Reversible Data Hiding in Color Images Using AES Data Encryption System

Sreelatha G
College:-Jagruthi Institute of Engineering &Technology.
Mtech DECS, India
gellisreelatha@gmail.com

ABSTRACT:-

The project proposes the enhancement of security system for secret data communication through encrypted data embedding in Color images. A given input image is converted to any one plane process. After plane separation, the encrypted data hider will conceal the secret data into the image pixels. The data hiding technique uses the LSB replacement algorithm for concealing the secret message bits into the input image. In the data extraction module, the secret data will be extracted by using relevant key for choosing the image pixels to extract the data. By using the decryption key, the data will be extracted from Input image to get the information about the data. Finally the performance of this proposal in Color Image and encryption data hiding will be analyzed based on image and Encrypted data.

Keywords:-RGB; Encryption, LSB Process; MSE; PSNR

INTRODUCTION:-

Since the rise of the Internet one of the most important factors of information technology and communication has been the security of information. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret.

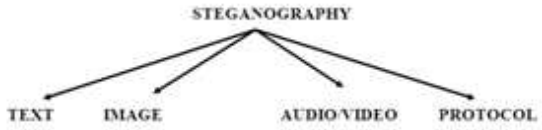


Fig: Different Types STEGANOGRAPHY

Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. It is the art of concealing a message in a cover without leaving a remarkable track on the original message. It Pronounced "ste-g&-'nä-gr&-fE" and Derived from Greek roots "Steganos" = covere "Graphie" = writing its ancient origins can be traced back to 440 BC. In *Histories* the Greek historian Herodotus writes of a nobleman, Hostages, who used steganography first time. The goal of Steganography is to mask the very presence of communication making the true message not discernible to the observer. As steganography has very close to cryptography and its applications, we can with advantage highlight the main differences. Cryptography is about concealing the content of the message. At the same time encrypted data package is itself evidence of the existence of valuable information. Steganography goes a step further and makes the cipher text invisible to unauthorized users. Two other technologies that are closely related to steganography are watermarking and fingerprinting . These technologies are mainly concerned with the protection of intellectual property. but steganography is concern with the hiding of text in information like image, text, audio, and video.

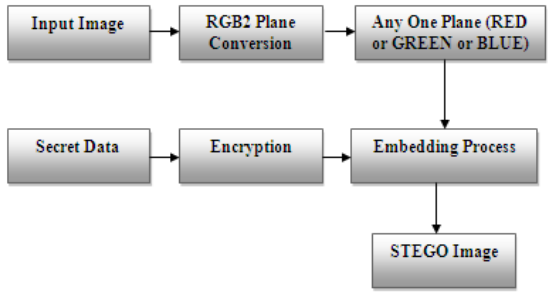


Fig: Block Diagram: Embedding Process

Image:-

An image can be defined as a two-dimensional signal (analog or digital), that contains intensity (grayscale), or color information arranged along an x and y spatial axis. Also it is defined as collection of pixels. Each pixel has a particular color; that color is described by the amount of red, green and blue in it

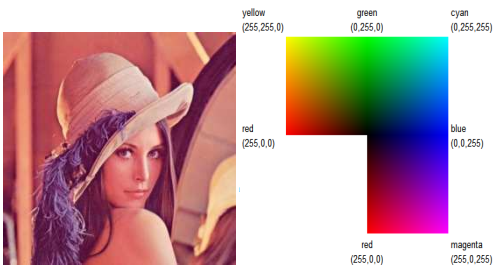


Fig: Input Image of Color Component

If each of these components has a range 0–255, this gives a total of 2563 different possible colors. Such an image is a "stack" of three matrices; representing the red, green and blue values for each pixel. This means that for every pixel there correspond 3 values.

Plane Separation Process:-

High spectral resolution is important when producing color components. For a true color composite an image data used in red, green and blue spectral region must be assigned bits of red, green and blue image processor frame buffer memory.

Fig: Plane Separation Process

A gray scale Image is digital image is an image in which the value of each pixel is a single sample, that is, it carries only intensity information. Images of this sort, also known as black-and-white, are composed exclusively of shades of gray (0-255), varying from black (0) at the weakest intensity to white (255) at the strongest.

Secret Data Encryption Process

With Help of AES Algorithm in Our Secret data we need to convert ASCII Format.

