International Journal of Research
eISSN: 2348-6848 & *pISSN:* **2348-795X** *Vol-5 Special Issue-13*
International Conference on Innovation and Research in Engineering, Science & Technology
Held on 23rd & 24th February 2018, Organized by Tulsiramji Gaikwad Patil College of Engineering & Technology, Nagpur, 441108, Maharastra, India.

Data Hiding With Improved Image Quality

Trushi Nandagawali, Nupur Taras,
Manjiri Suryawanshi, Snehal Zodpe,
Department Of Electronics Engineering,
K.D.K. College Of Engineering, Nagpur, India
snehalzodpe711@gmail.com

Abstract
In this paper, data hiding is done with the help of multimedia image and advanced security will be provided. In simple secure data hiding technique is use for reading the pixel capacity of images for text hiding. This method is applicable for RGB color model and JPEG images used to cover data for pixel value to check capacity. Then a secret key is used in data embedding process which makes very difficult for intruder to access to data and images. The intra prediction mode algorithm will be used for improving image quality and security enhancement.

Keywords: **- Encryption, Decryption, Intra prediction mode Data hiding, Data compression**.

I INTRODUCTION

The images and videos from various sources are frequently used and transmitted through the internet for various applications, such as online images, medical images or video albums and military image. Military images usually contain private or confidential information which is transmitted from sender to receiver over a communication network. Cryptography plays an important role for transmitting these secret images over insecure network. Now days when more sensitive information is stored on computers and transmitted over sender and receiver side through the Internet, we need image security and safety. Image is also an important part of information. Therefore it is very important to protect image from unauthorized access. There are many method/algorithms available to protect image from unauthorized access which include third party. Internet communication has become an integral part of the Infrastructure of today's world. The information communicated comes in numerous forms and is used in many applications. In a large number of these applications, it is desired that the communication be done in secrete. Such secret communication ranges from the obvious cases of bank transfers, corporate communications, and credit card purchases, on down to a large percentage of everyday email. With email, many people wrongly assume that their communication is safe because it is just a small piece of an enormous amount of data being sent worldwide. After all, who is going to see it? But in reality, the Internet is not a secure medium, and there are programs "out there" which just sit and watch messages go by for interesting information.

Encryption provides an obvious approach to information security, and encryption programs are readily available. However, encryption clearly marks a message as containing "interesting" information, and the encrypted message becomes subject to attack. Furthermore, in many cases it is desirable to send information without anyone even noticing that information has been sent secret information

Third party is nothing but intruder. Data hiding is embedding secret information inside image in such a way that quality of image should not degrade. The data is embedded in digital images by altering the pixel value of image for secret communication. The image which is used for hiding secret data can be recovered to its original state after the extraction of the secret data. Previous work includes encryption, compression and data hiding in a single step into other images. In section II the current literature, different data hiding techniques discussed. In section III we discussed proposed technique to solve the problem of image integrity and secrecy. After that In Section IV we discussed the proposed solution. In section V we conclude the paper and show possible areas of enhancement and our future plan for secure transmission of image.

II RELATED WORK

Ya-Lin Lee, and Wen-Hsiang Tsai, [1], proposed that in this paper, two images are taken, secret image and target image. Secret image is fitted in target image by transforming color characteristics. Encrypted image requires more space because compression algorithm is not used. This method makes a use of color characteristics of image for encryption. In pixels' values recording different images in transfer color space. The information is required for the recovering secret image is embedded into the mosaic image creation by data compression using such key.

Zhenxing Qian [2] in proposed system JPEG images are encrypted bit stream. The original JPEG bit stream maintains

International Journal of Research
eISSN: 2348-6848 & pISSN: 2348-795X Vol-5 Special Issue-13
International Conference on Innovation and Research in Engineering, Science & Technology
Held on 23rd & 24th February 2018, Organized by Tulsiramji Gaikwad Patil College of Engineering & Technology, Nagpur, 441108, Maharastra, India.

encrypted images to hide images content with bit stream preserve structure. The secret message bit an encoded with error correction code by using decryption and encryption to embedding key, bit stream carrying secret data can be correctly encoded. The secret message bits are encoded with error correction codes to gain perfect data extraction of image recovery. If receiver has both keys, the secret bits of original bit stream perfectly recovered.

