ISSN: 2278 – 7798
International Journal of Science, Engineering and Technology Research (IJSETR)
Volume 5, Issue 5, May 2016

A Secure image Transmission Using Mosaic Image creation in videos

Susan Mathew and Deepthy Mathew

***Abstract*— By using mosaic image creation method, a secure image transmission technique through video is introduced. The frames of the video include the created mosaic image and that mosaic image looks identical to target image. The mosaic image is created by dividing the secret image into small parts and converting their color characteristics with respect to the blocks of the target image and it can be used as cover for the secret image. By the proper application of this method the secret image can be easily recovered without any loss. Using lossless data hiding scheme, a key is embedded into the created mosaic image and the information needed to recovering the secret image is also embedded in the video.**

***Index Terms*— Color transformation, Data hiding, Image encryption, Mosaic image, Secure image transmission, Video technology.**

I. INTRODUCTION

Secure image transmission have an important role in our day today life. For various applications images are transmitted through internet. These images contain confidential as well as personal data, so they should be protected from leakages and attacks during transmissions. Various techniques are already used for secure image transmission such as data hiding and image encryption. In image encryption technique unauthorized user is not able to decrypt the image, so this will increase the image security. High redundancy and spatial correlation of an image is used in image encryption technique. Image is encrypted based on Shannon's confusion and diffusion properties [1]–[5] .Without the correct key it will act like a noisy image and only with correct key the secret image can be recovered. Due to this property before decryption the encrypted image is a meaningless image and due to its randomness nature an attacker's attention will easily affect. Another most commonly used method is data hiding, in which the secret image is hide inside a cover image.

Manuscript received May, 2016.

***Susan Mathew**, PG student, Electronics And Communication Department, College of Engineering, Kidangoor, Kottayam, Kerala, India, Phone/ Mobile No; 8129042408*

***Deepthy Mathew,** Assistant Professor, Electronics And Communication Department, College of Engineering, Kidangoor, Kottayam, Kerala, India, Phone/ Mobile No; 9447220498*

There are different types of data hiding method such as LSB substitution [6], histogram shifting etc. The main issue in data hiding method is that it is very difficult to embedding a large amount of data into a single image. And image should in highly compressed form for hiding a secret image into a cover image of same size. But for many applications such as medical images, military images, legal documents etc the compression technique is not a practical solution. Here a new technique is introduced in which an image is hiding inside a video and transmitted. This is done by converting the secret image to a meaningful mosaic image. The mosaic image looks very similar to the frames of the target video .The usage of key will improve security.

II. PREVIOUS WORK

Different methods are using for secure image transmission such as image encryption, watermarking, data hiding, steganography etc. These methods have advantages as well as disadvantages based on the concern of security issues, capacity issues, robustness issues etc. For improving security a new method is introduced, by using mosaic image creation method. Two images using for this method are secret image and target image. The secret image is first divide into rectangular blocks called tiles and fit them into similar blocks in target image. Based on some color similarity criteria the tiles of secret image is fit into the blocks in target image and that results the formation of mosaic image. The illustration for this method is shown below. Fig 1 represents the secret image; Fig 2 represents the target image in which the secret image is hiding and Fig 3 represents the mosaic image, which looks very similar to the target image. The color characteristics of each tile of secret image and target blocks should be same, for that some color transformation methods are used [9].

III. PROPOSED WORK

The technique used here for secure transmission is done by using mosaic image creation method. There are already several works done for secure image transmission such as data hiding method, watermarking method [7-8], encryption method etc. Some capacity, security, and robustness problems occurred for these types of transmission method. Nowadays security is one of the main problems when image is transmitted through internet. By mosaic image creation

Fig 1.Secret Image

Fig 2.Target Image

Fig 3. Mosaic Image

method the security will increase and the image can be recovered without any loss. Here proposing a new method for secure transmission of image through video. The secret image is first divide into rectangular blocks called tiles and fit them into similar blocks in target image in which these target image are the frames of the video called target video. Based on some color similarity criteria the tiles of secret image is fit into the blocks in target image. Fig 4 represents block diagram for this method. In the image encryption method without the correct key it will act as a meaningless image but in mosaic image creation method meaningful image is created. And in data hiding method highly compressed techniques should be used when the size of the secret image and target image is same, whereas this method is new in such a way that no compressing methods are using.

IV. ALGORITHM

The proposed work consists of two modules

- Mosaic image creation
- Secret image recovery

A. Algorithm 1: Mosaic image creation

Secret image is denoted by A, Target video is denoted by B, key is denoted by k and mosaic video is created by M.

- The tile images are fitting into target blocks:

Step 1: Split the target video into frames. If the size of A and B are different, then change its size to become same. Then divide the secret image into n tiles {T1, T2... Tn} and the target image into n blocks {B1, B2, ..., Bn} with each Ti and Bi with same size NT.

Step2: According to (1) and (2) compute the mean and the standard deviations of each tile image and each target block for the three color channels .

$$\mu c = 1/n \sum_{i=1}^{n} ci \, , \; \mu c' = 1/n \sum_{i=1}^{n} ci' \qquad (1)$$

$$\sigma c = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(ci - \mu c)^2} \, ,$$

$$\sigma c' = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(ci' - \mu c')^2} \qquad (2)$$

Step 3: Sort the tile images Stile = {T1, T2, ...,Tn} and the target blocks A target = {B1, B2, ..., Bn}, According to the standard deviation value and according to the calculated average standard deviation value, Map the blocks in the sorted Stile to those into the sorted A target.

