# Digital Image watermarking and Encryption using Public Key cryptosystem

**B SARITHA[1], L.MIHIRA PRIYA[2], V.THRIMURTHULU[3]**
P.G.SCHOLAR, Department of ECE, Chadalawada Venkata Subbaiah College of Engineering, Tirupati
Assistant Professor, Department of ECE, Chadalawada venkata Subbaiah College of Engineering,
Professor, Department of ECE, Chadalawada Venkata Subbaiah college of Engineering, Tirupati

***Abstract:*** ***This paper proposes a lossless and combined data hiding method for cipher text images encrypted by public key cryptosystem. In the lossless scheme, the lower byte cipher text pixels are replaced with watermark image pixels data and passed through the wavelet transforms. Then, the embedded data can be directly extracted from the encrypted domain, and the data embedding operation does not affect the decryption of original plaintext image. In this paper embedded text data also added where ever the input image is have the less important information. With the combined technique, a receiver may extract a part of embedded data before decryption, and extract another part of embedded data and recover the original plaintext image after decryption. This process ensures the secured transmission of the data from the transmitter to receiver by the authorized persons. The data from the transmitter to the receiver is thus processed through the authorized key accessed at the receiver and then the original image is recovered thus recovered through the decryption process. This work proposes the secured data transmission of data which may include the text and the image through necessary steps of developing the filtering algorithms and accessed at the receiver with the authentication key thus protecting the original imaged hidden inside through watermarking hence makes the system completely safe and worthwhile in communication systems.***

***Index Terms—Data hiding, image encryption, image Decryption***

---

## I INTRODUCTION

Steganography is the process of hiding the data in a covering media to provide security.in this process, a covering media is taken (i.e., plain text, images, audio, video and so on) and the secret message is imbibed into the covering media [1,2].Encryption and data hiding are two effective means of data protection. While the encryption techniques convert plaintext content into unreadable cipher text, the data hiding techniques embed additional data into cover media by introducing slight modifications.

We say a data hiding method is lossless if the display of cover signal containing embedded data is same as that of original cover even though the cover data have been modified for data embedding. For example, in [3], the pixels with the most used colour in a palette image are assigned to some unused colour indices for carrying the additional data, and these indices are redirected to the most used colour. This way, although the indices of these pixels are altered, the actual colours of the pixels are kept unchanged. On the other hand, we say a data hiding method is reversible if the original cover content can be perfectly recovered from the cover version containing embedded data even though a slight distortion has been introduced in data embedding procedure [4-6].

## II LITERATURE SURVEY

With the growing advancements in technology, there is a growing insecurity of data transmission from source to destination. The problem of confidentiality and access of data by unlicensed and unauthorized persons leading to the compromise of original data and thus may lead to a hazardous situation. ). Data transmission over a wide range of different networks is not a simple mission, audio, image, video and different multimedia having different type of data when we deal with multimedia. Security for multimedia has been developed in last two years, which offer a category of tool-units and design insights for safety, with enhancement of fundamental media. The major concern is safety and confidentiality of a digital packet of multimedia records is important query. This work develops a best method of ensuring security through arrangement of Encryption Algorithms by characterizing central idea of cryptographic system and image encryption and decryption thus ensuring protection of data.

## III PROPOSED METHOD

In the proposed algorithm, we are manipulating the image as well as the key part. Manipulation of image as well as the key [9] part gives more security to the image. The following steps are used in the proposed algorithm as shown in figure1.

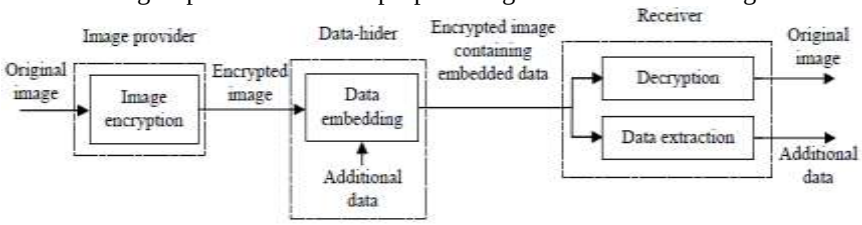


Fig 1. Lossless and data hiding public key encryption

This paper proposes a lossless, a reversible, and a combined data hiding method for public-key-encrypted images by exploiting the watermark image and text data [3, 4, 5]. With these schemes, the pixel division/reorganization is avoided and the encryption/decryption is performed on the cover pixels directly, so that the amount of encrypted data and the computational complexity are lowered. The encryption processing steps are shown in the following figure2.

