ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 8, February 2014

Data Hiding in Colored Encrypted Images

A.Pavithra, K. Saranya
Department of Pervasive computing Technology,
Kings College of Engineering, Punalkulam, Tamilnadu

Abstract*— Encryption plays a vital role in the domain of data security. Information retrieval from hidden content or encrypted data is an interesting task. That too the information has to be extracted to a plain environment where it can be utilized efficiently. RDH formula is used to reserve space for data which is used to attach additional data so it becomes easy for the users. Proposed system also extracts data from encrypted form without any error. Thereby hider and receiver can do their activities easily. Idea proposed will be with appreciable capacity of assuring secrecy. Real changeableness, information extraction and improvement on marked decrypted Images are features of novel method. To achieve image quality ten times as massive payloads are used while performing experiments based on this algorithm. Block smoothness can be used to perform data extraction and image recovery. When encrypting the complete information of associate uncompressed image by a stream cipher, the extra information may be embedded into the image by modifying tiny low proportion of encrypted information. With associate encrypted image containing extra information, one could first decode it victimization the cryptography key, and therefore the decrypted version is analogous to the initial image per the data-hiding key, with the help of spatial correlation in natural image, the embedded information may be with success extracted and therefore the original image may be absolutely recovered.

***Index Terms*—Advanced encryption standard, color histogram, least significant bit, Reversible Data Hiding**

I. INTRODUCTION

A large amount of information is being transmitted over the internet, not only text but image, audio, video and multimedia files. Images are used in day to day activities so security of image and data is very important. Steganography includes the concealment of information within computer files [1]. Electronic communications includes in digital Steganography so that the steganographic coding inside a transport layer, such as a document, image, program or protocol. Media files are unique for steganographic transmission because of their large size. Text steganography is the most difficult type of Steganography because of the lack of redundancy in text as compared to image and audio. It requires less memory and provides simple communication [2]. Steganography means secret communication which cannot be removed without significantly altering the data in which it is embedded. The embedded data must be confidential unless an attacker can find a way to detect it. So, attacker can easily find the data, because that module uses RSA algorithm [3].

II. PROBLEM STATEMENT

The cryptography concept is mainly used to hide the content of the messages. It does not hide the existence of the messages. To hide the data in particular bit using public key, original messages can be easily extracted [4]. The receiver decrypts the original image and embedded data using the single key. In the existing System more attention is paid to reversible data hiding (RDH) in encrypted images, since it maintains the property that the original cover can be losslessly recovered after embedded data is extracted while protecting the image content's confidentiality [5]. The previous methods embedded data by reversibly vacating room from the encrypted images, subjected to errors on data extraction and/or image. Previous methods implement RDH in encrypted images by vacating room after encryption, from that is proposed by reserving room before encryption [6]. The data hider can take advantage from the extra space emptied out in earlier stage to make this process effortless [7].

III. SYSTEM GOAL

The advantage of all traditional RDH techniques for plain images is used to achieve excellent performance without loss of perfect secrecy. This method can achieve real reversibility, separate extraction of data and improved on the quality of marked decrypted images [8]. Reserving room before encryption method with a traditional reversible Data Hiding algorithm, and it is easy for the data hider to reversibly embed data in the encrypted image and thus can achieve real reversibility that is extraction of data and recovery of image without error [9]. This system uses the concept of Stegano graphy to hide the content of messages and existence of the message. The original image is encrypted using an encryption key and the additional data are embedded into the encrypted image using a data-hiding key. It uses a novel scheme for separable reversible data hiding in encrypted image. Then, a data-hider may compress the least significant bits of the encrypted image using a data-hiding key to create a sparse space to accommodate some additional data [10].

IV. SYSTEM DESIGN

As stated earlier security is a main concern in this proposed idea. Therefore to assure security the data which is ready for transmission is subjected to cryptographic techniques such as encryption and decryption with a public key. Also a cover is embedded to the data which is the main entity of the proposed idea.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 8, February 2014

