Volume No:3, Issue No:2 (July-2017)
ISSN No : 2454-423X (Online)

International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Privacy Preserving of Image and Data Transmission using Hybrid Encryption and Image Mosaic Technique

Killi Satish Kumar
Final M.Tech Student,
Dept of CSE,
Sarada Institute of Science, Technology and Management (SISTAM),
Srikakulam, Andhra Pradesh.

Chintada Sunil Kumar
Assistant Professor,
Dept of CSE,
Sarada Institute of Science, Technology and Management (SISTAM),
Srikakulam, Andhra Pradesh.

Abstract:

Mosaic king is one of the techniques of Image processing which is useful for tiling digital images which generally is blending together of several arbitrarily shaped images to form one large radio-metrically balanced image with boundaries between the original images are not visional. Before transferring image we can perform the color damage of image and take that image performing mosaic operation. In this paper we are extend the concept of data also should be send through mosaic images. In this paper we are implementing mainly five concepts are key generation, data encryption and decryption, data hiding, image color damage and correction, image mosaic process. Before transferring image we can generate key and using that we can encrypt transferred data. After completion of encryption process take that data and put into image using least significant bit technique. Take the data hide image and apply pixel xor with key technique for reducing image color. After completion of image color reducing process and perform the mosaic process for tiling digital image number of shapes. Take those shaped image and send to respect receiver, the receiver will perform the reverse process it will get the original data and image without loss of color. By implementing those techniques we can improve the efficiency in image transferring process and also provide more security in data.

Keywords:

Image Mosaic, Privacy, key generation, shared key, hybrid encryption and decryption, pixels.

I. Introduction :

Image Mosaicing technology is becoming more and more popular in the fields of image processing, computer graphics, computer vision and multimedia. It is widely used in daily life by stitching pictures into panoramas or a large picture which can display the whole scenes vividly. For example, it can be used in virtual travel on the internet, building virtual environments in games and processing personal pictures. In Image Mosaicing is firstly divided into (usually equal sized) rectangular sections, each of which is replaced with another photograph that matches the target photo. When viewed at low magnifications, the individual pixels appear as the primary image, while close examination reveals that the image is in fact made up of many hundreds or thousands of smaller images. In image mosaic king two input images are taken and these images are fused to form a single large image. This merged single image is the output mosaiced image.

The first step in Image Mosaicing is feature extraction. In feature extraction, features are detected in both input images. Image registration refers to the geometric alignment of a set of images. The different sets of data may consist of two or more digital images taken of a single scene from different sensors at different time or from different viewpoints. In image registration the geometric correspondence between the images is established so that they may be transformed, compared and analysed in a common reference frame. This is of practical importance in many fields, including remote sensing, computer vision, medical imaging. Registration methods can be loosely divided into the following classes: algorithms that use image pixel values directly, e.g., correlation methods algorithms that use the frequency domain, e.g., Fast Fourier transform based (FFT-based) methods algorithms that use low level features such as edges and corners, e.g., Feature based methods and algorithms that use high-level features such as identified parts of image objects, relations between image features, for e.g., Graph-theoretic methods.

The next step, following registration, is image warping which includes correcting distorted images and it can also be used for creative purposes. The images are placed appropriately on the bigger canvas using registration transformations to get the output mosaicked image. The quality of the mosaicked image and the time efficiency of the algorithm used are given most importance in image mosaicking. Before performing image mosaic we can stored data into image. The storing data into image the sender will perform encryption of data using genetic operation. By performing encryption process the sender will convert data into unknown format. After converting data the sender will stored data into image using least significant bit technique. In this paper we are using another concept for generation of shared key by using Diffe hellmankey exchange protocol. Using that key the sender will encrypt the transferring message using encryption process using hybrid encryption algorithm.

After encryption the sender will put data into image and perform mosaic of image using region based technique. The sender will send those parts to specified receiver and the receiver will perform the reverse process. By performing reverse of process we can get original data and original image.

II. RELATED WORK:

A large number of different approaches to image mosaicing have been proposed. For a good survey, see [15]. The methods can be roughly divided into two classes: direct methods such as [14, 11, 8] and feature-based methods such as [2, 5, 1, 10]. Both of these have their pros and cons. Mosaic images can be classified into four types, crystallization mosaic, ancient mosaic, photo mosaic, and puzzle image mosaic. The first two types of mosaics decompose a source image into tiles (with different color, size and rotation), reconstructing the image by properly painting the tiles. So they can be grouped together under the denomination of tile mosaics The last two kinds are obtained by fitting images from a database to cover an assigned source image. Hence they may be grouped together under the denomination of multi-picture mosaics. This taxonomy should not be intended as a rigid one. Many mosaic techniques may fit in more than a single class and it is likely that other new types of mosaics will appear in the future. Automatic mosaic construction has been applied in many fields such as photogrammetry, computer vision, image processing and computer graphics. Building a mosaic image from a sequence of partial views is a powerful means of obtaining a broader view of a scene than from a single view and has been used in a large range of applications The most traditional application is the construction of large aerial and satellite photographs from collection of images. In the aspect of medical imaging, the large panoramic images can help doctors to conduct comprehensive and visual observation on the focus and the surrounding parts. An application in which mosaics are specifically useful is in the diagnosis and treatment of retinal diseases.

