Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 8, August 2014, pg.613 – 621

RESEARCH ARTICLE

An Enhanced Image Steganography Technique in Art Images

Shemi P B[1], Remya Paul[2]

[1]Department of Computer Science, Viswajyothi College of Engineering and Technology Kerala, India

[2]Assistant Professor of Computer Science, Viswajyothi College of Engineering and Technology Kerala, India

Shemee.p@gmail.com

Abstract— A new method of combining art image generation and hiding a secret image into this cubism-like image to enhance the camouflage effect for various information-hiding applications is proposed. First, a new type of computer art, called line-based Cubism-like image, which keeps a characteristic of the Cubism art created by extract prominent lines and regions. Then the cubism like image is divided into target tiles and the secret is also divided into secret tiles of same size as target. A mapping sequence is created based on secret-target tile similarity and the secret image is embedded into the target using that mapping sequence. To enhance security a secret key is shared between sender and receiver. The secret key will generate a random permutation that is used to permuting the mapping sequence. That mapping information is also embedded into the Cubism Image. Finally a secret-embedded-mosaic-image is created as stego image and that is sent to the receiver. When the receiver gets the output image, using the common secret key, he retrieves the mapping sequence and using that mapping sequence he will extract the secret image from the cubism image. Data hiding with the minimal distortion is carried out skillfully during the process of recolouring the regions and embedding is based on LSB replacement. The tile similarity algorithm avoids keeping a large database of matching images.

Keywords— Cubism-like-image, tiles, secret-embedded-mosaic-image

I. INTRODUCTION

In recent years, the topic of automatic art image creation via the use of computers arouses interests of 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.

Main two Issues in Information Hiding are: 1) Distortion rate when hiding huge amount of data 2) Selection of Matching images to the target image. So 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.

In the proposed system initially the source image is converted into Cubism-like-art image by extracting prominent lines and regions. Yi-Zhe Song, Paul L. Rosin, Peter M. Hall and John Collomosse [3] proposed a method to simple shapes (e.g. circles, triangles, squares, superellipses and so on) are optimally fitted to each region within a segmented photograph. Stipple Placement using Distance in a Weighted Graph is proposed by David Mould [4] provides extra emphasis to image features, especially edges.

Regarding lossless data hiding, several techniques have been proposed. Xiaomei Quan and Hongbin Zhang proposed "Lossless Data Hiding Scheme Based On Lsb Matching [4] deals data hiding based on bit change. A lossless data hiding method based on histogram shifting and encryption is proposed by Nutan Palshikar and Prof. Sanjay Jadhav, and C. Liu in Lossless Data Hiding using Histogram Modification and Hash Encryption Scheme [5] .

A novel scheme for separable reversible data hiding in encrypted images developed by Nutan Palshikar, Prof. Sanjay Jadhav in Separable Reversible Data Hiding in Encrypted Image [6]. A new secure image transmission technique which automatically transforms a given large-volume secret image into a so-called secret-fragment-visible mosaic image of the same size [7]. A pioneering work done by Wei-Jen Wang, Cheng-Ta Huang, and Shiuh-Jeng Wang, proposed a state-of-the-art review and comparison of the different existing data-hiding methods for VQ-based images in "VQ Applications in Steganographic Data Hiding Upon Multimedia Images"[7] and _Real-Time Audio Watermarking Based on Characteristics of PCM in Digital Instrument [8] is a work done by Kotaro Yamamoto and Munetoshi Iwakiri. A lot of research carried out in data hiding inside compressed video in "Data Hiding in Motion Vectors of Compressed Video Based on Their Associated Prediction Error" [9] and "Robust Video Data Hiding Using Forbidden Zone Data Hiding and Selective Embedding [10].

II. MODULE DESCRIPTION

There are two major stages in the proposed Image Stegnographic Technique

- Sender Side
- Receiver Side

At sender side a new type of computer art, called line-based Cubism-like image, which keeps a characteristic of the Cubism art created by extract prominent lines and regions. Then the cubism like image is divided into target tiles and the secret is also divided into secret tiles of same size as target. A mapping sequence is created based on secret-target tile similarity and the secret image is embedded into the target using that mapping sequence. To enhance security a secret key is shared between sender and receiver. The secret key will generate a random permutation that is used to permuting the mapping sequence. That mapping information is also embedded into the Cubism Image. Finally a secret-embedded-mosaic-image is created as steno image and that is sent to the receiver.