Step 4: By placing the tile images into the respective target blocks , create a mosaic image M

- Conducting color conversions between each tiles in the secret image and each blocks in the target image:

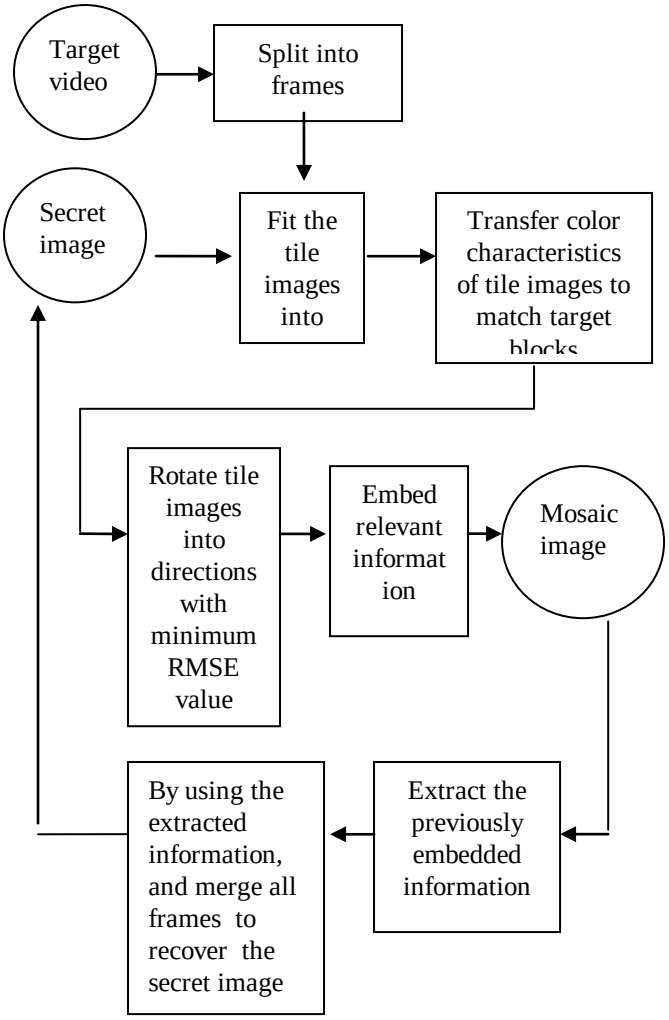

Fig 4. Block diagram

Step 5: Counting table (TB) with 256 entries is created, the index value is related to the residual value.

Step 6: By using the equation (3) transform each pixel value of mosaic image to a new color value ci ; if ci is greater than 255 or if it is smaller than 0, then change ci to be 255 or 0, respectively.

$$ci'' = qc(ci - \mu c) + \mu c' \quad (3)$$

- According to RMSE rotate the title images:

Step 7: Compute the RMSE value of the new color value pixels. Rotate the each pixels into different directions and in which direction the pixels values got minimum RMSE value, maintain that optimal direction.

- The secret image recovery information is embedding:

Step 8: To encode all the residual values calculated previously, obtain a Huffman table HT using the content of the counting table TB

Step 9: Construct a bit stream Mi for recovering Ti, For each tile image Ti in mosaic image M.

Step 10: To form a total bit stream Mt, Combine the bit streams Mi of all Ti in a raster-scan order. Use the secret key K to encrypt Mt into another bit Stream Mt'.

B. Algorithm 2: Secret image recovery

Secret image is denoted by A, Target video is denoted by B, key is denoted by k and mosaic video is created by M.

- Obtain the secret video recovery information:

Step 1: Reversing the last step in the above algorithm, obtain the bit stream Mt.

Step 2: By using K, Decrypt the bit stream Mt' into Mt

Step 3: Decompose Mt into n bit streams M1 through Mn and Decode M for each tile image.

- Recovering the secret image:

Step 4: To fit the block into T , Rotate each tile in the reverse direction.

Step 5: To recover the original pixel values, obtain the means and related standard deviation quotients.

Step 6: Scan each pixel values to find out which pixels have values 255 or 0 , and then take these values as the final pixel values. Formulate all the final tile images and Merge all the frames to form the secret image.

V. CONCLUSION

A secure image transmission technique through video is introduced, by using mosaic image creation method. Without any need of database Target image can be selected and by the proper usage of pixel color transformations visible mosaic image is created without any loss. Future studies may be one for applying the proposed method for transmission of secure video through videos.

ACKNOWLEDGMENT

Authors are grateful to the TEQIP, College of Engineering Kidangoor for the financial support to complete this paper work.

REFERENCES

.

[1] 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.
[2] 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.
[3] 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.
[4] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *Int. J. Bifurcat. Chaos*, vol. 8, no. 6, pp. 1259–1284, 1998.
[5] 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.
[6] C. K. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution," *Pattern Recognit.*., vol. 37, pp. 469–474, Mar. 2004.
[7] 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.
[8] W.-H. Lin, S.-J. Horng, T.-W. Kao, P. Fan, C.-L. Lee, and Y. Pan,"An efficient watermarking method based on significant difference of wavelet coefficient quantization," *IEEE Trans. Multimedia*, vol. 10, no. 5, pp. 746–757, Aug. 2008. 469–474, Mar. 2004
[9] E. Reinhard, M. Ashikhmin, B. Gooch, and P. Shirley, "Color transfer between images," *IEEE Comput. Graph. Appl.*, vol. 21, no. 5, pp. 34–41,Sep.–Oct. 2001.
[10] *Related images of the experiments* [Online].Available:http://people.cs.nctu.edu.tw/ yllee/yllee & whtsai sfv.html.

First Author

Ms. Susan Mathew received her BTech Degree in Electronics and Communications engineering From CUSAT, Kerala, India in 2013. She is currently pursuing her MTech Degree in Wireless Technology from college of engineering kidangoor, kottayam Kerala, India. Her areas of interest include image processing.