Image Encryption and Decryption based on Mosaic Image Creation in YUV Color Space and Reversible Color Transformations

Gita Kumari[1], Shilpi Sharma[2]

[1]*PG Scholar,* [2]*Professor, Dept. of ECE*

Bhopal Institute of Technology, Bhopal, India

Abstract - Image encryption is being possible through different techniques for various confidential applications. A novel image encryption and decryption technique is proposed in which mosaic image is created to hide the secret image and serves as enhanced method of secure image transmission. The mosaic image, which looks identical to the cover image and used as concealment of the secret image, is obtained by segmenting the secret image into fragments and their color characteristics are transformed to that of cover image blocks. The proposed method is implemented in YUV color space in addition with RGB color space, using techniques of reversible color transformations. The recovery of secret image based on the information embedded into created mosaic image using data hiding scheme. Security is increased by this novel method for image transmission.

Keywords- Mosaic image, image encryption, color transformation, YUV.

INTRODUCTION

With the advancement of computer technology and internet, images are extensively used to transmit information. The practice of images in various applications includes multimedia systems, medical imaging, telemedicine, medical systems, confidential military archives, enterprises and storage systems. While transmitting images through internet where hacking of confidential data may take place security is the major issue. Transfer of images from one place to another may contaminate the image information, so new methodology is derived to eliminate noise and to recover the secret image nearly losslessly.

Through use different techniques secure image transmission is gaining extensive popularity. Image encryption and data hiding are different earlier methods that were adopted for purpose of secure image transmission. In technique of encryption, natural properties of an image is used, thereby we get an encrypted image that is on the basis of Shannon's confusion and diffusion properties [1]. Without knowledge of encryption key, the secured image could not be obtained. As the encrypted image is worthless one, it does not provide additional information before the operation of decryption. But this could cause the attention of attackers during transmission operation.

Yet another method in the field of transmission involves the hiding of data that is it hides secret message into a cover image and hence the existence of secret image is really hidden. So that no one can realize the existence of the secrete data. Different techniques are used in existing data hiding methods, like Histogram shifting [2], LSB Substitution [3], discrete cosine or discrete wavelet transformations [4] etc. High compression is looked-for in case of secret image when, one wants to hide a secret image into a cover image with the same size. However for many applications, such as transmitting medical pictures, legal documents, and military images and so on that contains confidential information, in such cases data compression operations results in a loss of important information [5].

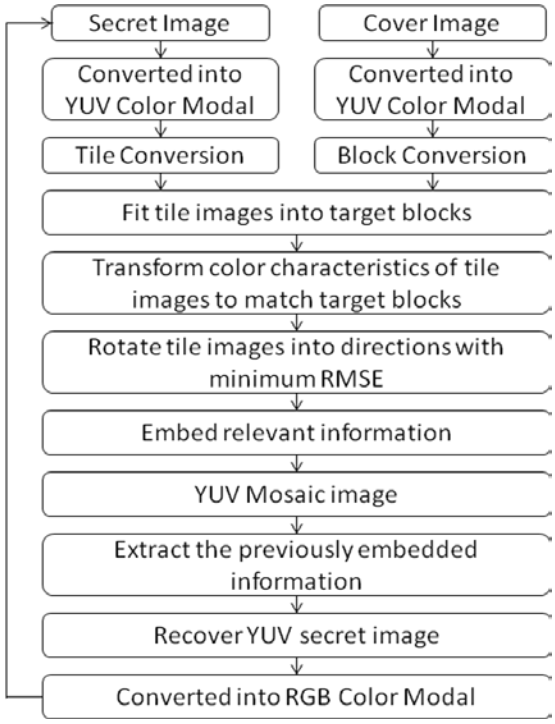
A novel technique for secure image transmission is proposed in this paper, that transforms a secret image into a meaningful mosaic image in YUV color model with the same size and the mosaic image looks like a selected cover image. The proposed method is inspired by technique proposed by Lai and Tsai [6], and Ya-Lin Lee and Tsai [7], in which a new type of computer fine 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 cover image preselected from a database.

The proposed technique takes RGB images as input and converts them into YUV color model, on which the whole operation is performed. The secret image, which is to be transmitted to the receiver, and cover images are segmented into tiles and blocks respectively of same size. The secret tiles are fitted into cover blocks and color transformations are applied on tile images such that they look similar to the cover blocks. At receiver from color transformed YUV mosaic image, YUV secret image is retrieved which in turn converted into RGB color modal.