Mosaicing is also applied for document image analysis when it is not possible to capture a large document at a reasonable resolution in a single exposure. Another application area is panoramic image mosaics from sequences of images. Here a review on the research works in the field of document image mosaic and retina image mosaic are discussed. The main challenges in image mosaicing are correcting geometric deformations using image data and/or camera models, image registration using image data and/or camera models and eliminating seams from image mosaics. In the digital realm, mosaics are illustrations composed by a collection of small images called ’tiles’. The tiles tessellate a source image with the purpose of reproducing the original visual information rendered into a new mosaic-like style. Computer generated Mosaic image creation is a new research area in recent years. Various mosaics can be created for an image depending on the choice of the tile dataset and the imposed constraints for positioning, deformations, etc. Mosaic images are images made by cementing together small colored tiles. Likely, they are the most ancient examples of discrete primitive based images. A picture (usually a photograph) is divided into (usually equal sized) small sections and each of which is replaced with another photograph that matches the target photo or reconstruct the image by properly painting the tiles.

III. PROPOSED SYSTEM:

Image mosaic is generally enhancing the granular information in images for viewers and offering improved input for different automated image processing techniques. The primary aim of segmenting an image is to enhance quality and suitability for presenting the image for a specific given task in front of an observer. Mosaic is a process partitioning of color or grey scale image into various set of segments. The major benefit of image mosaic is to provide a convenient way of image representation and analysis. In this process, whole image is distributed and categorized in to different group of image sectors. These sectors consist of similar image level on a pixel basis. Thus, displaying same level pixels prominent and making the image outlines brighter which can be used for further analysis. Application of image mosaic is vast and could be used in many fields. Before performing the mosaic technique the sender and receiver will choose shared key for data encryption, decryption process. After completion of cryptography technique we are take the send image and put cipher format data into image. Take the data hide image and perform the color correction process on the data hide image. By applying color correction process we are loss the color of data hide image. After completion of this process we are apply the mosaic technique on the color loosed image. Take those color loose image segmentation and send that parts to respect user. The receiver will get those parts and apply reverse process it will get original data and image. The implementation process those concepts are as follows.

Diffe Hellman Key Exchange Protocol:

In this module the sender and receiver will generate same shred key for encryption and decryption of transferring message. The generation of shared key is as follows.

1. The sender and receiver will agree to use modulus P and base G.

2. The sender will choose private key a and calculate public key by using following formula.

Public key= G^a mod P

3. After generating public the sender will send that public key to receiver.

4. The receiver will retrieve public key and choose private key.

5. Using that private the receiver will generate public by using same formula and send that public to sender.

6. The sender will retrieve receiver public key and generate shared key by using following formula.

Shared key= receiver public^{a} mod P

7. The receiver also generate shared key by using following formula.

Shared key= sender publickey^{a} mod P

After generating shared key those keys are same for both users. By using that shared key the sender will encrypt transferring message. By performing the data encryption and decryption process we are using hybrid encryption and decryption algorithm. The implementation procedure of hybrid encryption and decryption algorithm is as follows.

Hybrid Data Encryption Process:

In this module the sender will enter transferred message and encrypt that data by using the following process.

1. The sender will retrieve shared key and message as input of the algorithm.

2. Retrieve each character from the message and perform the xor operation with key until the length of message is completed.

3. Choose two large prime numbers P and Q and random number A, B and G, R.

4. Set A and B for Diffie Hellman key generation

5. R and G are automatic generated constants.

6. Calculate N= P * Q.

7. Find Phi (N) = (P-1)*(Q-1)

8. Choose integer E, which can satisfy GCD [E, Φ (N)] =1. Φ (N. Where 1<E< Φ (N)

9. Calculate D, where E*D = 1 mod Φ (N).

10. Now calculate following as public number

Calculate X= G^A mod R, Y= G^B mod R

11. Secret key K1 = Y^A mod R,

K2 = X^B mod R.

12. Encrypt message C1= (M ^ E) mod N.

13. X-OR between C1 and key K1,

S= C1$\oplus$ K1

After completion of encryption process take the cipher format data and convert into binary format. Take that binary format data and hide data into transferred message. The data hiding into image can be done by using random pixel pair matching technique. The implementation procedure of random pixel pair matching is as follows.