At the receiver side when the receiver gets the output image, using the common secret key, he retrieves the mapping sequence and using that mapping sequence he will extract the secret image from the cubism image.

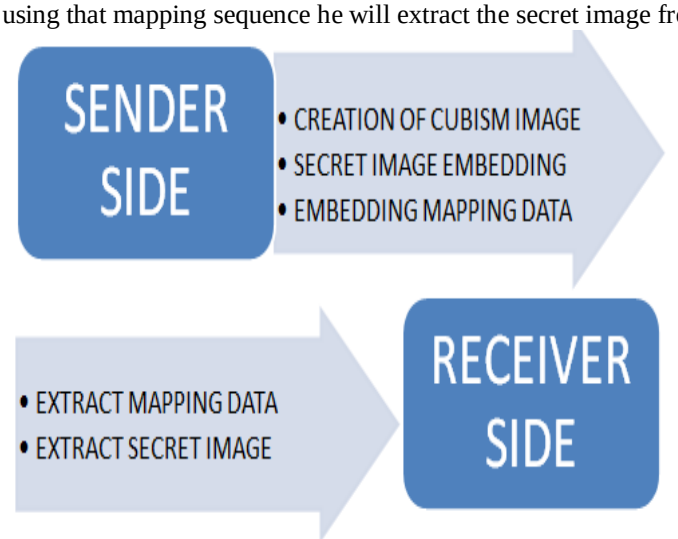

Fig 1 Main modules at sender and **receiver**

III. IMPLEMENTATION AT SENDER SIDE

The main steps at sender's side are

1. Line-based Cubism-like Image Creation
2. Creation of Target Tiles
3. Creation of Secret Tiles
4. Creation of Target-Secret Mapping Sequence
5. Hide Secret Image
6. Randomize Mapping Sequence using KBRP
7. Embedding Mapping Sequence

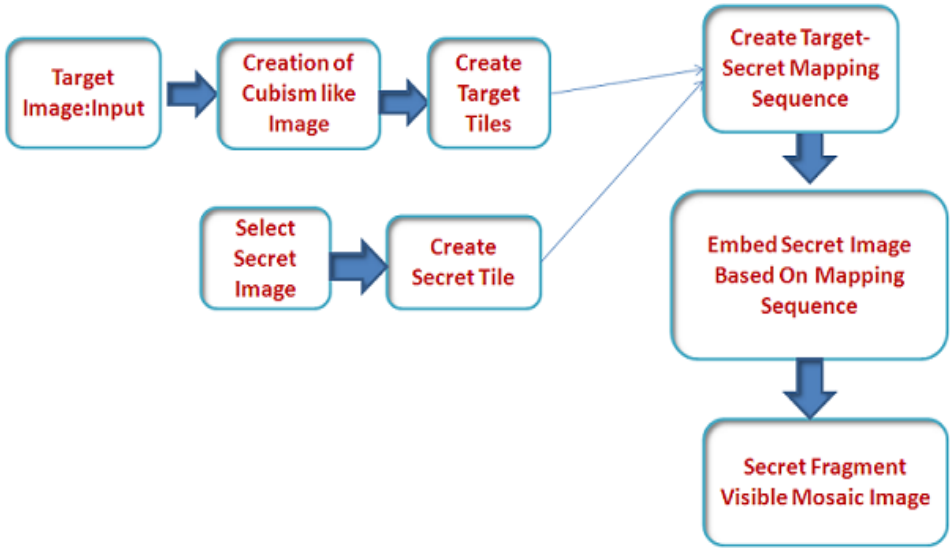

Fig 2 Sender Side Design.