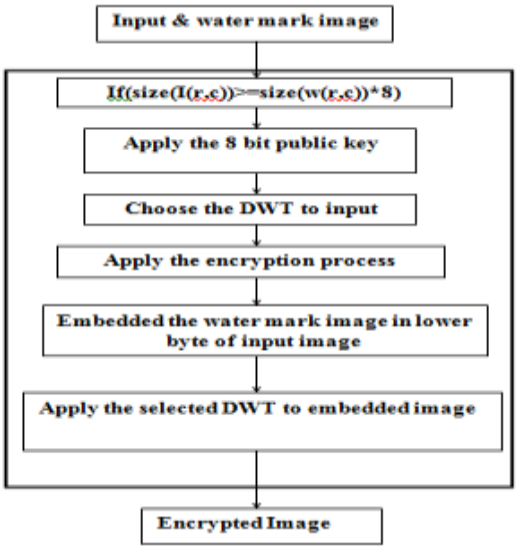


Fig 2 Block Diagram of Proposed Encryption Process

In the next step, we will divide the image into the blocks having 8 bits i.e., every block will contain 8 pixels. The lower byte of each pixel will be performed xor operation with the lower byte of original input image which is saved in the memory. This process will be repeated up to the last pixel of watermark image size covered in the embedded image. After performing these steps, the resultant image will be obtained which is similar the original image. This resultant image is called the decrypted image [9-11] as shown in figure 3.

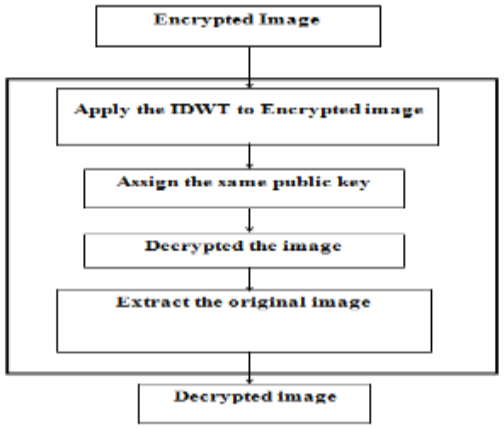


Fig 3 Block Diagram of Proposed Decryption Algorithm

IV RESULTS

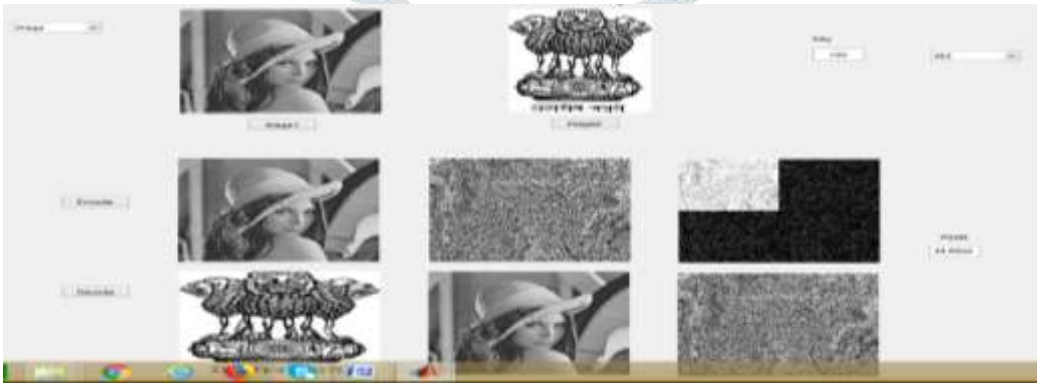

Figure 4 encryption and Decryption process for Lena with watermark image

The above figure 4 shows that encrypted image of given input and watermark data through the GUI. Here the watermark image has not shown in the embedded image but hided in the image and the encrypted image is in looking as corrupted for unauthorized persons and decrypted image of encrypted data through the GUI. Here the watermark image and original image are retrieved back to corresponding authorized persons [7, 8]