Random Pixel Pair Matching Algorithm:

The Random pixel pair matching technique uses pixel pair (x,y) as the coordinate, and searches a coordinate (x′,y′) within a predefined neighbourhood set Φ(x,y) such that f(x′,y′) = sB , where f is the extraction function and sB is the message digit in a B-ary notational system to be concealed. Data embedding is done by replacing (x,y) with (x′,y′). Suppose a digit sB is to be concealed. Data embedding is done by replacing (x,y) with (x′,y′). Suppose a digit sB is to be concealed. The range of sB is between 0 and B-1, and a coordinate (x′, y′) ϵ Φ(x,y) has to be found such that f(x′,y′) = sB. Therefore, the range of f(x, y) must be integers between 0 and B-1, and each integer must occur at least once. In addition, to reduce the distortion, the number of coordinates in should be as small as possible. The method also satisfies the following three requirements:

1) There are exactly B coordinates in Φ(x, y).

2) The values of extraction function in these coordinates are mutually exclusive.

3) The design of Φ(x, y) and f(x,y) is capable of embedding digits in any notational system so that the best can be selected to achieve lower embedding distortion.

The definitions of Φ(x, y) and f(x, y) significantly affect the stego image quality. The designs of Φ(x, y) and f(x, y) have to fulfil the requirements: all values of f(x, y) in Φ(x, y) have to be mutually exclusive and the summation of the squared distances between all coordinates in Φ (x, y) and f(x, y) has to be the smallest. This is because, during embedding, (x, y) is replaced by one of the coordinates in Φ(x, y). Suppose there are B coordinates in Φ(x, y), i.e., digits in a B-ary notational system are to be concealed, and the probability of replacing (x,y) by one of the coordinates in Φ(x,y) is equivalent. Data is embedded by using PPM based on this f(x, y) and Φ(x, y). The extraction function f(x, y) is described as follows:

$$F(x, y) = (x + cB * y) \bmod B \quad (2)$$

The base B which is followed in implementing the APPM method is 16 and the cB value used is 6. Thus we have the neighbourhood set defined by Φ16(x,y).

Embedding Procedure:

Suppose the cover image is of size M × M, S is the message bits to be concealed and the size of S is |S|. First we calculate the minimum B such that all the message bits can be embedded. Message digits are sequentially concealed into pairs of pixels. The detailed procedure is listed as follows.

Input: Cover image I of size M × M, secret bit stream S, and key K.

Output: Stego image I′, cB , ΦB(x,y) and Kr .

1. Find the minimum B satisfying ⌊M ×M/2⌋ ≥ |SB|, and convert S into a list of digits with B -ary notational system SB.

2. The value of cB and ΦB(x, y) are computed.

3. In the region defined by ΦB (0, 0), record the coordinate (xi′, yi′) such that f(xi′,yi′) = i , 0 ≤ i ≤ B - 1 .

4. Construct a nonrepeating random embedding sequence Q using a key Kr .
5. To embed a message digit sB, two pixels (x, y) in the cover image are selected according to the embedding sequence, and calculate the modulus distance between sB and f(x, y), then replace (x, y) with (x + xd, y + yd).

6. Repeat Step 5 until all the message digits are embedded.

After completion of data embedding process take the data hide image and perform the color loss and correction technique for reduce image color. The implementation procedure of color loss and correction technique is as follows.

Color Loss and Correction technique:

In this module the sender will take the data hide image and apply color loss and correction technique. Following are the implementing procedure of color loss and correction technique.

1. Take the data hide image, shared key and second level key as input of the technique.

2. Take the data hide image and read pixels from the first row the image.

3. Read the second row pixel and xor with first row pixel, then the xor result pixel will be stored into another array in the matrix format.

4. The xor process repeat until the total number of rows is completed in the data hide image.

5. After completion of xor process take the each pixel value and xor with shared key until the total number of pixels are completed.

Take those xor pixels value and generate image color loss image. After completion of this process we can perform the image mosaic technique on color loss image.

Edge Based Image Mosaic Technique:

In this module the sender will segment data hide image into number of parts by using region based image mosaic technique. In this technique we are segment image using region based. In this paper we are taking some amount of pixel will be consider in a region and split that region into one segment. After that take another part from previous region of some pixel values and next region of original image. Likewise we can segment image into specified parts and those segment will be send to receiver. The receiver will receive parts from the sender and generate single image by applying reverse of process of region based image mosaic technique. The completion of generating data hide image the receiver will again apply the color loss and correction reverse process it will get plain format data hide image. Take that data hide image and convert into binary format. After converting image into binary format the receiver will get all binary formatted cipher data by using extraction process of random pixel pair matching algorithm.

Extraction Procedure:

To extract the embedded message digits, pixel pairs are scanned in the same order as in the embedding procedure. The embedded message digits are the values of extraction function of the scanned pixel pairs. Input: Stego image I′, cB , ΦB(x,y) and Kr .. Output: Secret bit stream S.

