A reversible image transformation frame work for data hiding in an encrypted image

Md. Baig Mohammad[1], M.Ravindra Babu[2], G.Naga Sai Durga Prasad[3], P.Dilip Kumar[4]

[1]Lecturer, [2,3,4]Students
Department Electronics & Communication Engineering
Andhra Loyola Institute of Engineering and Technology, Vijayawada-8

Abstract: Securing data is one of the key areas of interest in today's world. There are many algorithms for data encryption, and data hiding such as LSB Substitution etc., which are frequently used. All the above methods suffer from disadvantages of threats by hackers. A new method which transforms automatically a given large-volume secret image into a secret-fragment-visible mosaic image of the same size has been proposed. The mosaic image, which looks similar to an arbitrarily selected target image and may be used as a camouflage of the secret image, is yielded by dividing the secret image into fragments and transforming their color characteristics to be those of the corresponding blocks of the target image. This paper focusses on near lossless recovery of secret image which is embedded in another mosaic image. The experimental results show the superior performance of the proposed method.

I. INTRODUCTION

In recent years, the topic of automatic art image creation by using computer algorithms interests many people and many methods have been proposed. The common goal of creating these image styles is to make the generated art images look like some other types of images. Mosaic image is also a type of computer art image is composed of many small identical tiles, such as squares, circles, triangles, and so on. Images may contain private or confidential information that should be protected from leakages during transmissions. There are mainly two issues associated with Information hiding viz: Distortion rate when hiding huge amounts of data and Selection of Matching images to the target image. In this connection a new idea of changing an image into a cubism-like image and hiding a secret image in the cubism image using a mapping sequence is introduced that is more secure from eavesdroppers and hackers.

Currently, images from various sources are frequently utilized and transmitted through the internet for various applications. Some of the images are online personal photograph albums, confidential enterprise archives, images from document storage systems, images from medical imaging systems, and military image databases etc., which usually contain private or confidential information. 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 random file, which cannot provide additional information before decryption and may warrant an attacker's attention during transmission due to its randomness. An alternative to avoid this problem is data hiding that hides a secret message into a cover image so that there is a least probability of guessing the existence of the secret data. Some of the existing data hiding methods are based on LSB sub situation, histogram shifting, difference expansion, prediction-error expansion, recursive histogram modification, and discrete cosine/wavelet transformations etc.,. 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. Thus, a main issue of these 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 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 lost and hence create noticeable artifacts.

A new technique for secure image transmission is proposed, which transforms a secret image into a meaningful mosaic image with the same size and appears like a preselected target image. The transformation process is controlled by a secret key, which can be used to recover the secret image nearly lossless 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 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.

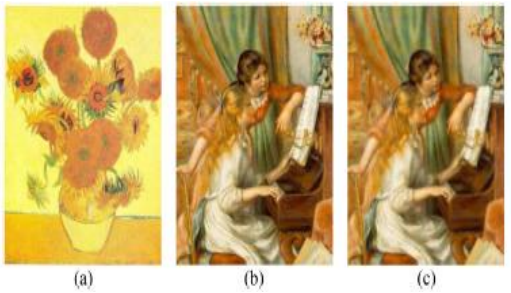


Fig1.1: Result yielded by the proposed method. (a) Secret image. (b) Target image. (c) Secret-fragment-visible mosaic image created from (a) and (b) by the proposed method.

The Fig. 1 shows a result yielded by the proposed method. 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 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. Relevant schemes are also proposed to conduct nearly lossless recovery of the original secret image from the resulting mosaic image.

II. SURVEY OF IMAGE ENCRYPTION TECHNIQUES

The information security is very important and has been used from ages. This section surveys some of the encryption techniques and highlights the advantages of proposed method. Following are some techniques discussed.

i. Steganography
ii. Water Marking Technique
iii. Visual Cryptography
iv. Encryption without sharing any keys

II. i. Steganography

The steganography word comes from the Greek word Steganos, which is used to cover or secret and a graphy, is used for writing or drawing. Therefore, steganography is, literally, covered writing. The main idea for covering the information or steganography is used for secure communication in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hidden data. During the transmission process, characteristics of these methods are to change in the structure and features so as not to be identifiable by human eye. Digital videos, images, sound files, and other files of computer that contain perceptually important information can be used as ―covers or carriers to hide secret messages. After embedding a message into the cover-image, a so-called ― stego image is obtained.