Kede Ma, Weiming Zhang, Xianfeng Zhao [3] proposed an image encryption method which makes a use of two keys, one for encryption and other for decryption plus data hiding. The least Significant bits (LSBs) of the encrypted image are compressed using a data hiding key to create space to embed an additional data. Reversible data hiding (RDH) is an encrypted images, it maintains the image quality an original cover can be lossless recovered after embedded data is extracted while protecting the image content's confidentiality. In novel methods embedded data by reversibly vacating room from the encrypted images, which may be subject to some errors on data extraction and image restoration.

Weiming Zhang, Xiaocheng Hu, Xiaolong Li, [4] proposed RDH method in which embedding process is divided into three step. The first step includes lossless encryption from original image of binary covers. Second step contain decryption message compress method to save spatial images. Third step contain embedding data inside image.

Parag Kadam [5] proposed a data hiding technique which makes an use of LSB technique. A new scheme is proposed to data cannot be extracted correctly. In order to enhance solve the problem in which the embedded secret and improve the image quality of the stego-image and to increase the embedding capacity of the source-image, a method to insert secret data into the host-image the adaptive LSB substitution technique based on the pixel-value differencing is discussed.

C. Anuradha [6] proposed the Secure and authentication discrete reversible data hiding in cipher images with security and authentication. Owner encrypts the original uncompressed image using an encryption key. Data hider may compress LSB bit of encrypt image using SHA-1 algorithm.

Weiming Zhang, Biao Chen, [7] In this paper eversible data hiding (RDH) technique, these two images are given first original image cover can be restored after the stego images embedded information is extracted, we improved the recursive code construction the rate–distortion RDH schemes that use binary feature sequence as covers, i.e., RS scheme for spatial images, one scheme for JPEG images, and a pattern substitution scheme for binary images.

V. Manjula, [8] proposed a method of lossless image or video compression in spatial domain. Algorithm divides into an image into number of blocks and each pixel in that block is represented using variable length bits. Variable bits calculation is dependent on pixel values of each block. The advantage of this method is dependent upon pixels correlation within a block and compressed video.

Samira Buchanan [9] proposed the Intra prediction mode method to improve data and bit rate increases. In this algorithm each pixel of the binary valued and secret images is 2x2 pixels.

Shih-Hau Fang [10] in this paper RSA algorithm is discussed. It takes 2 prime number. It is a public key encryption algorithm. It uses private key and public key. It should be similar bit length. Number p and q for security purposes the integer p and q should be chosen at random number.

III PROPOSED SYSTEM AND OBJECTIVE

An image is selected for the data hiding. The Stream ciphers are an important class of symmetric encryption. It encrypts binary digits of a plain-image one at a time using an encryption transformation which varies with time. A stream cipher is an encrypted key where plain-image bits are combined with a key stream. Image encryption is an important and effective technique to protect image from unauthorized access. Bit stream-based approach is designed for encryption without the need for recompression, which is useful when there is no possibility to intercept the encoding process. In Data hiding the fast intra prediction mode algorithm is used which virtually increase the memory capacity of an allowing data. A novel approach for encryption key generation is proposed which is further is used to encrypt the created image encryption and for fast transmission of that encrypted image lossless compression technique is used if the receiver has only data hiding key, receiver cannot extract the original content. If the receiver has both encryption and data hiding key, receiver can recover original images. The working of each of the module is explained in detailed below