1. Construct the embedding sequence Q using the key Kr.

2. Select two pixels (x′, y′) according to the embedding sequence Q.

3. Calculate f (x′, y′), the result is the embedded digit.

4. Repeat Steps 2 and 3 until all the message digits are extracted.

5. Finally, the message bits S can be obtained by converting the extracted message digits into a binary.

After getting all binary format cipher data and perform the decryption process it will get original plain format. The decryption process is as follows.

1. Read the eight bit from the binary cipher format and convert into decimal format. This process will repeat until the length of message is completed.

2. Take those decimal values and second level key, perform the decryption process of hybrid encryption and decryption algorithm.

3. The receiver will xor the s with second level key (K2) by using following formula.

$$C1= S \oplus K2.$$

4. Decrypt the C1 with public key with modulo of n.

$$M= (C1\text{^} D) \bmod N.$$

By performing the decryption process it will get original plain format and covert binary format image should be generated into original format. By implementing those techniques we can improve the efficiency of network and also provide more security of transferred data and image.

IV. CONCLUSIONS:

In this paper we are implementing novel color loss and correction technique in a image mosaic application. Before performing image mosaic technique we can hide data into image and that data hide image we are apply the color loss and correction technique. In this paper we are performing key generation process for encryption and decryption data. Another concept is hide data into image using random pixel pair matching algorithm. By using this technique we can hide data into image and take that data hide image apply the color loss and correction technique. Using color loss and correction take we can reduce color of data hide image and apply image mosaic technique in that image. By implementing image mosaic technique we using edge based image mosaic process. After completion of mosaic process we can get number of parts image with contain the color loss format. Those color loss partition will be send the respect receiver and receiver will take those partition. By apply reverse of process all above technique the receiver will get original plain format data and image. By implementing those concepts we can improve the network efficiency and also provide more security of transferred image and data.

REFERENCES:

B. Zitova and J. Flusser. Image registration methods: a survey. Image and Vision Computing, (21):977–1000, 2003

R. Szeliski. Image mosaicing for tele-reality applications. In Proceedings of the Second IEEE Workshop on Applications of Computer Vision, pages 44–53, Sarasota, FL USA, 1994.

J. A. Robinson. A simplex-based projective transform estimator. In International Conference on Visual Information Engineering, pages 290–293, 2003.

M. Irani, P. Anandan, and S. Hsu. Mosaic based representations of video sequences and their applications. In 5th International Conference on Computer Vision, pages 605–611, Cambridge, MA, 1995.

D. Capel and A. Zisserman. Automated mosaicing with super-resolution zoom. In IEEE Computer Society Conference on Computer Vision and Pattern Recognition, pages 885–891, Santa Barbara, CA USA, 1998.

A. Fusiello, M. Aprile, R. Marzotto, and V. Murino. Mosaic of a video shot with multiple moving objects. In International Conference on Image Processing, volume 2, pages 307–310, 2003.

M. Brown and D. Lowe. Recognising panoramas. In Ninth IEEE International Conference on Computer Vision, volume 2, pages 1218–1225, 2003.

R. Marzotto, A. Fusiello, and V. Murino. High resolution video mosaicing with global alignment. In IEEE Computer Society Conference on Computer Vision and Pattern Recognition, volume 1, pages 692–698, 2004

A. Abadpour and S. Kasaei, “A fast and efficient fuzzy color transfer method,” in Proc. 4th IEEE Int. Symp. Signal Process. Inf. Technol., Dec. 2004, pp. 491–494.

V. Lempitsky and D. Ivanov, “Seamless mosaicing of image-based texture maps,” in Proc. IEEE Conf. Comput. Vis. Pattern Recognit., Jun. 2007, pp. 1–6. (2002) The IEEE website.

E. Reinhard, M. Ashikhmin, B. Gooch, and P. Shirley, “Color transfer between images,” IEEE Comput. Graph. Appl., vol. 21, no. 5, pp. 34–41,Oct.

BIOGRAPHIES:

Killi Satish Kumar is student in M.tech (CSE) in Sarada Institute of Science Technology and Management, Srikakulam. He has received his B.tech

(IT) from Sri Sivani College of Engineering, Chilakapalem, Srikakulam. His interesting areas are data mining, network security and cloud computing

Chintada Sunil Kumar working as a Asst Professor of CSE in Sarada Institute of Science, Technology and Management (SISTAM), Srikakulam, Andhra Pradesh. He received his M.Tech (CSE) from Jntuk, Kakinada. Andhra Pradesh. His interest research areas are Database management systems, Computer Architecture, Image Processing, Computer Networks, and Distributed Systems. He published 4 international journals and he was attended number of conferences and workshops.