The Security, Capacity and robustness are three different aspects which is affecting steganography and its usefulness. Capacity is used to the amount of information that can be hidden in the cover medium. Security relates to an eavesdropper‘s inability to detect hidden information and robustness is the amount of modification the stego medium can withstand before an adversary can destroy the hidden information. The concept of the mosaic images in was created perfectly and it has been widely used. Four types of mosaic images namely crystallization mosaic, ancient mosaic, photo mosaic and puzzle image mosaic are proposed in. In the first two types, the source image is split into tile image and then it is reconstructed by painting the tiles and they are named as tile images. The next two types include obtaining target image and with the help of database, cover image has been obtained. They may be called as multi-picture mosaics.

II-II. WATER MARKING

Water marking is also one of the technique used to hide the digital image, Digital watermarking is a process of embedding (hiding) marks which are typically invisible and that can be extracted only by owners of the authentication. This is the technology which is used with the image that cannot be misused by any other unauthorized miss users. This technology allows anyone to do without any distortion and keeping much better quality of stegno-image, also in a secured and reliable manner guaranteeing efficient and retrievals of secret file. Digital watermarking finds wide application in security, authentication,

copyright protection and all walks of internet applications. There has been effective growth in developing techniques to discourage the unauthorized duplication of applications and data. The watermarking technique is one, which is feasible and design to protect the applications and datarelated. The term‘ cover‘ is used to describe the original message in which it will hide our secret message, data file or image file. Invisible watermarking and visible watermarking are the two important types of the above said technology. The main objective of this package is to reduce the unauthorized duplication of applications and data, provide copyright protections, security, and authentication, to all walks of internet applications.

II-iii. Water Marking

Visual Cryptography is used to hide information in images, a special encryption technique in such a way that encrypted image can be decrypted by the human eyes, if the correct key image is used. It is uses two transparent images. One image contains image contains the secret information and the other random pixels. It is not possible to get the secret information from any one of the images. Both layers and transparent images are required to get the actual information. The easiest way to implement Visual Cryptography is to print the two layers onto a transparent sheet.

II-iv Encryption without sharing any keys

Secring image for transmission without sharing his encrypted key, but it needs two transmission for a single image transmission, the image is encrypted with private key and is sent without sharing key to the receiver, after receiving the encrypted image receiver again encrypted the image by its own keys, and send it to the first sender, first sender removed the first encrypted key and again send to opponent, The opponent already had its keys then with this key the image is finally decrypted. Thus different person applying different-different techniques for securing his information.

III. THE PROPOSED METHOD

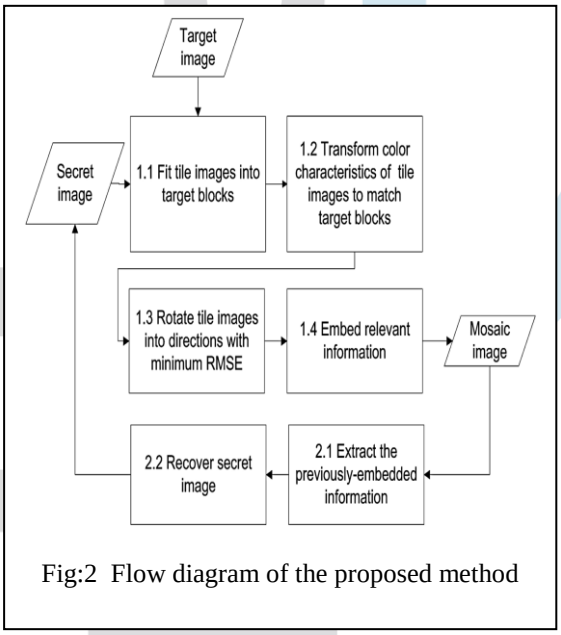


Fig:2 Flow diagram of the proposed method

The proposed method includes two main phases as shown by the flow diagram of Fig.2 : 1) mosaic image creation and 2) secret image recovery In the first phase, 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 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 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 second phase, the embedded information is extracted to recover nearly losslessly the secret image from the generated mosaic image. The phase includes two stages: 1) extracting the embedded information for secret image recovery from the mosaic image, and 2) recovering the secret image using the extracted information