Ex: - **Naresh →[78 65 82 69 84 72]**

Here Arithmetic Encryption Process for each and every data +187

[78 65 82 69 84 72] +**95**= [173 160 177 164 179 167]

And Subtract (-) 17

[173 160 177 164 179 167] – **72**= [101 88 105 92 107 95 36]

In Our Encryption Symbol Based we can get Data for (Encrypted Data)

ENCRYPTED DATA: eXi\j_

Least-Significant Bit (LSB) Technique

8-bit Single Plane image matrix consisting m × n pixels and a secret message consisting of k bits. The first bit of message is embedded into first bit of

first pixel and the second bit of message is embedded into the second bit of first pixel for Reversible Manner of Encrypted data selection. The resultant STEGO-image which holds the secret message is also a 8-bit blue plane image and difference between the cover image and the STEGO-image is not visually perceptible.

PIXEL PROCESSING

After the converting our information in secret code or encrypted form we need to patch that data in the image. We use least significant bit for the patching of data because of following reason.

a. Because the intensity of image is only change by 1 or 0 after hiding the information.

b. Change in intensity is either 0 or 1 because the change at last bit .e.g.

1111100**0**

11111001

The change is only one bit so that the intensity of image is not affected too much and we can easily transfer the data.

181	186	185	181	182
181	185	186	180	181
181	182	186	181	181
177	181	183	180	181
177	182	182	182	180
177	181	183	179	180

[101 88 105 92 107 95]

180	184	184	181	182
180	184	184	181	181
180	183	184	181	181
179	183	183	180	181
179	182	183	180	180
178	182	182	179	180

DATA Hide in Input image

Cover IMAGE Pixel		Secret DATA	
INPUT Samples	Binary Data	Dec Value	Binary Value
64	1000001	89	1011001
68	1000010		
72	1001000		
101	1100101		

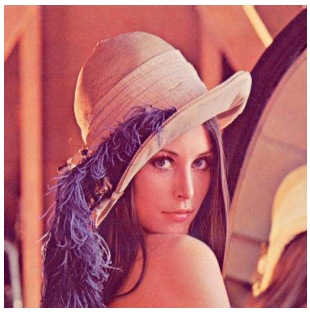
Embedding Process1		
64	10000001	
89	1	
Output	100000	65

Embedding Process2		
68	1000010	
89	10	
Output	1000011	70

Embedding Process3		
72	1001000	
89	11	
Output	10001011	75

Embedding Process4		
101	1100101	
89	10	
Output	10000011	103

Reconstruct for Color Plane:-



The least significant bit (in other words, the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret message. Digital images are mainly of two types (i) 24 bit images and (ii) 8 bit images. In 24 bit images we can embed three bits of information in each pixel, one in each LSB position of the three eight bit values. Increasing or decreasing the value by changing the LSB does not change the appearance of the image; much so the resultant stego image looks almost same as the cover image.

Extraction Process:-

It is important to recognize that payload location only reveals the message bits, not the message itself. In order to obtain the message, we must arrange the located payload in their logical order.

RESULT Analysis:-

Reversible Data Hide in Gray Scale Image

When the database manager gets the data hiding key, he can decrypt the LSB-planes of and extract the additional data by directly reading the decrypted version. When requesting for updating information of encrypted images, the database manager, then, updates information through LSB replacement and encrypts updated information according to the data hiding key all over again. As the whole process is entirely operated on encrypted domain, it avoids the leakage of original content.

On the other hand, there is a different situation that the user wants to decrypt the image first and extracts the data from the decrypted image when it is needed. The following example is an application for such scenario. Assume Alice outsourced her images to a cloud server, and the images are encrypted to protect their contents. Into the encrypted images, the cloud server marks the images by embedding some notation, including the identity of the images' owner, the identity of the cloud server and time stamps, to manage the encrypted images. Note that the cloud server has no right to do any permanent damage to the images.

Reversible Data Hide in Color Image

The primary reason why payload location fails to establish this order is due to the fact that it assumes each STEGO image carries a fixed payload of size m. By relaxing this constraint so that the size of each payload can vary between 1 and m, we show that the mean residuals contain enough information to logically order the located payload to obtain the hidden messages. The next two sub-sections establish this fundamental result for simple LSB steganography and group-parity steganography, respectively.

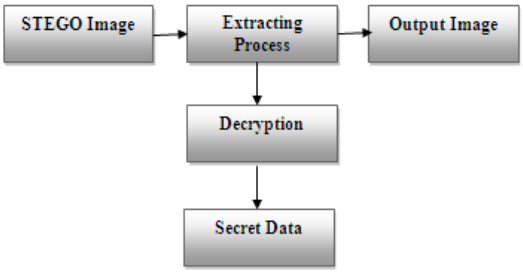


Fig: Block Diagram: Extracting Process

Receiver Decrypt Text: - Naresh

Advantages:-

a. This algorithm use random size of key.

b. Because of this random size the middle person can't predict the size of key and data.

c. The number of times execution of loop is not fixed so that more secure algorithm.

d. This is more secure and easy to implement.