1. Line-based Cubism-like Image Creation

Cubism artists transform a natural scene into geometric forms in paintings by breaking up, analyzing, and reassembling objects in the scene from multiple viewpoints. In addition, with the scene objects rearranged to intersect at random angles, each Cubism painting seems to be composed of intersecting lines and fragmented regions in an abstract style. The idea of the proposed art image creation technique is inspired by these concepts of the Cubism art.

There are two major stages in the proposed line based Cubism-like image generation process—Prominent line extraction and Region recoloring.

a. Prominent line extraction: The line segments are extracted from a given source image by edge detection and the Hough transform. Then, short line segment filtering and nearby line merging is conducted.

b. Region recoloring: The regions are created in the image by extending the line segments to the image boundary to partition the image space. Then, the regions are recolored by the average color of that region

Algorithm 1: line-based cubism-like image creation

The details of the above process are described as an algorithm in the following

Input: A source image S, and two thresholds the minimum line segment length L_{min} and the minimum line distance $D_{min.}$

Output: A line-based Cubism-like image S_C .

Stage 1 Prominent line extraction.

Step 1. (Edge detection) Apply Canny edge detection to image S, resulting in a new image S' of edge points.

Step 2. (Line segment detection)Applying the Hough transform to S' to find a list of line segments $L_1,L_2,....L_m$ sorted according to their lengths, yielding a second new image S'' of the line type.

Step 3. (Prominent line extraction) Find prominent lines in S'' by the following steps.

3.1 Select those line segments in S'' with lengths larger than threshold L_{min} and discard the others, resulting in a shorter list of line segments $L_1', L_2', ...L_m'$.

3.2 For all i=0 through n and all j=0 through n with i≠j and both L_i' and L_j' not deleted yet, compare L_i' and L_j' and and if the distance between L_i' and L_j' and is smaller than threshold , D_{min} then delete the shorter one of L_i' and L_j' .

Stage 2 Region recoloring.

Step4. (Line extension) Extend each remaining line segment in S'' to the image boundaries of S''.

Step5.(Region partitioning) Partition S'' into regions $R_1, R_2, ...R_k$ by the extended lines.

Step6. (Region recoloring) Recolor each region R_i in S'' by the following steps with i=1,2,....K.

6.1 Compute the area A_i (in unit of pixel) of R_i and the average color (C_{ir} ,C_{ig} ,C_{ib}) of all the pixels in R_i. r each pixel in R_i by (C_{ir} ,C_{ig} ,C_{ib}).

6.2 Recolor each pixel in R_i by (C_{ir}, C_{ig}, C_{ib}).

Step7. (Line recoloring) Recolor all region boundaries in S'' by the white color.

Step8. Take the final S'' as the desired line-based Cubism-like image S_C.

Fig 3 Source image and Generated Cubism-like image

2. Creation of Target Tiles

Then the cubism-like images are divided into small tiles of 5x5 or 8x8 of equal size in matrix form of an image file as shown in Fig 4. The similarity score of every tile is extracted and embedded on to the matching tile of target image space, which is a random location in the target image. This is called mosaic information hiding. Based on any random techniques shuffles the tiles again for security. Embedding the tile fitting information in to the blocks of the mosaic image is done for later recovery.

Fig 4 Creation target tiles.

3. Creation of secret tile

Arbitrarily select any secret Image and Divide the Secret image into small tiles of equal size as target image as shown in Fig 5

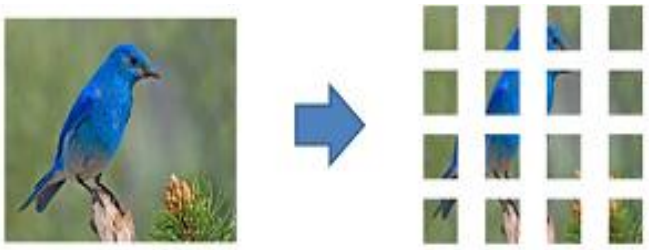

Fig 5. Creation of secret tiles.

4. Create Target-Secret Mapping Sequence

Find the target tile that most similar to the secret tile, the Similarity algorithm uses fitness function to place the tile in the matching place. Then Create Mapping Sequence, this mapping sequence is created at the sender side.