The pairing of the images will be done based on the Class Index Table (CIT) here we have to find the standard deviation (SD) and mean values of the each block and based on the SD the CIT table is defined

Example:-

1 2 3	9 8 7	(1,6) (2,5) (3,4)
4 5 6	3 2 1	(4,7) (5,8) (6,9)
7 8 9	4 5 6	(7,3) (8,2) (9,1)
secret image	target image	Block paired image

Pairing table:-

secret image	1	2	3	4	5	6	7	8	9
target image	6	5	4	7	8	9	3	2	1

IV. ALGORITHM

==========

Algorithm-1 Mosaic image creation (Stage1)

==========

Input:
a secret image S, a target image T, and a secret key K.
Output:
a secret-fragment-visible mosaic image F.

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

Step 2:
Compute the means and the standard deviations of each tile image Ti and each target block Bj for the three color channels according to (1) and (2); and compute accordingly the average standard deviations for Ti and Bj , respectively, for i = 1 through n and j = 1 through n.
Step 3:
Sort the tile images in the set Stile = {T1, T2, . . . , Tn} and the target blocks in the set Starget = {B1, B2, . . . , Bn} according to the computed average standard deviation values of the blocks; map in order the blocks in the sorted Stile to those in the sorted Starget 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: T1 → Bj1 , T2 → Bj2 , . . . , Tn → Bjn .
Step 4:
Create a mosaic image F by fitting the tile images into the corresponding target blocks according to L.

==========

Algorithm-2 Mosaic image creation (Stage2)

==========

Stage 2. Performing color conversions between the tile images and the target blocks.

Step1. Create a counting table TB with 256 entries, each with an index corresponding to a residual value, and assign an initial value of zero to each entry (note that each residual value will be in the range of 0 to 255).
Step 2. For each mapping Ti →Bji in sequence L, represent the means μc and μ _ c of Ti and Bji, respectively, by eight bits; and represent the standard deviation quotient qc by seven bits,
Step 3. For each pixel pi in each tile image Ti of mosaic image F with color value ci where c = r, g, or b, transform ci into a new value c__ i by (3); 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 Ri for pixel pi by the way described in Section III(C); and increment by 1 the count in the entry in the counting table TB whose index is identical to Ri.

Stage 4. rotating the tile images.

Step 5. Compute the RMSE values of each color transformed tile image Ti in F with respect to its corresponding target block Bji after rotating Ti into each of the directions θ =0o, 90o, 180o and 270o; and rotate Ti into the optimal direction θo with the smallest RMSE value.

Stage 4. embedding the secret image recovery information.

Step 9. Construct a Huffman table HT using the content of the counting table TB to encode all the residual values computed previously.
Step 10. For each tile image Ti in mosaic image F, construct a bit stream Mi for recovering Ti in the way as described in Section III(D), including the bit-segments which encode the data items of: 1) the index of the corresponding target block Bji; 2) the optimal rotation angle θ° of Ti; 3) the means of Ti and Bji and the related standard deviation quotients of all three color channels; and 4) the bit sequence for overflows/underflows with residuals in Ti encoded by the Huffman table HT constructed in Step 9.
Step 11. Concatenate the bit streams Mi of all Ti in F in a raster-scan order to form a total bit stream Mt ; use the secret key K to encrypt Mt into another bit stream M_ t ; and embed M_ t into F by the reversible contrast mapping scheme proposed.
Step 12. Construct a bit stream I including: 1) the number of conducted iterations Ni for embedding M_ t; 2) the number of pixel pairs Npair used in the last iteration; and 3) the Huffman table HT constructed for the residuals; and embed the bit stream I into mosaic image F by the same scheme used in Step 11.

Algorithm-2 Secret image recovery
Input: a mosaic image F with n tile images {T1, T2, . . . ,Tn} and the secret key K.

Output: the secret image S.