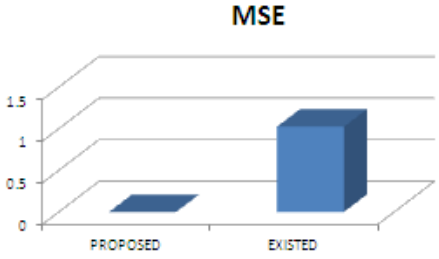
Fig: Result for Data Hide inn Color Image

Quality Measurement:-

The Quality of the reconstructed image is measured in-terms of mean square error (MSE) and peak signal to noise ratio (PSNR) ratio. The MSE is often called reconstruction error variance σ_q^2. The MSE between the original image f and the reconstructed image g at decoder is defined as:

$$\mathbf{MSE} = \frac{1}{MXN} \sum_{j,k} (f[j,k] - g[j,k])$$

	MSE
PROPOSED	0.000038
EXISTED	1.0229

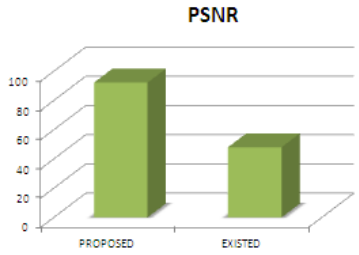


Where the sum over j, k denotes the sum over all pixels in the image and N is the number of pixels in each image. From that the peak signal-to-noise ratio is defined as the ratio between signal variance and reconstruction error variance. The PSNR between two images having 8 bits per pixel in terms of decibels (dB) is given by:

$$\mathbf{PSNR} = \mathbf{10\ log_{10}} \left(\frac{255^2}{MSE} \right)$$

Generally when PSNR is 20 dB or greater, then the original and the reconstructed images are virtually in-distinguishable by human eyes.

	PSNR
PROPOSED	92.2355
EXISTED	48.0325



Conclusion:-

In this research, I presented an efficient technique for hiding data in an image for Color Component The basic idea of our technique is to hide data in an image file and that image which contains data is hided in to an image. From the experimental results, it is found that the hidden secret data creates minimal changes in the cover media and without altering its quality. Moreover, the secret data itself is successfully hidden and extracted with no distortion.

Future Scope:-

In future work, this process can extends to video files by embedding encrypt data in to video files (any one input frame). So the secrecy is increase. This is mainly used in military applications and defence applications.

REFERENCES:-

[1]. *Siva Janakiraman , Pixel Bit Manipulation for Encoded Hiding -An Inherent stego,2012 IEEE,978-1-4577.*

[2]. Bruice Schneier, Applied Cryptography Protocols, Algorithm and Source Code in C. 2nd ed. Wiley India edition, 2007.

[3]. C.K. Chan, L.M. Chen, Hiding data in images by simple LSB substitution, Pattern Recognition. 37 (3) (2004) 469–474.

[4]. Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt Digital Image Steganography:Survey and Analysis of Current Methods.

[5]. Hiding data in images by simple LSB substitutionChi-Kwong Chan∗, L.M. Cheng Department of Computer Engineering and Information Technology, City University of Hong Kong, Hong Kong Received 17 May 2002; received in revised form 11 July 2003; accepted 11 August 2003.

[6]. Information Hiding Using Least Significant Bit Steganography and Cryptography Shailender Gupta Department of Electrical & Electronics Engineering, YMCAUST,

[7] Marvel, L., M., Boncelet Jr., C.G. & Retter, C.,"Spread Spectrum Steganography", IEEE Transactions on Image Processing, 1999.

[8] Waugh & Wang, S,"Cyber Warfare: Steganography vs. Steganalysis", Communications of the ACM, 47:10, October 2004.

[9] Stefan Katznbeisser, Fabien. A., P.Petitcolas editors, Information Hiding Techniques for Steganography and Digital Watermarking,Artech House, Boston.London,2000.

[10] Jamil,T., "Steganography: The art of Hiding Information is Plain Sight", IEEE Potentials,18:01,1999.

[11] B.Pfitzmann ,"Information Hiding Terminology," proc.First Int'l Workshop Information Hiding, Lecturer Notes in Computer Science No.1,174,Spring – