging systems and military image database are frequently used by these system. These images are usually contain private or confidential information so that they should be protected from leakages during transmissions. Image encryption is a technique that makes use of the natural property of an image, such as high redundancy and strong spatial correlation. In the proposed system, a new method for secure image transmission technique is used. Based on this technique a given large volume of secret image is automatically transformed into a 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 camouflage of the secret image, is yielded by dividing the secret image into fragments and transforming their color characteristics to be those in of the corresponding blocks of the target image. By the use of proper pixel color transformations as well as a skillful scheme for handling overflows and underflows in the converted values of the pixels colors, secret fragment visible mosaic images with very high visual similarities to arbitrarily selected target image can be created with no need of a target image data base.Also the original secret image can be recovered nearly lossless from the created mosaic images.

KEYWORDS: Secure image transmission technique, confidential information, Mosaic Image, Fragment- visible mosaic image.

I. INTRODUCTION

In the proposed system 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. Recently, many methods have been proposed for securing image transmission, for which two common approaches are image encryption and data hiding. 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 secretdata, in which the data type of the secret message investigated in this paper is an image.Existing data hiding methods mainly utilizethe techniques of LSB substitution, histogram shifting, difference expansion prediction-error expansion, recursive histogram modification and discrete cosine/wavelet transformations.

However, in order to reduce the distortion of the resulting image, an upper bound for the distortion value is usually set on the payload of the cover image. A discussion on this rate distortion issue can be found. Thus, a main issue of the methods for hiding data in images is the difficulty to embed a large amount of message data into a single image. Specifically, if one wants to hide a secret image into a cover image with the same size, the secret image must be highly compressed in advance. For example, for a data hiding method with an embedding rate of 0.5 bits per pixel, a secret image with 8 bits per pixel must be compressed at a rate of at least 93.75% beforehand in order to be hidden into a cover image.But, for many applications, such as keeping or transmitting medical pictures, military images, legal

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization *Vol. 5, Special Issue 2, March 2016*

National Conference on Future Technologies in Power, Control and Communication Systems (NFTPCOS-16)

on 10, 11 and 12th March 2016

Organised by

Dept. of EEE, College of Engineering Perumon, Kollam, Kerala – 691601, India

documents, etc., that are valuable with no allowance of serious distortions, such data compression operations are usually impractical. Moreover most image compression methods, such as JPEG compression, are not suitable for line drawings and textual graphics, in which sharp contrasts between adjacent pixels are often destructed to become noticeable artifacts. In this paper, a new technique for secure image transmission is proposed, which transforms a secret image into a meaningful mosaic image with the same size 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.

The proposed method is inspired by Lai and Tsai. in which a new type of computer art image, called secret-fragment-visible mosaic image, was proposed. The mosaic image is the result of rearrangement of the fragments of a secret image in disguise of another image called the target image preselected from a database. But an obvious weakness of Lai and Tsai is the requirement of a large image database so that the generated mosaic image can be sufficiently similar to the selected target image. Using their method, the user is not allowed to select freely his/her favorite image for use as the target image. It is therefore desired in this study to remove this weakness of the method while keeping its merit, that is, it is aimed to design a new method that 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.

Specifically, 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 ofeach tile image is transformed to be that of the correspondingtarget block in the target image, resulting in a mosaic image whichlooks like the target image. Relevant schemes are also proposed to conduct nearly lossless recovery of the original secret image from the resulting mosaic image. The proposed method is new in that a meaningful mosaic image is created, in contrast with the image encryption method that only creates meaningless noise images. Also, the proposed method can transform a secret image into a disguising mosaic image without compression, while a data hiding method must hide a highly compressed version of the secret image into a cover image when the secret image and the cover image have the same data volume.

II. RELATED WORK

Data Hiding

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. The worst case mean-square-error between the stego-image and the cover-image is derived. In this paper, a data hiding scheme by simple LSB substitution with an optimal pixel adjustment process (OPAP) is proposed. The basic concept of the OPAP is based on the technique proposed.. In this paper, 8-bit grayscale images are selected as the covermedia. These images are called cover-images. Cover-images with the secret messagesembedded in them are called stego-images. For data hiding methods, the image quality refers to the quality of the stego-images. A novel reversible data hiding algorithm, which can recover the original image without any distortion from the marked image after the hidden data have been extracted, is presented in this paper. This algorithm utilizes the zero or the minimum points of the histogram of an image and slightly modifies the pixel grayscale values to embed data into the image. It can embed more data than many of the existing reversible data hiding algorithms. This lower bound of PSNR is much higher than that of all reversible data hiding techniques reported in the literature. The computational complexity of this proposed technique is low and the execution time is short. Reversible data hiding facilitates immense possibility of applications to link two sets of data in such a way that the cover media can be losslessly recovered after the hidden data have been extracted out, thus providing anadditional avenue of handling two different sets of data. The algorithm has been successfully applied to a wide range of images, including commonly used images, medical images, texture images, aerial images and all of the 1096 images in CorelDraw database.