Steps:

Stage 1. extracting the secret image recovery information.

Step 1. Extract from F the bit stream I by a reverse version of the scheme proposed and decode them to obtain the following data items: 1) the number of iterations Ni for embedding M_ t ; 2) the total number of used pixel pairs Npair in the last iteration; and 3) the Huffman table HT for encoding the values of the residuals of the overflows or underflows.
Step 2. Extract the bit stream M_ t using the values of Ni and Npair by the same scheme used in the last step.
Step 3. Decrypt the bit stream M_ t into Mt by K.

Step 4. Decompose Mt into n bit streams M1 through Mn for the n to-be-constructed tile images T1 through Tn in S, respectively.
Step 5. Decode Mi for each tile image Ti to obtain the following data items: 1) the index ji of the block Bji in F corresponding to Ti; 2) the optimal rotation angle θ° of Ti; 3) the means of Ti and Bji and the related standard deviation quotients of all color channels; and 4) the overflow/underflow residual values in Ti decoded by the Huffman table HT.

Stage 2. recovering the secret image.

Step 6. Recover one by one in a raster-scan order the tile images Ti, i = 1 through n, of the desired secret image S by the following steps: 1) rotate in the reverse direction the block indexed by ji, namely Bji, in F through the optimal angle θ° and fit the resulting block content into Ti to form an initial tile image Ti; 2) use the extracted means and related standard deviation quotients to recover the original pixel values in Ti according to (4); 3) use the extracted means, standard deviation quotients, and (5) to compute the two parameters cS and cL; 4) scan Ti to find out pixels with values 255 or 0 which indicate that overflows or underflows, respectively, have occurred there; 5) add respectively the values cS or cL 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 Ti.
Step 7. Compose all the final tile images to form the desired secret image S as output.

ADVANTAGES

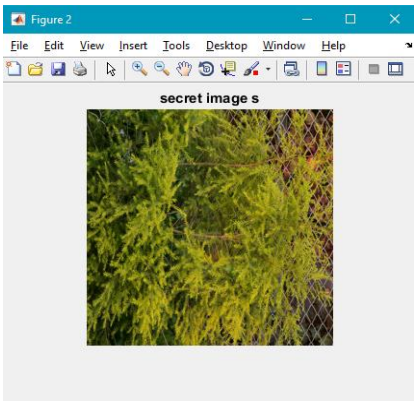
- A new secure image transmission method has been proposed, can transform a secret image into a mosaic one with the same data size for use as a camouflage of the secret image.
- In order to increase the security of the proposed method, the embedded information for later recovery is encrypted with a secret key

CONCLUSION

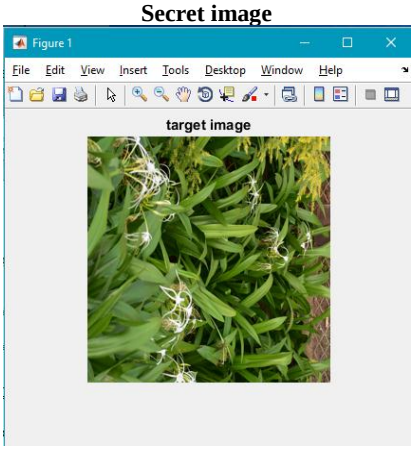
A new secure image transmission method has been proposed, which not only can create meaningful mosaic images but also can transform a secret image into a mosaic one with the same data size for use as a camouflage of the secret image. By the use of proper pixel color transformations as well as a skillful 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. Good experimental results have shown the feasibility of the proposed method. Future studies may be directed to applying the proposed method to images of color models other than the RGB.

FUTURE SCOPE

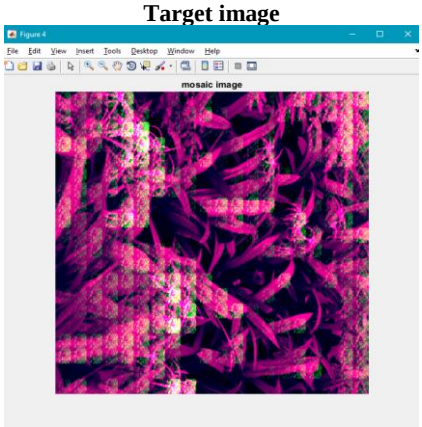
In this paper we propose a novel framework for reversible data hiding in encrypted image (RDH-EI) based on reversible image transformation (RIT). Several interesting problems can be considered in the future ,including how to improve the quality of the encrypted image and how to extend idea of RIT to audio and video.



