Volume 6, Issue 2, February 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Increasing the Security Level of Mosaic Image for Secure Transmission: A Review

Prachi D. Meshram*, Ranjana Shende
Computer Science & Engineering, RTMNU, Nagpur,
Maharashtra, India

Abstract— ***A secure image transmission technique is proposed, which transforms automatically a given large volume secret image into a secret-fragment-visible mosaic image having same size. The mosaic image which looks similar to selected target image and it can be used as a camouflage of the secret image. Only mosaic image creation may risk to security threats. To overcome this problem encryption is performed on that image. Instead of directly sending the image from source to destination encryption is performed on that image. So that this method will provide more security by performing encryption on mosaic image.***

Index Terms- Mosaic Image, Encryption, Security

I. INTRODUCTION

Now a day's images from various sources are frequently utilized and transmitted through the internet for various applications, such as online document storage systems, personal photograph albums, confidential enterprise archives, military image databases and medical imaging systems. These images usually contain private or confidential information so that they should be safe from leakages during transmissions [2]. Recently, many methods have been proposed for securing image transmission, for which there are two common approaches, image encryption and data hiding. An encrypted image is a meaningless file and has no use until it is decrypted and due to its randomness, it may also arouse an attacker's attention during transmission [1]. To overcome this problem, we have an alternative known as, data hiding that hides a secret message into a cover image. A main issue of hiding data in images is the difficulty to embed a large amount of message data into a single image [4]. Specifically, if one wants to hide a secret image into a cover image with the same size, then this secret image must be highly compressed in advance. But, for many applications such as keeping or transmitting military images, medical pictures, legal documents, etc., that are valuable with no allowance of serious distortion, such data compression operations are not useful for us [2]. A new secure image transmission technique is proposed, where the secret image is converted into a mosaic image which is meaningful and of the same size as of secret image and looks like a previously selected target image with the contrast difference [3]. Only mosaic image creation may risk to security threats. Suppose any attacker performs zoom operation on mosaic image, he/she can easily get that the image is mosaic image. To overcome this problem encryption is performed on that image. Instead of directly sending the image from source to destination encryption is performed on that image. So that, this method will provide more security by performing encryption on mosaic image.

II. RELATED WORK

Now a day's security is a big issue. In the previous research they used the different techniques to create Mosaic Image. But, only mosaic image creation may risk to security threats. To overcome this problem encryption is performed on that Mosaic image. Instead of directly sending the image from source to destination encryption is performed on that image. So that this method will provide more security by performing encryption on mosaic image.

III. PROPOSED RESEARCH

In this paper, A secure image transmission technique is proposed. Fig. shows a result yielded by the secure image transmission technique. Specifically, after a target image is selected arbitrarily, given secret image is first divided into tiles, tiles means nothing but rectangular blocks, then these tiles are fit into similar blocks in the target image, called as target blocks, Next, the mosaic image will created. To improve the security level of secret image, encryption is performed on that mosaic image. After receiving this secret image to destination, decryption is performed on secret image and then secret image is retrieved.

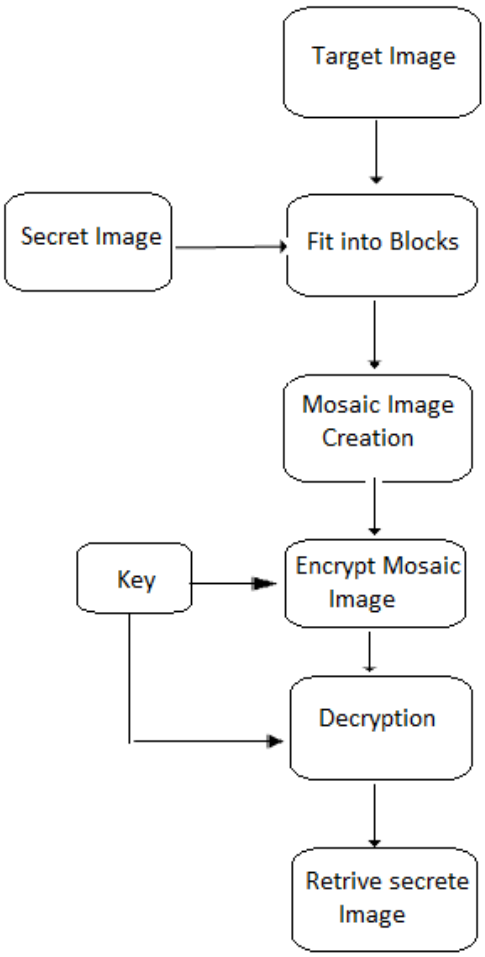

Fig. Flowchart

IV. EXPECTED OUTCOME

Proposed technique will produce noiseless decrypted secret image from target image.

V. CONCLUSION

The proposed method mainly used for secure image transmission which not only can create mosaic image but also can transform a secrete image into a meaningful mosaic one having same data size for use as a camouflage of the secrete image and after that this method can perform the encryption on that mosaic image to increase the security. If we could properly decrypt it and retrieve the original one from mosaic then it would better approach than the previous one.

ACKNOWLEDGMENT

I thank to Ms. Ranjana Shende for her valuable guidance and also thank to IEEExplore.org for references. .

REFERENCES

[1] Jaya. S,Varalatchoumy. M, Meghali. C,jitendra. k,Nagesh.H," A secure mosaic image transmission by reversible integer color transformation technique", Proceedings of 13th IRF International Conference, Bengaluru, India, 24th May 2015.

[2] 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 transactions on circuits and systems for video technology, vol. 24, no. 4, april 2014.

[3] Wei-Jen Yang, Kuo-Liang Chung, Le-Chung Lin and Chien-Hsiung Lin," Universal Reversible Data Hiding for Arbitrary RGB-CFA Captured Images", 2013 IEEE, Department of Computer Science and Information Engineering National Taiwan University of Science and Technology.

[4] I-Jen Lai and Wen-Hsiang Tsai," Secret-Fragment-Visible Mosaic Image–A New Computer Art and Its Application to Information Hiding", IEEE transactions on information forensics and security, vol. 6, no. 3, september 2011.

[5] 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.

[6] 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.

[7] 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.

[8] Linhua Zhang, Xiaofeng Liao and Xuebing Wang," An image encryption approach based on chaotic maps", Accepted 14 September 2004, Chongqing University, China College of Science, Chongqing University, Chongqing 400044, China.

[9] Chi Kwong Chan and L.M. Cheng," Hiding data in images by simple LSB substitution", Received 17 May 2002; received in revised form 11 July 2003; accepted 11 August 2003

[10] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," Int. J. Bifurcat. Chaos, vol. 8, no. 6, pp. 1259–1284, 1998.