Reversible data embedding, which is also called lossless data embedding, embeds invisible data (which is called a payload) into a digital image in a reversiblefashion. as a basic requirement, the qualitydegradation on the image after data embedding should be low. an intriguing feature of reversible data embedding is the reversibility, that is, one can remove the embedded data to restore the original image. from the information hiding point of view, reversible data embedding hides some information in a digital image in such a way that an authorized party could decode the hidden information and also restore the image to its original, pristine state. . In this paper, a novel reversible data embedding

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization *Vol. 5, Special Issue 2, March 2016*

National Conference on Future Technologies in Power, Control and Communication Systems (NFTPCOS-16)

on 10, 11 and 12th March 2016

Organised by

Dept. of EEE, College of Engineering Perumon, Kollam, Kerala – 691601, India

method for digital images has been proposed. This explore the redundancy in digital images to achieve very high embedding capacity, and keep the distortion low.Current difference-expansion (DE) embedding techniques perform one layer embedding in a difference image. They do not turn to the next difference image for another layer embedding unless the current difference image has no expandable differences left. Based on integer Haar wavelet transform, this paper propose a new DE embedding algorithm, which utilizes the horizontal as well as vertical difference images for data hiding. This paper introduces a dynamical expandable difference search and selection mechanism. This mechanism gives even chances to small differences in two difference images and effectively avoids the situation that the largest differences in the first difference image are used up while there is almost no chance to embed in small differences of the second difference image. The advantage of this algorithm is more obvious near the embedding rate of 0.5 bpp.

A high capacity reversible image data hiding scheme is proposed based on a generalization of prediction-error expansion (PEE) and an adaptive embedding strategy. For each pixel, its prediction value and complexity measurement are firstly computed according to its context. Then, a certain amount of data bits will be embedded into this pixel by the proposed generalized PEE. Here, the complexity measurement is partitioned into several levels, and the embedded data size is determined by the complexity level such that more bits will be embedded into a pixel located in a smoother region. The complexity level partition and the embedded data size of each level are adaptively chosen for the best performance with an advisable parameter selection strategy. In this way, the proposed scheme can well exploit image redundancy to achieve a high capacity with rather limited distortion.

A high capacity reversible image watermarking scheme based on integer-to-integer wavelet transforms. This scheme divides an input image into non overlapping blocks and embeds a watermark into the high-frequency wavelet coefficients of each block. The conditions to avoid both underflow and overflow in the spatial domain are derived for an arbitrary wavelet and block size. The payload to be embedded includes not only messages but also side information used to reconstruct the exact original image. To minimize the mean-squared distortion betweenthe original and the watermarked images given a payload, the watermark is adaptively embedded into the image. The experimental results show that this scheme achieves higher embedding capacity while maintaining distortion at a lower level.Tominimize the mean squared distortion between the original and the watermarked images givena payload, the watermark is adaptively embedded into the image.

MosaicImage

A new type of computer art image called secret-fragment-visible mosaic image is proposed, which is created automatically by composing small fragments of a givenimage to become a target image in a mosaic form, achieving aneffect of embedding the given image visibly but secretly in theresulting mosaic image. This effect of information hiding is usefulfor covert communication or secure keeping of secret images. A fast greedy searchalgorithm is proposedto find a similar tile image in the secret image to fit into each blockin the target image. The information of the tile image fittingsequence is embedded into randomly-selected pixels in the createdmosaic image by a lossless LSB replacement scheme using a secretkey.