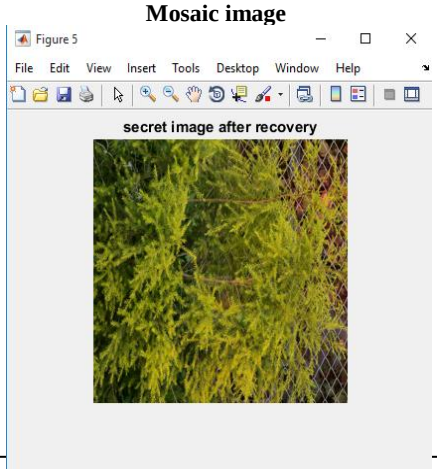
Secret image



Target image



Mosaic image



REFRENCES:

[1] J. Fridrich, “Symmetric ciphers based on two-dimensional chaotic maps,” Int. J. Bifurcat. Chaos, vol. 8, no. 6, pp. 1259–1284, 1998.
[2] G. Chen,Y. Mao, and C. K. Chui, “A symmetric image encryption scheme based on 3D chaotic cat maps,” Chaos Solit. Fract., vol. 21, no. 3, pp. 749–761, 2004.
[3] L. H. Zhang, X. F. Liao, and X. B. Wang, “An image encryption approach based on chaotic maps,” Chaos Solit. Fract., vol. 24, no. 3, pp. 759–765, 2005.
[4] H. S. Kwok and W. K. S. Tang, “A fast image encryption system based on chaotic maps with finite precision representation,” Chaos Solit. Fract., vol. 32, no. 4, pp. 1518–1529, 2007.
[5] S. Behnia, A. Akhshani, H. Mahmodi, and A. Akhavan, “A novel algorithm for image encryption based on mixture of chaotic maps,” Chaos Solit. Fract., vol. 35, no. 2, pp. 408–419, 2008.
[6] D. Xiao, X. Liao, and P. Wei, “Analysis and improvement of a chaosbased image encryption algorithm,” Chaos Solit. Fract., vol. 40, no. 5, pp. 2191–2199, 2009.
[7] V. Patidar, N. K. Pareek, G. Purohit, and K. K.Sud, “A robust and secure chaotic standard map based pseudorandom permutation substitution scheme for image encryption,” Opt. Commun., vol. 284, no. 19, pp. 4331–4339, 2011.
[8] C. K. Chan and L. M. Cheng, “Hiding data in images by simple LSB substitution,” Pattern Recognit.., vol. 37, pp. 469–474, Mar. 2004.
[9] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, “Reversible data hiding,” IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar. 2006.
[10] J. Tian, “Reversible data embedding using a difference expansion,” IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug. 2003.
[11] Y. Hu, H.-K. Lee, K. Chen, and J. Li, “Difference expansion based reversible data hiding using two embedding directions,” IEEE Trans. Multimedia, vol. 10, no. 8, pp. 1500–1512, Dec. 2008.
[12] V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y.-Q. Shi, “Reversible watermarking algorithm using sorting and prediction,” IEEE Trans. Circuits Syst. Video Technol., vol. 19, no. 7, pp. 989–999, Jul. 2009.
[13] X. Li, B. Yang, and T. Zeng, “Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection,” IEEE Trans. Image Process., vol. 20, no. 12, pp. 3524–3533, Dec. 2011.
[14] W. Zhang, X. Hu, X. Li, and N. Yu, “Recursive histogram modification: Establishing equivalency between reversible data hiding and lossless data compression,” IEEE Trans. Image Process., vol. 22, no. 7, pp. 2775–2785, Jul. 2013.[15] J. Fridrich, M.Goljan, and R. Du, “Invertible authentication,” Proc. SPIE, vol. 3971, 2001, pp. 197–208.