I. SYSTEM MODEL

The proposed technique involves two phases which includes 1) Generation of mosaic image and 2) Retrieval of secret image. The flow diagram of two phases is shown in

the Fig. 1. In the first phase, a mosaic image is obtained, which comprises of the fragments of an input secret image with color corrections according to a similarity criterion based on color variations



A. Mosaic image generation: The first phase incorporates six stages: 1) Transforming secret and cover images into YUV color model [8], 2) Fragmentation of secret and cover images into tiles and blocks respectively, 3) fitting the tile images of the secret image into the target blocks of a preselected target image, 4) changing the color characteristic of every tile image in the secret image to turn that of the corresponding target block in the target image [9], 5) pivoting every tile image into a direction with the minimum RMSE value with respect to its corresponding target block, and 6) implanting required information into the created mosaic image for future recuperation of the secret image.

B. Retrieval of secret image: In the second phase, the implanted information is extracted to recuperate the secret image nearly losslessly from the generated mosaic image. The phase incorporates three stages: 1) extracting the implanted information from the mosaic image for recovery of the secret image, 2) recuperating the YUV secret image using the extracted information and, 3) transforming YUV secret image into RGB image [8].

II. PREVIOUS WORK

Y. Hu, et al, proposed a "Difference expansion based reversible data hiding using two embedding directions" [10], current difference expansion embedding technique performs only one layer embedding in a difference image because of that there will be degradation in the image. So in this paper a new difference expansion embedding algorithm which is based on Harr wavelet transform is used, which make use of two embedding directions horizontal as well as vertical difference image for data hiding which refines the algorithm and makes it flexible to different types of images.

V. Sachnev, et al, proposed "Reversible watermarking algorithm using sorting and prediction" [11], this algorithm uses a prediction errors to embed data into an image. A sorting technique is used to record the prediction errors based on magnitudes of its local inconsistency This algorithm allows us to embed more data into the image with less distortion by using a reduced size location map.

X. Li, B. Yang, et al, proposed an "Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection" [12], Prediction-error expansion is one of the important technique of reversible watermarking which can embed a large payload into digital image with less distortion. Pixel selection allows us to select pixels of smooth area for data embedding by decreasing maximum modification to pixel values. As a result, when compared with conventional prediction-error expansion we obtain more sharply distributed prediction-error histogram and a better visual quality of watermarked image.

S. Lee, et al, proposed "Reversible image watermarking based on integer -to-integer wavelet transform" [4], this technique divides an input image into non-overlapping blocks and embeds a watermark into the high frequency wavelet co-efficient to avoid both overflow and underflow in the spatial domain. The payload to be embedded includes not only message but also side information used to reconstruct the exact original image. The experimental results show that the proposed scheme achieves a higher embedding capacity when compared to the existing reversible watermarking schemes.

W. H. Lin, et al, proposed an "Efficient watermarking method based on significant difference of wavelet coefficient quantization" [13], this paper proposes a blind watermarking algorithm based on the significant difference of wavelet coefficient quantization for copyright protection. Every 7 non-overlap wavelet coefficient of the target image are grouped into a block. The largest 2 coefficient in a block are called significant coefficient and their difference is called significant difference. The local maximum wavelet coefficient is quantized in a block by comparing the significant difference value in a block with the average significant difference value in blocks. The maximum wavelet coefficient are so quantized that their significant difference between watermark bit 0 and 1 occupies large energy difference which can be used for watermark extraction.

The experimental results show that the proposed method is more effective than JPEG compression, low-pass filtering and Gaussian noise.

C. K. Chan and L. M. Cheng, proposed a "Hiding data in images by simple LSB substitution" [14], it is a method of hiding the secret message into a cover image so that unauthorized observer will not realize the existence of hidden message. In this paper, 8-bit grayscale images are selected as cover media and are called cover images. LSB is one of the common data hiding technique, which replaces the LSB's of the cover image with the message bits. Experimental results show that with low extra computation complexity we can get the enhanced image quality.

I. J. Lai and Tsai, proposed a "Secret-fragment-visible mosaic image-A new computer art and its application to information hiding" [6], in this paper a new type of computer art image called secret-fragment-visible mosaic image is proposed which is created automatically by arranging small fragments of a given image in a mosaic form, and then embedding given secret image in the resulting mosaic image. This type of information hiding is useful for covert communication and secure keeping of secret images.

Ya-Lin Lee and Wen-Hsiang Tsai, proposed "A New Secure Image Transmission Technique via Secret-Fragment-Visible Mosaic Images by Nearly Reversible Color Transformations" [7], in this paper mosaic image is created to hide the secret image and the size of cover image is same as secret image.

III. PROPOSED METHODOLOGY

In this section author need to mention his simulation/experimental research model with neat block diagrams and flow charts.