Figure 5 Encryption and decryption process for Lena with watermark text data

The above figure 5 shows that encrypted image of given input and watermark text data through the GUI. Here the watermark text data has not shown in the embedded image but hided in the image and the encrypted image is in looking as corrupted for unauthorized persons and decrypted image of encrypted data through the GUI. Here the watermark text data and original image are retrieved back to corresponding authorized persons [10-12].
The performance measures for the both embedded data are shown in the following table 4.1.

Table 4.1 The performance measures of the existing and proposed methods

| **Embedded data** | **PSNR** |
|---|---|
| Image | 48.6942 |
| Text | 74.9602 |

IV CONCLUSION AND FUTURE SCOPE

Digital image transmission has become very common in these days. To improve the security of the image in the transmission process, encryption is used. In the process, every pixel is taken which is having eight bits and encrypted with only image to get the encrypted image. In the proposed method, embedded process is done with watermark image and text data. By observing the results and the performance measures, the proposed method is giving the better results.

This paper proposed a modified process in the image encryption process by manipulating both the input image as well as the key. In this paper, we have created a blocks of 8 bits of public key. This paper can be done by taking the blocks of 64 bits size, 128 bits size and so on. The encryption process is done in many stages to improve the security. If the number of stages is increasing, the extent of security will be increased. This process will also be used for the encryption of colour images [13].

REFERENCES

[1] AtulKahate, Cryptography and Network Security, 2nd edition,TataMcgraw Hill Education Private Limited, 2011
[2] Xiukun Li, Xiangqian Wu*, Ning Qi, Kuanquan Wang, A Novel Cryptographic Algorithm based on Iris Feature, 2008.
[3] B. Santhi, K.S. Ravichandran, A.P. Arun and L. Chakkarapani, A Novel Cryptographic Key Generation Method Using Image Features, 2012.
[4] B.Acharya, SK Panigrahy, SkPatra, Image Encryption Using Advanced Hill Cypher Algorithm, 2009.
[5] A.Jolfari, XW Wu, V Muthukkumarasamy, Commenta on the Security of "Diffusion-Substistution Based Gray Image Encryption" Scheme, 2014.
[6] Q Wang, Q Ding, Z Zhang, L Ding, Digital Image Encryption Research Based on dwt and chaos,2008.
[7] Z Lin, H Wang, Efficient Image Encryption Using Chaos-based PWL Memrister, 2010.
[8] PP Dang, PM Chau, Image Encryption for Secure Internet Multimedia Applications, 2000.
[9] P. Paillier, "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes," Proceeding of the Advances Cryptology, EUROCRYPT'99, LNCS, 1592, pp. 223-238, 1999.
[10] T. Bianchi, A. Piva, and M. Barni, "On the Implementation of the Discrete Fourier Transform in the Encrypted Domain," IEEE Trans. Information Forensics and Security, 4(1), pp. 86–97, 2009.
[11]T. Bianchi, A. Piva, and M. Barni, "Composite Signal Representation for Fast and Storage-Efficient Processing of Encrypted Signals," IEEE Trans. Information Forensics and Security, 5(1), pp. 180–187, 2010.
[12]P. Zheng, and J. Huang, "Discrete Wavelet Transform and Data Expansion Reduction in Homomorphic Encrypted Domain," IEEE Trans. Image Processing, 22(6), pp. 2455-2468, 2013.
[13] Pratik Srivastava, Ratesh Jain, K.S. Raghuwanshi, A Modified Approach of Key Manipulation in Cryptography using 2D Graphics Image, 2014.