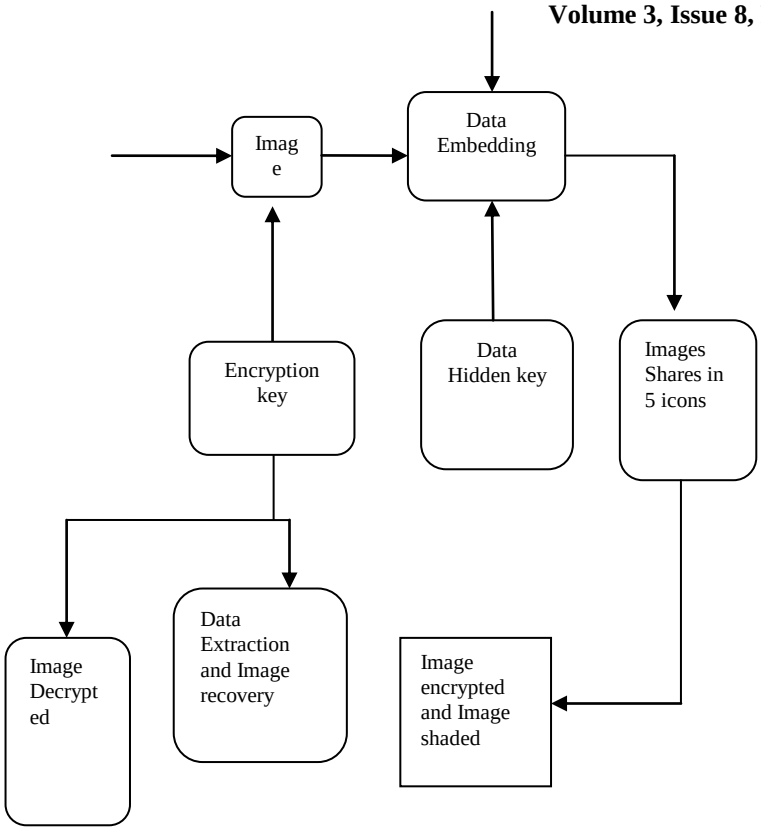

Fig.1 System Architecture

V. IMPLEMENTATION

A real time images as well as text content are considered as data for transmission between authenticated parties. This data is encrypted in the sender part and decrypted in the receiver part so that intruders are not familiar about the data which is transmitted during communication. Public key plays a main role in this task. Additionally text is embedded when the data transmitted is an image whereas this text does not appear in textual data. Data is encrypted and hided within an image. Overall task includes the process of capturing image and adding a cover for encryption. It is termed as data embedding and here data refers to the process of adding additional image. This indicates the completion of encryption. Key is known between trusted parties. Mean while in decryption the added cover is removed so that original data can be accessed and processed. Altering data refers to encryption and decryption and retrieving data is the work done in Data extraction and image recovery. Images and text can be encrypted and decrypted using public keys. Assurance of security is the most prioritized task in the proposed idea. Embedded cover can be partitioned into various segments using color histograms.

VI. CONCLUSION

Real changeability can be achieved by utilizing this novel technique. Information extraction is done separately apart from the decrypting images using the public key. Image secret writing, data embedding and knowledge extraction/image recovery are performed in Encryption. The content owner encrypts the initial uncompressed image using associate secret writing key is done in the initial phase. If the data hider is not capable of retrieving full data content which is hidden then small bits of information in the encrypted data is used to form the original data. The key can be used effectively if the lost data The lossy compression technique is compatible with encrypted pictures. In future, a comprehensive combination of image secret writing and knowledge activity is compatible with lossy compression deserves additional investigation.

REFERENCES

[1] Efficient Reversible Watermarking Based on Adaptive Prediction-Error Expansion and pixel selection, Authors: Xiaolong Li, Bin Yang, TieyongZeng, IEEE Transaction Image Processing., vol. 20, no.12, pp.3524-3533, December 2011.

[2] Reversible Data Hiding, Authors: Z.Ni, Y.Shi, N.Ansari, S.Wei IEEE Transaction Circuit System Video Technology. vol. 16, no. 3, pp. 354-362, March 2006.

[3] Reversible Data Hiding in Encrypted Image, Authors: Xinpeng Zhang IEEE Signal Processing. vol. 18, no. 4, April 2011.

[4] Fundamentals Of Data Hiding Security And Their Application To Spread-Spectrum Analysis, Authors: Henrique S. Malvar IEEE Transaction on Signal Processing., vol. 51, no.4,April 2003.

[5] The Effective Key Length Of Watermarking Schemes, Authors: Patrick Bas, Teddy furon, Francois Cayre IEEE ICASSP 2012.

[6] Spread-Spectrum Watermarking Security, Authors: Fernando perez-Gonzalez IEEE Information Forensics and Security. vol. 4 March 2009.

[7] Watermarking Security: Theory And Practice, Authors: Francois Cayre, Caroline Fontaine, and Teddy Furon IEEE Transactions on Signal Processing, vol xx, no.y, xyz 2005.

[8] Reversibility improved data hiding in encrypted images, Authors: WeimingZhangn, KedeMa, NenghaiYu Signal Processing., vol. 94 January 2014.

[9] Reversible Watermarking of 3D Mesh Models by Prediction-error Expansion, Authors: Hao-tian Wu, Jean-Luc Dugelay IEEE Conference on Multimedia Signal Processing, October 2008.

[10] Expansion Embedding Techniques for Reversible Watermarking Authors: Diljith M. Thodi Jeffrey J. Rodríguez IEEE Transactions on Image Processing, vol. 16 March 2007.