Algorithm 2 :Create Target-Secret Mapping Sequence

Input: TargetTiles T_t,Secret Tiles S_t .

Output: Mapping Sequence Map .

Stage 1 Calculate Similarity Score

For each Secret Tile S_t

Call Fitness Algorithm

Returns T_t and Similarity Score

Stage 2 Store Mapping Sequence

Map(1)=S_t

Map(2)=T_t

Map(3)=Similarity Score

Algorithm 3: Fitness

Step 1: Assign Min=Infinity

Step 2: For each Target Tile Tt

2.1 If it is not assigned to any SecretTile St

Compute Hsv Plane of Tt and St as Hsv1 and Hsv2

Take the difference of Hsv1 and Hsv2 as DiffH

If DiffH less than Min

Min=DiffH

Map=Tt

Similarity score=DiffH

Step 3: Returns Tt and Similarity Score

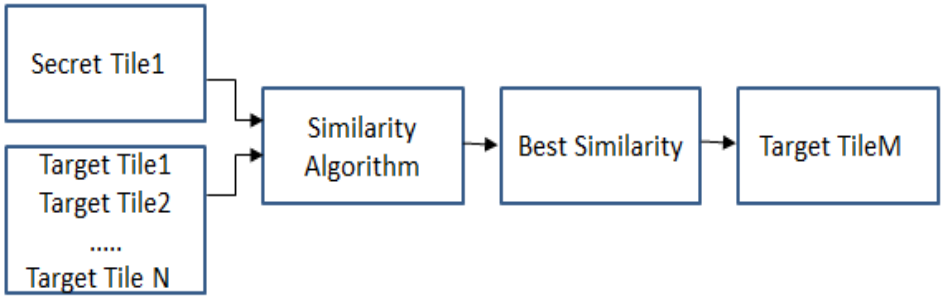

Fig 6. Creation of mapping sequence

5. Hide Secret Image

Find the target tile that most similar to the secret tile, the Similarity algorithm uses fitness function to place the tile in the matching place. Then Create Mapping Sequence, this mapping sequence is created at the sender side

6. Randomize Mapping Data using KBRP

The Mapping data is randomized using KBRP algorithm. The Key Based Random Permutation (KBRP) introduces a method for generating a particular permutation P of a given size N out of N! Permutations from a given key. This method computes a unique permutation for a specific size since it takes the same key; therefore, the same permutation can be computed each time the same key and size are applied. The name of random permutation comes from the fact that the probability of getting this permutation is 1 out of N! possible permutations. Besides that, the permutation cannot be completely on a given key and size.

The process involves three consecutive steps:

1. init()
2. eliminate()
3. fill()

1. init()

In this step initialize array of size n with elements from the given key, by taking the ASCII code of each element in the key and storing them in the array consecutively. To complete all elements of the array, add elements to the array by adding two consecutive values of the array until all the elements of the array are set to values. Finally, all values are set to the range 1 to N by applying the mode operation.

2. eliminate()

Get rid of repeated values by replacing them with value of zero and keep only one value out of these repeated values.

3.fill()

Replace all zero values with nonzero values in the range 1 to N which are not exist in the array. The resulted array now represents the permutation.

7. Embedding Mapping Data

The Mapping data is also hide in the source image using LSB replacement algorithm. LSB hiding is one of the simplest hiding methods that embeds one bit in the least significant position of each pixel. If the bit to be hidden is 1 then the LSB of the pixel is set to 1. If the bit to be hidden is 0 then the LSB bit is changed to 0. Here each bit is hidden in randomly positioned pixels determined by the random numbers generated in the previous step. Here hiding is performed on the red component of the encrypted image. With this step the encryption process is completed. Finally a Secret-embedded-Mosaic Image is produced which Contains image as well as Mapping Data. This image is the send to the receiver side

IV. IMPLEMENTATION AT RECEIVER SIDE

1. Extract Mapping Data

At the receiver side mapping data is extracted using reverse of LSB replacement algorithm. Embedding is defined as the mapping secret message to pixel's steganography is the most classic steganographic techniques, which embeds secret messages in a subset of the LSB plane of the image. A large number of popular steganographic tools, such as S-Tools 4, Steganos and StegoDos, are based on LSB replacement in the spatial domain.