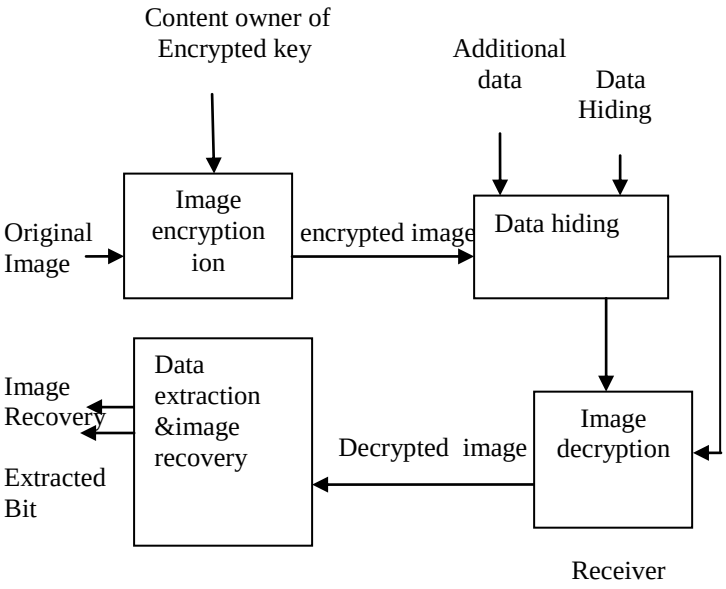

fig .flow of data hiding scheme

Flow of data hiding scheme

Sender side data or content owner

1 Select original image

International Journal of Research
eISSN: 2348-6848 & pISSN: 2348-795X Vol-5 Special Issue-13
International Conference on Innovation and Research in Engineering, Science & Technology
Held on 23rd & 24th February 2018, Organized by Tulsiramji Gaikwad Patil College of Engineering & Technology, Nagpur, 441108, Maharastra, India.

2 Encrypted key using image encryption

3 Data hiding an cover image into encrypted image

4 Display result of hide image

Receiver side data

1 Select hide image

2 Extraction of hidden encrypted image

3 Decrypted image

4 Data extraction

5 Generate original image

6 Show receiver side result

A. Reading the average value of RGB

Reading the images from hard disk and calculating there pixel information and writing on the picture box. The pixel scanning stores the information of pixel in the buffers memory In the form of the color information by using a RGB function which shows the capacity of the pixel so that the compressed data can be stored accordingly The compressed data with key is calculated in from bit size which will be stored in pixel. While storing these data in the image pixel we have get the matching size so that the image should not get damage. Calculating the value of each pixel in that image from that matrix from each row and column. Image size and pixels each digital image on a computer is a file which contains graphical information instead of text executable program .the digital image contain pixel which can be considered as small dots on an image. They are spared on a digital image across the height and width. They are very small in size and place so closely to each other we cannot identify a particular pixel in an image when it is display on computer monitor .in RGB image, each pixel has a color which is a combination 3 primary color -red, blue, and green. So, each pixel has a RED, GREEN and BLUE color component. The physical dimensions of a digital image are measured with respect to number of pixel in it and are commonly called as pixel or image resolution .pixel in a digital image are scalable to different physical size However, all the pixels in an image are of the same size. If pixel does not have sufficient size with show that there no space in image pixel.

EXPERIMENTAL SETUP

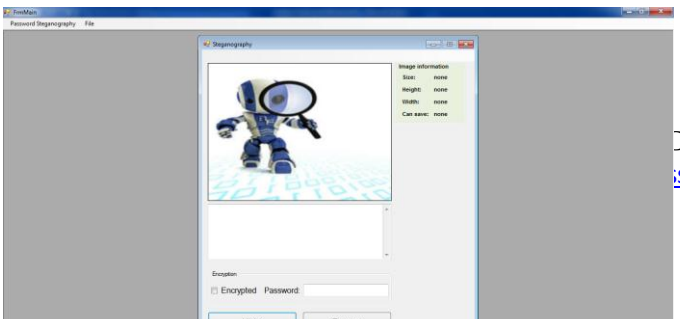

Fig 1. Browse any standard grayscale or color image which sender want to transmit securely.

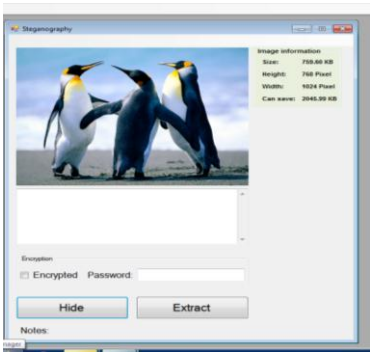

Fig 2. Reading pixel capacity

Fig 3. Data Has been Hide in image

B. Collection of pixel capacity

Collect the information of pixel capacity to store hidden data to calculate amount of data stored in an image. Range of pixel value lies between 0-255.

C Getting the encrypted data

In this module encrypted image is generated. So that scrambled image is generated which is untraceable.

D Generation of random key

The process will be generating random key to provide security. Using this key reverse process will be done by receiver side. The secret key is used for providing security to image. so that intruder can't access the original image.

