International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 1, Issue 2, pp 23-26, November-2017

A Grayscale Based Block Scrambling Image Encryption to Enhance the Security of Encryption Then Compression for Jpeg Images

Yeramala Kalavathi

Assistant Professor, Department of Electronics and Communication Engineering, Malla Reddy College of Engineering for Women, Hyderabad -500100, Telangana, India

***Abstract* - A grayscale based block scrambling image encryption scheme is presented to enhance the security of Encryption then Compression systems, which are used to securely transmit images through an un trusted social channel provider. This scheme is implemented by using the small sized blocks and a large number of blocks than the previously used encryption scheme. Due to the use of less color information (I.e. we use the grayscale images) the encryption can be done securely. The original image has three color channels (RGB) which decreases the security against various attacks, such as jigsaw puzzle solver and brute force attacks. This scheme allows the use of color sub sampling, which can improve the compression performance, although the encrypted images have no color information. In these schemes we upload the encrypted images and then download from Social networking sites, and the results after that is effective for Encryption then- Compression systems, while maintaining a high compression performance using advance compression algorithm.**

Keywords: image encryption, jigsaw puzzle, EtC system, JPEG, Grayscale based.

I. INTRODUCTION

Encryption then Compression systems with JPEG compression has been proposed to be applied to Social Network Sites and Cloud Photo Storage Services. The robustness because of the system cannot be provided by the color based image encryption scheme against color sub sampling used for JPEG compression because the encrypted image is fully colored image. To solve these issue this system is proposed. In this system the gray scale based images encryption has been proposed to encrypt a full color image as a gray scale based image. The effect of color sub sampling can be avoid by using gray scale based image encryption system, The color sub- sampling operation is not considered in gray scale- based image encryption system because it is generated from RGB components. In the color based image encryption the compression performance is decrease strongly due to the presence of colors. According to, the gray scale based image encryption generated from YCbCr components and the quantization table for gray scale based images has been proposed to provide the better compression performance. However, the color sub sampling operation has not been considered. In this system we discuss the color sub sampling operation for gray scale based image encryption. Instead of generating the gray scale based image from RGB components, a full color image in RGB color space is firstly transformed to YCbCr color space. Hence, color sub- sampling operation can be performed to generate gray scale based images. The enhancements of compression performance and robustness against color sub sampling are evaluated in terms of Rate-Distortion (RD) curves.

II. LITERATURE SURVEY

Warit Sirichotedumrong , Tatsuya Chuman , Shoko Imaizumi and Hitoshi Kiya. Description: The rapid growth of the Internet and multimedia systems causes the increment of using images and video especially in Social Networking Service (SNS). To securely transmit images through an untrusted channel provider such as SNS, encryption has to be performed. There are many encryption schemes which have been studied for securing an im age . The most secure option is to fully encrypt the whole image using the famous crypto systems, such as RSA and AES. However, security is not the only requirement that crypto systems should satisfy. Low processing cost and the format compliance have to be considered for using in many applications. A lot of perceptual encryption schemes have been proposed to satisfy the requirements by trading-off the security of encryption schemes. This paper focuses on encrypting images before compression process which is called Encryption-then-Compression (ETC) systems. For transmitting the encrypted images over the internet via many platforms, the format of encrypted image has to be compatible with the international image compression standards. The previously proposed ETC This work was partially supported by Grant-in-Aid for Scientific Re search(B), No.17H03267, from the Japan Society for the Promotion Science. Systems are not compatible with

ISSN (online): 2581-3048
Volume 1, Issue 2, pp 23-26, November-2017

with the international standards. Consequently, the encryption schemes for ETC systems with format compliance to international standards have been proposed. Furthermore, the security of conventional ETC systems against jigsaw puzzle and brute force attacks have been discussed and evaluated. Considering the applicability of ETC systems to SNS, it has been confirmed that the conventional ETC is applicable to SNS. However, color components of images with the conventional scheme can be affected by JPEG compression. Due to the limitation, the color image must be split into 16 × 16- blocks. Because of such a situation, this paper proposes a new encryption scheme to improve format compliance, robustness against SNS recompression, and the security against several attacks. The contributions of this work are: • We propose a new block scrambling encryption scheme for ETC systems which enhances the security by dividing the image into smaller block size, having a large number of blocks, and containing less color in formation.