LSB steganography can be described as follows: if the LSB of the pixel value I(i, j) is equal to the message bit m to be embedded, I(i, j) remain unchanged; if not, set the LSB of I (i,j) to m. The message embedding procedure can be described using an Equation as follows;

$$ls(i,j) = \begin{cases} I(i,j) - 1 & LSB(I(i,j) = 1 \quad and\ m = 0 \\ I(i,j) & LSB(i,j) = m \\ I(i,j) + 1 & LSB\big(I(i,j)\big) = 0 \quad and \quad m = 1 \end{cases}$$

2. Extract Secret Image

Then using the Mapping data the secret Image is extracted.

Fig 7 Extracted secret image.

V. EXPERIMENTAL RESULTS

Results with various inputs are checked. The experimental results obtained indicate that the degrees of information hiding are higher when using smaller tiles, and the different sizes of tile images are selected for verification. Simulation is done in MATLAB. Different inputs are given. Created mosaic image is based on a mapping sequence by LSB replacement algorithm. On the recovery of the secret image, provided the same sequence and key elsewhere the noise image will results.

The peak signal to noise ratio (PSNR) and the RMSE values of the mosaic image is checked and it is above 30 and the secret image is similar to the extracted secret image and the human visual system is difficult to differentiate it. Thus providing the higher degree of information hiding and it should be visually please. Hence it is suitable for covert communication. So it proposed method is a lossless secret image hiding method. Comparison with the previous method proposed by Lai and Tsai [8] indicates that the proposed method have smaller RMSE values with respect to the target images, indicates that they are more similar to the target images. And noted that, the proposed method allows users to select their favourite images for uses as target images. This

provides great edibility in practical applications without the need to maintain a target image database which usually is very large.

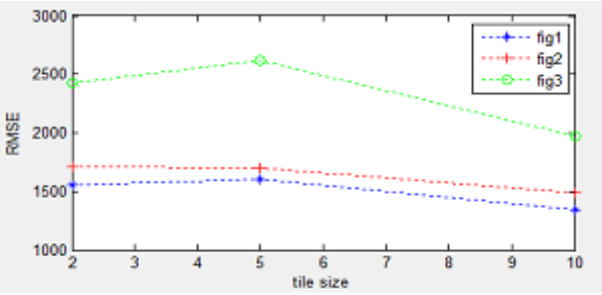

Fig .8. Plots of different tile image sizes (2x2; 5x5and10x10) with input secret images, RMSE values of created mosaic images with respect to target images.

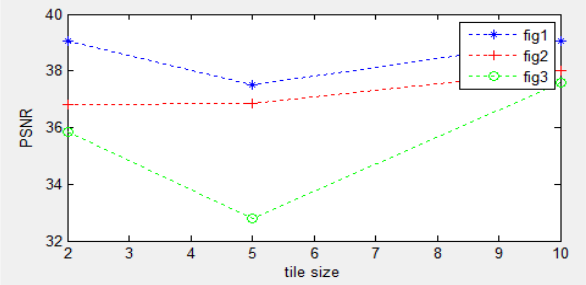

Fig9. Plots of different tile image sizes (2x2; 5x5and10x10) with input secret images, PSNR values of recovered secret images with respect to original ones.

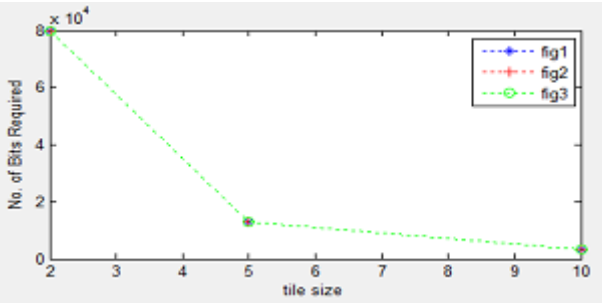

Fig10. Plots of different tile image sizes (2x2; 5x5and10x10) with input secret images, Numbers of required bits embedded for recovering secret images.