IV. SIMULATION/EXPERIMENTAL RESULTS

Images are selected arbitrarily as secret and target images and mapping is done after the division of images into blocks, then mosaic of images is done by transformation, Rotation and Residual value handling process after that embedding and Secret Image Recovery process is being done.

Table 1: Comparison of RMSE and PSNR Value for Different Color Modal

Metric	RGB	YUV
RMSE	25.51	11.25
PSNR	26.2487	5.20

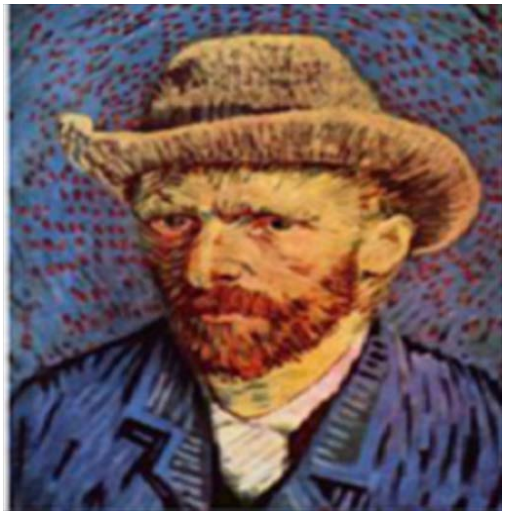


Figure 1: Cover Image – RGB

Figure 2 : Secret Image - RGB

Figure 3: Cover Image – YUV

Figure 4: Secret Image - YUV

Figure 5: Mosaic Image - YUV

Figure 6: Retrieved Secret Image – YUV

Figure 6: Retrieved Secret Image - RGB

V. CONCLUSION

The proposed technique is a novel approach of secure image transmission for creation of mosaic image in a meaningful manner and the confidential information can be transmitted in a secure way. The proper usage of pixel based color transformations provides mosaic image which is alike to the selected cover image without the need of cover image data base. Time utilization and enhanced output is being obtained with this new technique But PSNR ratio of secret image is decreasing in use of YUV color space. Therefore some image enhancement techniques are required at the receiver end. Use of YUV space should be Subjected to further research.

VI. FUTURE SCOPES

The proposed technique is a novel approach of secure image transmission for creation of mosaic image in a meaningful manner and the confidential information can be transmitted in a secure way. The proper usage of pixel based color transformations provides mosaic image which is alike to the selected cover image without the need of cover image data base. Time utilization and enhanced output is being obtained with this new technique But PSNR ratio of secret image is decreasing in use of YUV color space. Therefore some image enhancement techniques are required at the receiver end. Use of YUV space should be Subjected to further research.

REFERENCES

[1] Ya-Lin Lee and Wen-Hsiang Tsai, “A New Secure Image Transmission Technique via Secret-Fragment-Visible Mosaic Images by Nearly Reversible Color Transformations” IEEE Trans. on circuits and systems for video technology, vol. 24, no. 4, April 2014.

[2] 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.

[3] J. Lai and W. H. Tsai, “Secret-fragment-visible mosaic image—A new computer art and its application to information hiding,” IEEE Trans. Inf. Forens. Secur., vol. 6, no. 3, pp. 936–945, Sep. 2011.

[4] 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.

[5] 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.

[6] Y. Hu, H.-K. Lee, K. Chen, and J. Li, “Difference expansion basedreversible data hiding using two embedding directions,” IEEE Trans.Multimedia, vol. 10, no. 8, pp. 1500–1512, Dec. 2008.

[7] 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.

[8] S. Lee, C. D. Yoo, and T. Kalker, “Reversible image watermarking based on integer-to-integer wavelet transform,” IEEE Trans. Inf. Forens. Secur., vol. 2, no. 3, pp. 321–330, Sep. 2007.

[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] C. K. Chan and L. M. Cheng, “Hiding data in images by simple LSB substitution,” Pattern Recognit.., vol. 37, pp. 469–474, Mar. 2004.

[11] Che-Yen Wen and Chun-Ming Chou, "Color Image Models and its Applications to Document Examination", Forensic Science Journal, Jan. 03,2004.

[12] E. Reinhard, M. Ashikhmm, B. Gooch and P. Shirley, “Color transform between images”, IEEE Comput. Graph. Appl., Vol. 21, no. 5,pp. 34-41, Sep-Oct. 2001.

[13] W. B. Pennebaker and J. L. Mitchell, JPEG: Still Image Data Compression Standard. New York, NY, USA: Van Nostrand Reinhold, 1993, pp. 34–38.