Security Enhancement for Color Images Via Invisible Watermarking and Reversible Data Hiding in Encrypted Domain

Rinta Eldhose

Student, Dept. of Computer Applications, Christ Knowledge City College, Kerala, India

---

Abstract – *In this paper we propose a security enhancement method for color images. Our proposed algorithm is a LSB(least significant bit)method for steganography and AES(advanced encryption standard)for cryptography. Reversible data hiding technique is used to embed additional bits into the ciphered chrominance information. With purpose of ownership authentication, and invisible watermarking technique is used to embed a watermark into the ciphered luminance information. Experimental results show the imperceptibility, capacity and security of the proposed method in the context of watermarking and reversible data hiding techniques, respectively.*

***Key Words*:** Reversible Data-Hiding, Robust Watermarking, Encrypted Images, Decrypted images.

1.INTRODUCTION *(Size 11 , cambria font)*

Data hiding technique over encrypted domain gain more and more attentiveness; the research about modality reversible is triggered. In this way, to securely store and share of multimedia data between transmitter-receiver, a content owner may encrypt the data before transmission. An application manager hopes to append some additional message, e.g., the source information, image annotation or authentication data, within the encrypted media,even though he does not know to the plaintext content. It may be also hopeful to that the original content or an approximation of this can be recovered after the decryption and data extraction at receiver side.

Reversible data hiding in encrypted domain consist of two stages, the first one embeds additional information into encrypted data without revealing the plaintext content, the second one allows recover embedding data and the original or an approximated version of the plaintext content. In invisible watermarking, a signal is called the 'watermark' is embedded in to a frequency domain of the image in a such a way that observers are incapable to the distinguishing of Reversible data hiding technique is used to embed additional bits into the ciphered chrominance information.

difference to the original and watermarked images with a naked eye.

In this project the three options are available for the receivers to who hold different keys: a) extract embedded additional bits and the watermark, b) decrypt in the watermarked image with embedded additional bits, or c) extract in the additional bits, the watermark and generate to the recovered image that is identical to the original, respectively. In the experimental results show imperceptibility, capacity and security of the proposed method in the context of watermarking and reversible data hiding techniques, respectively.

2. PROPOSED METHOD

We proposed a security enhancement method for color images management by combining invisible watermarking and reversible data-hiding. Our proposed algorithm is a LSB(least significant bit)method for steganography and AES(advanced encryption standard)for cryptography. Reversible data hiding technique is used to embed additional bits in to the ciphered chrominance information. With purpose of ownership authentication, an invisible watermarking technique is used to embed a watermark in to the ciphered luminance information. Embedding to a invisible watermark is a luminance information in an a YCbCr color model gives the mark to a certain number of the robust properties with respect to the JPEG lossy compression and the another common signal processing operations. And also, the use of chrominance information increases a capacity of the RDH (reversible data hiding)in encrypted domain proposed method.

2.2 OBJECTIVE OF THE PROJECT

Main objective and scope of the this project is to provide more security, high robustness, high imperceptibility the use of chrominance information increases the capacity of the RDH in encrypted domain proposed method. The security enhancement method for color images management by combining invisible watermarking and reversible datahiding. Advantages are

- High robustness
- Common signal processing operations
- High imperceptibility

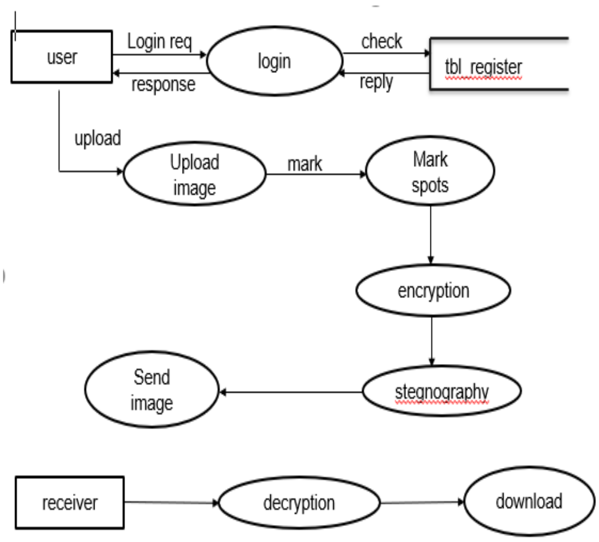

Fig1: Data flow diagram

Encryption

- Watermarking is used to encryption the most effective way to achieve data security.
- It access to a secret key or password.

Decryption

- Watermarking is used to decryption the conversion of encrypted data into its original form.

Stegnography

- Stegnography an encryption technique .
- Stegnography is data hidden with data.

This diagram to explain to this paper we propose a security enhancement method of the color images. The diagram is composed by a combination of invisible watermarking and reversible datahiding, they both performed after encryption of the color images. Also this diagram to explain how user and receiver can send and receive the images and the other processing to diagrammatically explain.