VI. CONCLUSIONS

In this paper, a new method of combining art image generation and data hiding is proposed. At first, a new type of computer art, called line-based Cubism-like image, created by prominent line extraction and region recolouring. Then, by utilizing the characteristics of the Cubism-like image creation process, a data hiding technique has been proposed. The cubism image and secret image is divided into different tiles of equal size and then create target-secret mapping sequence based on the similarity score of them. This mapping sequence is used to embed secret image into cubism image and that mapping information also embed into the target image using LSB replacement algorithm. Finally get the Secret-Embedded-Visible-Mosaic image that is sent to the receiver. At the receiver side the common secret key is used to extract mapping sequence and the secret image is extracted using this extracted mapping sequence.

Data hiding for art images is important because it can protect data and communication against malicious attacks, such as information stealing and copyright piracy. Security is enhanced by using KBRP algorithms and secret key. The proposed method proven to have minimum distortion using Tile Similarity algorithm in the case of huge amount of data.

REFERENCES

[1] Shan-Chun Liu and Wen-Hsiang Tsai,*"Line-Based Cubism-Like ImageA New Type of Art Image and its Application to Lossless Data Hiding "* in IEEE Trans On Information Forensics And Security ,Vol. 7, No. 5, OCTOBER 2012

[2] Yi-Zhe Song, Paul L. Rosin, Peter M. Hall and John Collomosse,"*Arty Shapes"* , in Computational Aesthetics in Graphics, Visualization, and Imaging.

[3] David Mould, *"Stipple Placement using Distance in a Weighted Graph", in Computational Aesthetics in Graphics"*, Visualization, and Imaging , 2008.

[4] Xiaomei Quan and Hongbin Zhang, "Lossless *Data Hiding Scheme Based On LSB Matching"*, in ISBN 978-0-9891305-0-9,2013.

[5] Nutan Palshikar, Prof. Sanjay Jadhav, *"Lossless Data Hiding using Histogram Modification and Hash Encryption Scheme ",* in International Journal of Emerging Technology and Advanced Engineering,January 2014

[6] Xinpeng Zhang, *"Separable Reversible Data Hiding in Encrypted Image"*, in in Proc. IEEE Trans. on Information Forensics and security,Vol. 7, No. 2, APRIL 2012.

[7] Ya-Lin Lee and Wen-Hsiang Tsai, *"A new secure image transmission technique via secret- fragment-visible mosaic images by Nearly-reversible Color Tranformations,"* in IEEE Trans. 2013.

[8] Wei-Jen Wang, Cheng-Ta Huang, and Shiuh-Jeng Wang *,"VQ Applications in Steganographic Data Hiding Upon Multimedia Images"* IEEE Systems Journal, Vol. 5, No. 4, December 2011.

[9] Kotaro Yamamoto , *"Real-Time Audio Watermarking Based on Characteristics of PCM in Digital Instrument,"* in Journal of Information Hiding and Multimedia Signal Processing ,2010

[10] Hussein A. Aly *, "Data Hiding in Motion Vectors of Compressed Video Based on Their Associated Prediction Error*," IEEE Trans On Information Forensics And Security, Vol. 6, No. 1, March 2011.

[11] Ersin Esen and A. Aydin Alatan ,*"Robust Video Data Hiding Using Forbidden Zone Data Hiding and Selective Embedding ,"* in Trans On Circuits And Systems For Video Technology, Vol. 21, No. 8, August 2011

[12] Zahra Toony and Mansour Jamzad ,"*A Novel Image Hiding Scheme Using Content Aware Seam Carving Method"* in International Conference on Availability, Reliability and Securityy, 2010

[13] V.Rajkumar *," Modifier Digital Image Steganography Using Discrete Wavelet Transform ,"* in Trans On Circuits And Systems For Video Technology,Volume 1, Issue 1, March 2013

Nilanjan Dey, Anamitra Bardhan Roy and Sayantan Dey *,"A Novel Approach of Color Image Hiding using RGB Color planes and DWT ,"* in International Journal of Computer Applications (0975 – 8887), Volume 36– No.5, December 2011

