Encryption and Authentication of Image by Using Data Hiding

Komal Gaikwad[1], Kshitija Kurnawal[2], Dhanashri Padase[3], Deokate S.T.[4], Salve B.S.[5]

[1]Komal Gaikwad & Indapur
[2]Kshitija Kurnawal & Indapur
[3]Dhanashri Padase & Indapur
[4]Deokate S.T. & Indapur
[5]Salve B.S. & Indapur
Student, Computer Engineering, SBPCOE Indapur, Maharashtra, India
Assistant professor, Computer Engineering ,SBPCOE Indapur, Maharashtra, India

---***---

Abstract - *Day by day, data broadcasting over internetworking is accelerating tremendously. As we see lot of data is abducted over network, so it necessitates providing data security. The RDH (Reversible Data Hiding) approach is intended for gray scales images previously and it cannot be directly applied to the palette image. Here, at the sender side the palette image is used as input and the encryption of image is done by using the encrypted key. In the image, alterations are done by using the color partitioning with RGB model. After performing the encryption of the intended image, some data is hidden by utilizing data hiding key. At receiver side the received image is decrypted and the result is identified. The original contents can be reconstructed after data extraction and the contents of owners privacy remains protected.*

Key Words: **Encryption, palette image, color partitioning.**

1. INTRODUCTION

Now a day's, it is very crucial to transfer message from sender to receiver with security. In this proposed system RDH (Reversible Data Hiding Technique) allows the original contents to be properly recovered. This technique is more desirable and useful in some sensitive applications such as remote sensing, multimedia archive management and military communication. In this proposed system the image is transmitted from sender to receiver side by using the data hiding technique. The image content are only accessible to the authorized recipient and user must need to known the encryption key, data hiding key and decryption key. The sender encrypted the input palette image by using the encryption key and the color partitioning is also used for the image encryption. The data hiding side the image is hidden with data hiding key. At the last step data receiver side the decryption of image is done and the output is the original image. The data extraction is free from any and maintain the very good quality of decrypted.

1.1. PROPOSED SYSTEM

This proposed system is used to transfer message from sender to receiver with security .To secure this data from unauthorized users,we are developing a system using the Encryption,decryption and Data Hiding key. In this system colorful image(palette) is considered.The palette image means colorful image which is used as input at the sender side.Palette swill be encrypted and after that the image data will be hidden into the image using data hiding technique . At receiver side data is getting extracted by giving keys that are the data hiding and image will be decrypted by using decryption key.At the last stage we will try to gain original image with high accuracy.

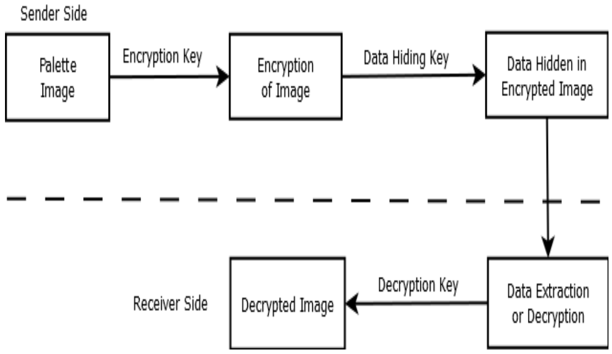

Fig. 1 Proposed System Architecture

2. LITERATURE SURVEY

The two new invertible watermarking methods for authentication of digital images in the JPEG format. The first technique is based on damage free brevity of biased bit-streams derived from the quantized JPEG coefficients. The second technique modifies the quantization matrix to enable damage free embedding of one bit per DCT coefficient. This two techniques are fast and can be used for general distortion-free (invertible) data embedding. The further focus on extending the methods to the MPEG-2 format [1].

Reversible data embedding has drawn lots of fondness scope recently. The original digital content can be completely restored. In proposed system [2] a novel reversible data embedding method for digital images. The system explores the redundancy in digital images to achieve very high embedding capacity, and keep the distortion low. The only Gray scale image distortions is low and achieve the very high embedding capacity. The further work is for difference expansions for a colorful image.

Reversible data hiding algorithm, which can recover the original image without any distortion from the marked image after the secret data have been extracted. This lower bound of PSNR is greater than that of Entire reversible data hiding techniques reported. The computational complexity is low and the execution time is short. This technique [3] frequently used images, medical images, Texture images, Aerial images and they represents the histogram of an image.

The reversible or lossless watermarking algorithm for images without using a location map in most cases. This algorithm employs forecast errors to embed data into an image. The performance of the proposed reversible watermarking scheme is evaluated using different images and compared with methods of Kamstra and Heijmans et al. these result clearly indicate that the embed more data with less distortion [4].

The integer transform based reversible watermarking is proposed. The system 1st show that Tian's difference expansion (DE) technique can be reformulated as an integer transform and other is establishing the payload dependent location map which occupies a small payload. The system [5] Tian's DE technique uses to aspects of reversible watermarking. Furthermore, selected the block with better expandable based on distortion estimation function.