A Capacity and invisibility are two targets of the methods for information hiding. Because these two targets contradict each other, to hide large messages into the cover image and remain invisible is an interesting challenge. The simple least-significant-bit (LSB) substitution approach, which embeds secret messages into the LSB of pixels in cover images, usually embeds huge secret messages. After a large message is embedded, the quality of the stego-image will be significantly degraded. In this paper, a new LSB-based method, called the inverted pattern (IP) LSB substitution approach,is proposed to improve the quality of the stego-image. Each section of secret images is determined to be inverted or not inverted before it is embedded. The decisions are recorded by an IP for the purpose of extracting data and the pattern can be seen as secret key or an extra data to be re-embedded.

III. SYSTEM OVERVIEW

Image encryption is a techniques that makes use natural properties of image, such as high image encryption is a technique that makes use of the natural property of an image such as highredundancy 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 canobain the secret image from it unless he/she has the correct keys. 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.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization Vol. 5, Special Issue 2, March 2016

National Conference on Future Technologies in Power, Control and Communication Systems (NFTPCOS-16)

on 10, 11 and 12th March 2016

Organised by

Dept. of EEE, College of Engineering Perumon, Kollam, Kerala – 691601, India

The method is new in that a meaningful mosaic image is created, in contrast with the image encryption method that only creates meaningless noise images. Also, the proposed method can transform a secret image into a disguising mosaic image without compression, while a data hiding method must hide a highly compressed version of the secret image into a cover image when the secret image and the cover image have the same data volume. a mosaic image is yielded, which consists of the fragments of an input secret image with color corrections according to a similarity criterion based on color variations.

The mosaic image generation includesfourstages: 1) fitting the tile images of the secret image into the target blocks of a preselected target image 2) Transforming the color characteristic of each tile image in the secret image to become that of the corresponding target block in the target image 3) rotating each tile image into a direction with the minimum RMSE value with respect to its corresponding target block and 4) Embedding relevant information into the created mosaic image for future recovery of the secret image.

In the first stage 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. More specifically, let *T* and *B* be described as two pixel sets *{p*1, *p*2, . . . ,*pn}* and *{p*_1, *p*_ 2, . . . , *p*_*n}*, respectively. Let n the color of each *pi* be denoted by (*ri*, *gi*, *bi*) and that of each *p*_*i* by (*r*_*i*, *g*_*i*, *b*_*i*). The means can be calculated by the equations given below,

$$\mu_c = \frac{1}{n}\sum_{i=1}^{n} c_i \quad (3.1)$$

$$\mu'_c = \frac{1}{n}\sum_{i=1}^{n} c'_i \quad (3.2)$$

The standard deviation of T and B can be calculated by,

$$\sigma_c = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(c_i - \mu_c)^2} \quad (3.3)$$

$$\sigma'_c = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(c'_i - \mu'_c)^2} \quad (3.4)$$

in which *ci* and *c*_ *i* denote the C-channel values of pixels *pi*and *p*_*i*, respectively, with *c* = *r*, *g*, or *b* and C=R, G, or B. New color values $(r_i^{"}, g_i^{"}, b_i^{"})$ for each p_i in T can be calculated using the equation 3.5,

$$c_i^{"} = q_c(c_i - \mu_c) + \mu'_c \quad (3.5)$$

in which $q_c = \sigma'_c/\sigma_c$ is 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.

The original color values (r_i ,g_i, b_i) of p_i from the new ones ($r_i^{"}, g_i^{"}, b_i^{"}$) can be computed by the equation6 given below,

$$c_i = (1/q_c)\left(c_i^{"} - \mu'_c\right) + \mu_c \quad (3.6)$$

Furthermore, 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. 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, the numbers of bits used to represent relevant parameter values in (3.5) and (3.6) are limited. 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 to255, and the standard deviation quotient qc in (3.5) 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.

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, use the standard deviation of the colors in the block as a measure to select the most similar B for each T.

By using the following two formulas, first the smallest possible color value c_S (with c=r, g, orb) in T that becomes larger than 255, as well as the largest possible value c_L in T that becomes smaller than 0, respectively, can be computed after the color transformation process has been conducted:

$$c_s = [(1/q_c)(255 - \mu'_c) + \mu_c] \quad (3.7)$$

$$c_L = [(1/q_c)(0 - \mu'_c) + \mu_c] \quad (3.8)$$

For the rotation and fixing of the secret image on to the target image Root Mean Square Error should be calculated. The RMSE value can be calculated by the equation ,

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization *Vol. 5, Special Issue 2, March 2016*