2.3 Content-Owner

Using the encryption key conceal to the original image with or without some pre-processing. Data-Hider: To increase a security, the data hiding key is used to a embed the additional bits of the encrypted image. Receiver: Three options are available for receivers who hold different keys: first is extract embedded additional bits, second is decrypt the image with embedded additional bits, or third the extract the additional bits and generate the recovered image that is identical to the original.

On the other hand, digital image watermarking is consider to a suitable solution for the ownership authentication purposes they it is able to add a signal to the image that can be seal or mark it . Accordingly the different applications and requirements, the digital image watermarking can mainly classify into two types: visible and invisible. In invisible watermarking, a signal is called a 'watermark' they embedded in a spatial or frequency domain of the image . In such a way that the observers are incapable the distinguishing of difference between the original and watermarked images with the naked eye.

Diagram is composed by a encryption, decryption and steganography. Encryption is used the watermarking is used to encryption the most effective way to achieve data security. It access to a secret key or password. Decryption is watermarking is used to decryption the conversion of encrypted data into its original form.Steganography an encryption technique. Steganography is a data hidden with the data. Initially the original image is safely to hidden to the form of encryption and then the each component is ciphered by applying a chaotic mixing procedure and the most effective method to achieve a data security. Reversible data hiding technique are used to embed a additional bits in the ciphered chrominance information via the data hider. With the purposes of a ownership authentication, in an invisible watermarking technique are used to embed a watermark in the ciphered luminance information via the data hider. Finally, to increase a security of the method, and also steganography an encryption technique. The steganography is data hidden with data.

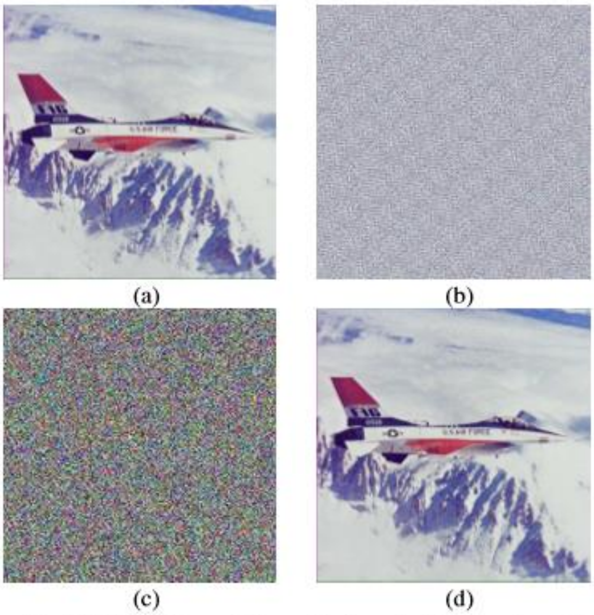

Fig :2 (a) Original image. (b) Image (a) after embedding procedure and encryted. (c) Image (d) Recovered image after the conversion of encrypted image to the original image.

3.CONCLUSION

A security enhancement method for the color images management to combining the invisible watermarking and reversible data-hiding , and both performed in the encrypted domain for the color images. The viewpoint of invisible watermarking, the proposed method are shows high robustness against several geometric, common signal processing operations and combined distortions, as well as high imperceptibility. The Hybrid applications are the purposes of authentication and confidentiality, that requiring the color image continue protected to when it has decrypted and/or restored by the reversible data hiding method.

ACKNOWLEDGEMENT

I would like to extend my heartfelt thanks to Ms. Geethu Krishna Kartha, HoD, Assistant Professor, Department of Dual Degree Master Of Computer Applications for their valuable advices and guidance throughout my course of study. My most sincere thanks go to my mentor, Asst. Prof. Ms. Aimy Susan Thomas for her encouragement and support. I would like to show my sincere gratitude to Asst. Prof. Ms. Saranya Shaji for her guidance and idea, without her this paper would not be complete. She has given idea which helped me to accomplish writing this paper.

REFERENCES

[1] [1] Y.Q. Shi, X. Li, X. Zhang, H.T. Wu and B. Ma, “Reversible data hiding: Advances in the past two decades” in IEEE Access, vol. 4, pp. 3210-3237, 2016.

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

[3] C.-W. Shiu, Y.-C. Chen, and W. Hong, "Encrypted image-based reversible data hiding with public key cryptography from difference expansion," Signal Process., Image Commun., vol. 39, pp. 226-233, Nov. 2015.

[4] X. Zhang, "Reversible data hiding in encrypted image," IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255-258, Apr. 2011.

[5] M. Cedillo-Hernandez, A. Cedillo-Hernandez, F. Garcia-Ugalde, M. Nakano-Miyatake, H. Perez-Meana, "Digital Color Images Ownership Authentication via Efficient and Robust Watermarking in a Hybrid Domain," Radioengineering Journal. 26(2), pp. 536-551, 2017.