Kalyani G. Nimbokar , Milind V.Sarode, Mangesh M.Ghonge, Firstly we conduct the Image encryption and then conducted prior to image compression. In this system how to design a pair of image encryption and compression algorithms such that compressing encrypted images can still be efficiently performed. This paper introduced a highly efficient image encryption then compression (ETC) system which gives a best output in the form of encrypted image. This image encryption scheme operated in the prediction error domain which is able to provide a reasonably high level of security from different attacks. More notably, the proposed compression approach applied to encrypted images is only slightly worse, unencrypted images as inputs. In contrast, most of the existing ETC solutions induce significant penalty on the compression efficiency

Warit Sirichotedumrong, Tatsuya Chuman and Hitoshi Kiya, Multimedia systems and the Internet have been rapidly growth. A lot of studies on secure, efficient and flexible communications have been reported. For securing multimedia data, full encryption with provable security (like RSA, AES, etc) is the most secure options. However, many multimedia applications have been seeking a trade-off in security to enable other requirements, e.g., low processing demands, retaining bit stream compliance, and signal processing in the encrypted domain. To satisfy those requirements, a lot perceptual image encryption schemes has been proposed. In order to apply the image encryption to Social Network Services (SNS) or Cloud Photo Storage Services (CPS), encryption schemes have to be compatible to international compression standards, such as JPEG, and also be available to be recompressed by the providers because almost SNS and CPS providers manipulate every uploaded image. Although, most studies on EtC systems utilize a proprietary compression scheme which is incompatible with international standards. Image encryption for EtC systems have been proposed to provide the compatibility with international compression standards and availability of recompression. According to the grayscale-based image encryption, which is the extension of conventional EtC systems has been proposed to enhance the robustness against several attacks such as jigsaw puzzle and brute- force attacks and also avoid the effect of color sub sampling carried out by SNS and CPS providers. The grayscale-based image encryption firstly generates the grayscale-based image from a full-color image, then the grayscale-based image is encrypted.

III. RELATED WORK

A. Block Scrambling Based Image Encryption:

A block scrambling based image encryption scheme was proposed for ETC systems in which a user wants to securely transmit image through different layers via a Social Networking Service (SNS) provider which is visible at end of the process, The user does not provide any secret key K to the SNS provider, The privacy of image may be shared is under control of the user even when the SNS provider also recompresses the image . Therefore, the user can sure about the privacy by him/her. No we compare the ETC system with CTE systems, In these the user has to disclose the unencrypted images to recompress them. In the system , an image having pixel size X × Y is firstly divided into non overlapped blocks with Bx × By; then four block scrambling based processing steps are applied to the divided image. The steps required for performing the image encryption to generate an encrypted image is as follows.

Step 1: Divide image having pixel size X × Y into blocks, each with Bx ×By pixels and permute randomly. The divided blocks using a random integer generated by a secret key K1, where K1 is commonly used secret key for all color components.

Step 2: Rotate and invert randomly each block by using a random integer generated by a key K2, where K2 is commonly used secret key for all color components as well. Step 3: Apply negative positive transformation to each block by using a random binary integer generated by a key K3, where K3 is commonly used secret key for all color components.

B. Jigsaw Puzzle Solver Attack:

ISSN (online): 2581-3048
Volume 1, Issue 2, pp 23-26, November-2017

To assemble encrypted images including inverted, negative positive transformed and color component shuffled blocks extended jigsaw puzzle solvers for block scrambling based image encryption have been proposed. It has been shown that assembling jigsaw puzzles becomes difficult when the encrypted images are satisfied with under three conditions

(a) Number of blocks is large.

(b) Block size is small.

(c) Encrypted images include JPEG distortion

The block size defines the difficulty of assembling encrypted images . In addition, the most conventional jigsaw puzzle solvers also utilize color information to assemble puzzles. Thus, reducing the number of color channels in each pixel makes assembling encrypted images much more difficult. The block scrambling scheme has a higher security level than that of the conventional ETC scheme, because novel scheme provides a large number of blocks and the small block size. Other attacking strategies like known plain text attack (KPA) and chosen - plain text attack (CPA) should be considered for the security purpose. The block scrambling based image encryption becomes robust against KPA through the assigning of a different key to each image for the encryption. In addition, the keys used for the encryption do not need to be disclosed because the encryption scheme is not public key cryptography. Therefore, the encryption can avoid the CPA, unlike public key cryptography.