National Conference on Future Technologies in Power, Control and Communication Systems (NFTPCOS-16)

on 10, 11 and 12th March 2016

Organised by

Dept. of EEE, College of Engineering Perumon, Kollam, Kerala – 691601, India

$$RMSE = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(y_i - \hat{y}_i)^2} \quad (3.9)$$

The root-mean-square deviation (RMSD) or root-mean-square error (RMSE) is a frequently used measure of the differences between values (sample and population values) predicted by a model or an estimator and the values actually observed. The RMSD represents the sample standard deviation of the differences between predicted values and observed values. These individual differences are called residuals when the calculations are performed over the data sample that was used for estimation, and are called prediction errors when computed out-of-sample. RMSD is a good measureof accuracy, but only to compare forecasting errors of different models for a particular variable and not between variables, as it is scale-dependent.

A secure image transmission technique is proposed. Target image, secret image and secret key are used. The color characteristics of the target and secret image are considered in the proposed system . The proposed system can transform secret imageinto mosaic image without compression The mosaic image consists of the fragments of an input secret image with color corrections according to a similarity criterion based on color variations. The mosaic imagegeneration includes four stages: 1) fitting the tile images of the secret image into the target blocks of a preselected target image; 2) transforming the colorcharacteristic of each tile image in the secret image to become that of the corresponding target block in the target image; 3) rotating each tile image into a direction with the minimum RMSE value with respect to its corresponding target block; and 4) embedding relevant information into the created mosaic image for future recovery of the secret image.

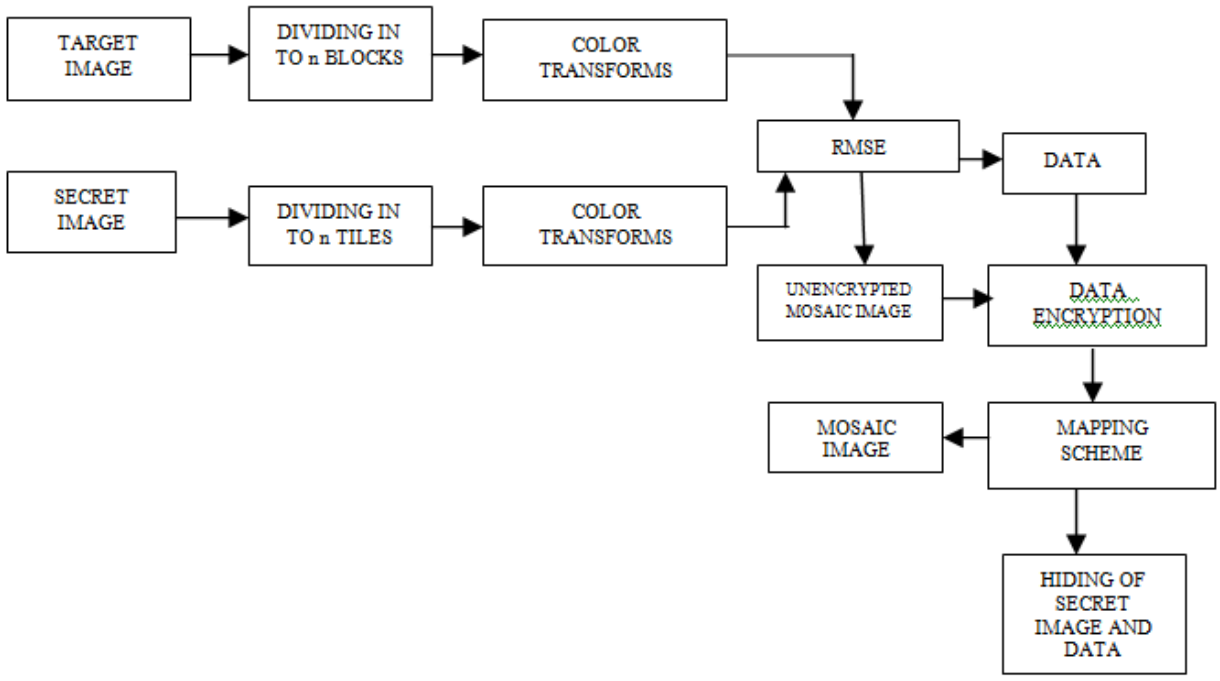

Fig.1 : Block diagram of data hiding

In the first phase, a mosaic image is yielded, which consistsof the fragments of an input secret image with color corrections according to a similarity criterion based on color variations. The phase includes four stages: 1) fitting the tile images of the secret image into the target blocks of a preselected target image; 2) transforming the color characteristic of each tileimage in the secret image to become that of the correspondingtarget block in the target image; 3) rotating each tile imageinto a direction with the minimum RMSE value with respectto its corresponding target block; and 4) embedding relevantinformation into the created mosaic image for future recoveryof the secret image. In the second phase, the embeddedinformation is extracted to recover nearly losslessly the secretimage from the generated