A new blind authentication method based on the secret sharing technique with a data repair capability for grayscale document images via the use of the Portable Network Graphics (PNG) image is proposed. In the process of image authentication an image blocked is marked as tampered. Data repairing is then applied to each tampered block by a reverse Shamir scheme after combining two shares from unmarked blocks. Measures for protecting the security of the data hidden in the alpha channel are proposed. For more studies may be directed to choices of other block sizes just like a prime number, coefficient latent sharing etc. to improve the data repair effects [6].

The two-dimensional difference histogram modification is based on a novel reversible data hiding (RDH) scheme is proposed by using difference-pair-mapping (DPM). By considering each pixel-pair and its context, a sequence consisting of pairs of variance values is computed and a two-dimensional variance-histogram is generated by counting the frequency of the resulting difference-pairs [7]. In addition of this system a pixel pair selection strategy is used to further enhancement of embedding performance.

The novel method by using reserving room before encryption with a traditional RDH algorithm, and thus it is easy for the data hider to reversibly embed data in the encrypted image. The proposed method can achieve real reversibility, that is, data extraction and image recovery are free of any error [8]. The further improvement on the quality of marked decrypted image.

In proposed system [9] technique for authentication of images with self-repair capability for fixing tampered image data is explained. Alpha channel is collect in the greyscale image. Authentication signal is calculated by using binary image and embedded in the alpha channel to create an authentic image. After embedding the authentication signal, image is encrypted and the stego-image is detected. Then data is repaired at the pixel level by using reverse secrete sharing scheme and secret image can be recovered without any loss.

Now a days many digital documents are transferred on the internet regularly e.g. circuit diagrams, signed documents, etc.

The authentic image is encrypted at sender side and receiver side this image is decrypted. The embedded authentication signal is extracted from the received authentic image. The new authentication signal is calculated by the binary image of the received authentic image. New authentication signal is compared with the extracted signal then the integrity check is provided. The tampering of data is detected successfully without any original image backup [10]. The result is provided only for the grayscale images and supposed to expand for color images as well.

For better explore the correlation between neighbor pixels, we propose to consider the patch-level sparse representation when hiding the secret data. The widely used sparse coding technique has demonstrated that a patch can be linearly represented by some atoms in an over-complete dictionary. In this method HC-SRDHEI method which inherits the merits of RRBE and the separability property of RDH method in encrypted image [11].Further in the powerful representation of sparse coding, a large vacting room can achieved and this the data hidder can embedded more secret message.

RDH into encrypted images is increasing and regarding to researchers as the inherent content can be accurately restored after the embedded data are extracted while the content owner's secrecy remains protected. The existing RDH techniques are designed for grayscale images and cannot be directly applied to palette images. In this system we will use the encryption key and data hiding key at the sender side for encryption of image and at the receiver side the decryption is done and original image is gain. The system can be extend for video marking [12].

3. CONCLUSION

This system introduces a reliable separable RDH method for encrypted palette images. The data hider can benefit from the data-embedding space reserved by the color partitioning procedure, and apply the color replacement method to embed the additional data. The data extraction and image recovery are separable and free of any error. The proposed method can provide a satisfactory embedding payload, as well as maintain high PSNR values for the directly decrypted image.

REFERENCES

[1] J. Fridrich, M. Goljan and R. Du, "Invertible authentication," Proc. SPIE, San Jose, CA, vol. 3971, pp. 197-208, 2001.

[2] Jun Tian, "Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890-896, 2003

[3] Z. Ni, N. Ansari and W. Su, "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354-362, 2006.

[4] V. Sachnev, H. Joong 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, 2009.

[5] X. Wang, X. Li and B. Yang, "Efficient generalized integer transform for reversible watermarking," IEEE Signal Process. Lett., vol. 17, no. 6, pp. 567-560, 2010.

[6] C. Li , "A secret-sharing-based method for authentication of grayscale document images via the use of the PNG image with a data repair capability," IEEE Trans. Image Process., vol. 21, no. 1, pp. 207-218, 2012.

[7] X. Li, W. Zhang and X. Gui , "A novel reversible data hiding scheme based on two-dimensional difference-histogram modification," IEEE Trans. Inf. Forensics Security, vol. 8, no. 7, pp. 1091-1100, 2013.

[8] K. Ma, W. Zhang, X. Zhao and N. Yu, "Reversible data hiding in encrypted images by reserving room before encryption," IEEE Trans. Inf. Forensics Security, vol. 8, no. 3, pp. 553-562, 2013.

[9] Jyoti Rao, Sarika Jankar, "Greyscale Image Authentication and Repairing", IJRET, Volume: 02 Issue: 09, 2013.

[10] J. Rao, S. Jankar, "Image Tampering Detection and Repairing, International Journal of Computer Applications (0975 – 8887) Volume 85 – No 17, 2014.

[11] X. Cao, L. Du, X. Wei, D. Meng and X. Guo, "High capacity reversible data hiding in encrypted images by patch-level sparse representation," IEEE Trans. Cybernetics, [Online Available], 2015.

[12] Han-Zhou Wu, Yun-Qing Shi, Hong-Xia Wang and Lin-Na Zhou, "Separable Reversible Data Hiding for Encrypted Palette Images with Color Partitioning and Flipping Verification ." IEEE Trans. Circuits Syst. Video Technol., 2015.