E. Regeneration of image

In this module original image is recovered which is same as transmitted image. Data is recovered from image. After that quality of recovered image is checked based on the some image parameter.

TABLE I
COMPARATIVE ANALYSIS

Parameters	methods	description
Image pixel density	Reversible data hiding	Image recover to the receiver
histogram value	Recursive histogram modification	Input the stego -sequence
Message bit	Error correction codes Used to encodes the plain message bit	Correct extraction of the secret data
Signal	rate distortion model	Improve the image quality
Pixel	Intra prediction mode	Divide the pixel capacity

From the above comparative analysis intra prediction mode (IPM) approach is well suited for providing more security to image, so that image quality is improved.

V CONCLUSION

The main goal of secure transformation of data in encrypted image is to provide high security for data transformation and also to extract the hidden data and recover the original content without any error by exploiting spatial correlation in natural image if the amount of data is not too large. When using a color image instead of gray, each bit of the red, green and blue color components can be used, so a total of 3 bits can be stored in each pixel. It gives a relatively large amount of space to hide data. The image based data hiding technique is tried to improve the capacity of hidden data since, there is a limitation on how much information can be hidden into an image. To overcome the capacity problem, the data hiding has been achieved and to provide high security separate key can be used for encryption and decryption. In this paper different methods for hiding data inside the image were discussed and there drawbacks are removed by discussing proposed method.

REFERENCES

[1] Ya-Lin Lee, " A New Secure Image Transmission Technique Via Secret Fragment Visible Mosaics Images By Nearly Reversible Color Transformation. ," IEEE Transaction On Circuit and System For Video Technology, Vol . 24 no. 4 April 2014.

[2] Zhenxing Qian,"Reversible Data Hiding In Encrypted JPEG Bit Stream," IEEE Transaction On Multimedia Vol.16 no. August 2014

[3] W. Zhang, "Reversible Data Hiding In Encrypted Images By Reserving Room Before Encryption," IEEE Transaction on Information Forensic and Security, Vol, 8 no. 3 March 2013.

[4] Xiaochen Hu, Recursive Histogram Modification Establishing Equivalency Between Reversible Data Hiding And Lossless Data Compression," IEEE Transaction On Image Processing Vol, 22 no 7, July 2013.

[5] P. Kadam, "Separable Reversible Encrypted Data Hiding In Encrypted Using AEs Algorithm And Lossy Technique", International Conference On Pattern Recognition February 2013.

[6] C. Anuradha, "Secure and Authentication Reversible Data Hiding in Encrypted Image", International Journals of Advanced Research in Computers Science Vol no.3, 4 April 2013.

[7] W. Zhang, B. Chen, and N. Yu, "Improving Various Reversible Data Hiding Scheme Via Optimal Codes For Binary Covers," IEEE Transaction Image Process., Vol. 21 no. 6,June 2012.

[8] V. Manjula, "Secure Data Hiding Technique In Compressed Video Using A Secret Key," International Journals Computers Science and Technology, Vol .3 2012.

[9] Samira Bauchama, "H.264/AVC Data Hiding Based On Intra Prediction Mode for Real Time Application," ISSN Oct 2012

[10] Shih-Hau Fang; Wei-Jia Lai; Yi-Chung Liang, "An encryption-based approach for protecting privacy in network-

based location systems," Machine Learning and Cybernetics (ICMLC), 2011 International Conference on , vol.1, no., pp.377,380, 10-13 July 2011.

[11] R. Tao, X. Meng, and Y. Wang, "Image encryption with multiorders of fractional Fourier transforms," IEEE Trans. Inf.Forensics Security, vol. 5, no. 4, pp. 734–738, Dec. 2010.

[12] Ponomarenko, N.N.; Egiazarian, K.O.; Lukin, Vladimir V.; Astola, J.T., "High-Quality DCT-Based Image Compression Using Partition Schemes", Signal Processing Letters, IEEE , vol.14, no.2, pp.105,108, Feb. 2007

[13] Suk-Ling Li, Kai-Chi Leung,Cheng, L. M. Chi-Kwong Chan, "Data Hiding in Images by Adaptive LSB Substitution Based on the Pixel-Value Differencing",