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization *Vol. 5, Special Issue 2, March 2016*

National Conference on Future Technologies in Power, Control and Communication Systems (NFTPCOS-16)

on 10, 11 and 12th March 2016

Organised by

Dept. of EEE, College of Engineering Perumon, Kollam, Kerala – 691601, India

mosaic image. The phase includestwo stages: 1) extracting the embedded information for secretimage recovery from the mosaic image, and 2) recovering thesecret image using the extracted information.

IV. SIMULATION RESULTS

The performance of the proposed system results are analyzed by simulating the targetand secret image in MATLAB. The inputs are the target and secret image.

fig a. secret image

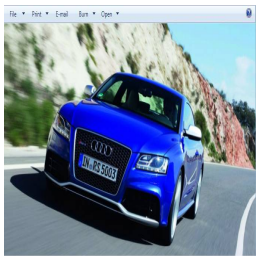

fig b.target image

Fig a. shows the input secret image that is used for analyzing the performance of the proposed system. The secret image is of the JPEG format and it is in RGB color space.Fig b. shows the input target image in which the secret image shown in fig4.1. is to be hided. Target image is used as the base image in which the secret images to be hided. The target image chosen arbitrarily i.e. the user can chose an image based on his/her interest. As the secret image, the target image is also in RGB format with JPEG compression standard. The RGB color model is an additive color model in which red, green, and blue light are added together in various ways to reproduce a broad array of colors.

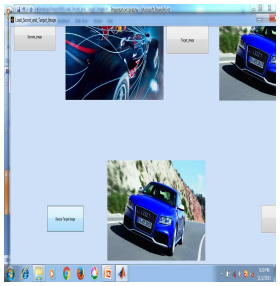

Fig c.Resized target image

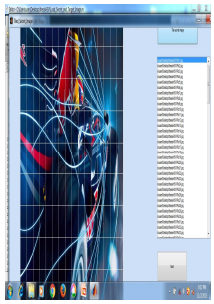

Fig d .Tiled secret image

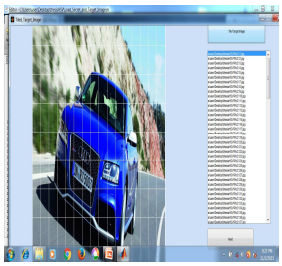

Fig e. Target image blocks

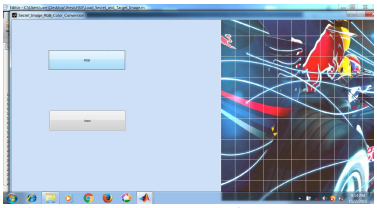

Fig.f. Color Conversion of secret image.

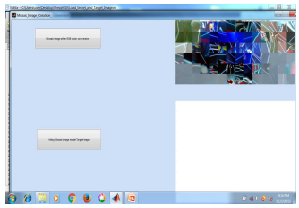

Fig.g Unencrypted mosaic image

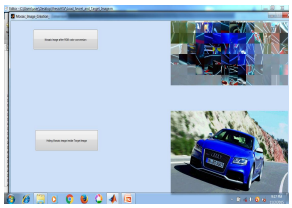

Fig h.Encrypted mosaic image

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization *Vol. 5, Special Issue 2, March 2016*

National Conference on Future Technologies in Power, Control and Communication Systems (NFTPCOS-16)