C. Summary of Image Encryption for ETC Systems

The properties of the conventional encryption scheme that is one such a conventional scheme for ETC systems with the JPEG standard. The proposed ETC scheme enables to the use of a smaller block size and a larger number of blocks which increases both invisibility and security against several and different attacks. The proposed scheme includes less color information due to the use of grayscale images for image encryption which makes the ETC system more robust. The proposed scheme not only allow us to enhance security against several attacks but also to avoid the effect of color subsampling.

IV. PROPOSED SYSTEM

To proposed a novel image encryption scheme using Blowfish encryption algorithm that enhances the security of EtC systems for JPEG images. To use DCT Algorithm for Compression. To provide security using encryption. The proposed ETC scheme enables to the use of a smaller block size and a larger number of blocks which increases both invisibility and security against several and different attacks. The proposed scheme includes less color information due to the use of grayscale images for image encryption which makes the ETC system more robust. The privacy of image may be shared is under control of the user even when the SNS provider also recompresses the image. Therefore, the user can sure about the privacy by him/her. No we compare the ETC system with CTE systems, in these the user has to disclose the unencrypted images to recompress them. In the system , an image having pixel size X × Y is firstly divided into non overlapped blocks with Bx × By; then four block scrambling based processing steps are applied to the divided image.

V. CONCLUSION

This paper considered color sub-sampling operation on the grayscale-based image encryption for EtC systems. Firstly, the scenario and requirements of the image encryption were described. Moreover, we proposed to generate the grayscale based image from the luminance and sub-sampled chrominance components. A lot of images were compressed with 4:4:4 and 4:2:0 color sub-sampling ratio and decompressed to evaluate the compression performance and the robustness against color sub-sampling. The results proved that considering color sub-sampling operation to the grayscale-based image encryption does not affect the compression performance and also provides the robustness against color sub-sampling.

REFERENCES

[1] C. T. Huang, L. Huang, Z. Qin, H. Yuan, L. Zhou, V. Varadharajan, and C.- C. J. Kuo, “Survey on securing data storage in the cloud,” APSIPA Transactions on Signal and Information Processing, vol. 3, e7, 2014.

[2] R. Lagendijk, Z. Erkin, and M. Barni, “Encrypted signal processing for privacy protection: Conveying the utility of homomorphic encryption and multiparty computation,” IEEE Signal Processing Magazine, vol. 30, no. 1, pp. 82–105, 2013.

ISSN (online): 2581-3048
Volume 1, Issue 2, pp 23-26, November-2017

[3] J. Zhou, X. Liu, O. C. Au, and Y. Y. Tang, "Designing an efficient image encryption-then-compression system via prediction error clustering and random permutation," IEEE Transactions on Information Forensics and Security, vol. 9, no. 1, pp. 39–50, 2014.

[4] M.-R. Ra, R. Govindan, and A. Ortega, "P3: Toward privacy-preserving photo sharing," in Proceedings of the 10th USENIX Conference on Networked Systems Design and Implementation, 2013, pp. 515–528.

[5] W. Zeng and S. Lei, "Efficient frequency domain selective scrambling of digital video," IEEE Transactions on Multimedia, vol. 5, no. 1, pp. 118–129, 2003.

[6] I.Ito and H. Kiya, "A new class of image registration for guaranteeing secure data management," in IEEE International Conference on Image Processing (ICIP), 2008, pp. 269–272.

[7] H. Kiya and I. Ito, "Image matching between scrambled images for secure data management," in 16th European Signal Processing Conference (EUSIPCO), 2008, pp. 1–5.

[8] H. Kiya, "One-time key based phase scrambling for phaseonly correlation between visually protected images," EURASIP Journal on Information Security, vol. 2009, no. 841045, pp. 1–11, 2010.

[9] Z. Tang, X. Zhang, and W. Lan, "Efficient image encryption with block shuffling and chaotic map," Multimedia Tools Applications, vol. 74, no. 15, pp. 5429–5448, 2015.

[10] C. Li, D. Lin, and J. Lu, "Cryptanalyzing an image- scrambling encryption algorithm of pixel bits," IEEE Transactions on Multimedia, vol. 3, pp. 64–71, 2017.

****