on 10, 11 and 12th March 2016

Organised by

Dept. of EEE, College of Engineering Perumon, Kollam, Kerala – 691601, India

Fig c. shows the resized target image. The resizing is done to the target image based on the input secret image(Fig a.). The secret image size is not changed because any change in the size of the secret image will result in the loss of data. The target image should be resized based on the size of secret image. Then the target image is divided into n blocks of size 256×256 or according to the size of the tile secret image. Then the color transformation is applied to each block of the target image. Fig d. shows the secret image(Fig a.)which isconverted to n- number of tiles. The tiling of the secret image is done inorder to hide the secret image into the target image. Secret image is the image which is to be transmitted to the receiver more securely. The secret image encapsulated within the target image. The secret image is should not be resized based on the target image because any loss in the secret image will result in the loss of large information. The tile can be of the size 16×16, 24×24,32×32,8×8,40×40 etc. Fig e shows the target image (b) which is converted to n number of blocks. To these bocks tiled secret image is fixed. The target image should be resized based on the size of secret image. Then the target image is divided into n blocks of size 256×256 or according to the size of the tile secret image. Fig(f) shows the color conversion of secret image. Color conversion is applied to each tile of the secret image. RGB is a device-dependent color model: different devices detect or reproduce a given RGB value differently, since the color elements (such as phosphors or dyes) and their response to the individual R, G, and B levels vary from manufacturer to manufacturer, or even in the same device over time.Thus an RGB value does not define the same color across devices without some kind of color management.

Figure(g) shows the unencrypted mosaic image which consists of combination of target image and secret image. Here no encrypted data is attached this mosaic image. Encryption does not of itself prevent interception, but denies the message content to the interceptor. In an encryption scheme, the intended communication information or message, referred to as plaintext, is encrypted using an encryption algorithm, generating cipher text that can only be read if decrypted

Fig h. shows the encrypted mosaic image which consist of combination of target image and secret image have encrypted data. Encrypted data consists of index, optimal rotation angle, truncated means, standard deviation quotients, underflow residuals. Encryption is a technique for transforming information on a computer in such a way that it becomes unreadable. So, even if someone is able to gain access to a computer with personal data on it, they likely won't be able to do anything with the data unless they have complicated, expensive software or the original data key. Encryption can help ensure that data doesn't get read by the wrong people, but can also ensure that data isn't altered in transit, and verify the identity of the sender.

V. CONCLUSION

A new secure image transmission method has been proposed, which not only can create meaningful mosaic images but also can transform a secret image into a mosaic one with the same data size for use as a camouflage of the secret image. By the use of proper pixel color transformations as well as a skillful scheme for handling overflows and underflows in the converted values of the pixels' colors, secret-fragment visible mosaic images with very high visual similarities to arbitrarily-selected target images can be created with no need of a target image database. Also, the original secret images can be recovered nearly losslessly from the created mosaic images. 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. The proposed method in which a new type of computer art image, called secret-fragment-visible mosaic image, was proposed. The mosaic image is the result of rearrangement of the fragments of a secret image in disguise of another image called the target image preselected from a database. The proposed method can transform a secret image into a disguising mosaic image without compression, while a data hiding method must hide a highly compressed version of the secret image into a cover image when the secret image and the cover image have the same data volume. The retrieval of the secret image from the mosaic image generated in this phase. The secret image retrieval uses the secret data encapsulated within the mosaic image. The secret image and the target images can be retrieved without any lose using the data.

REFERENCES

[1] J. Fridrich, "Symmetric ciphers based on two-dimensional chaoticmaps," *Int. J. Bifurcat. Chaos*, vol. 8, no. 6, pp. 1259 1284, 1998.
[2] G. Chen,Y. Mao, and C. K. Chui, "A symmetric image encryptionscheme 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 encryptionapproach based on chaotic maps," *Chaos Solit. Fract.*, vol. 24, no. 3,pp. 759–765, 2005.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization *Vol. 5, Special Issue 2, March 2016*

National Conference on Future Technologies in Power, Control and Communication Systems (NFTPCOS-16)

on 10, 11 and 12th March 2016

Organised by

Dept. of EEE, College of Engineering Perumon, Kollam, Kerala – 691601, India

[4] H. S. Kwok and W. K. S. Tang, "A fast image encryption system basedon chaotic maps with finite precision representation,"*Chaos Solit. Fract.*,vol. 32, no. 4, pp. 1518–1529, 2007.
[5] S. Behnia, A. Akhshani, H. Mahmodi, and A. Akhavan, "A novelalgorithm 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 chaosbasedimage encryption algorithm," *Chaos Solit. Fract.*, vol. 40, no. 5,pp. 2191–2199, 2009.
[7] V. Patidar, N. K. Pareek, G. Purohit, and K. K. Sud, "A robustand secure chaotic standard map based pseudorandom permutationsubstitutionscheme 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 LSBsubstitution," *Pattern Recognit*.., vol. 37, pp. 469–474, Mar. 2004.
[9] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," *IEEETrans. 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. 2003.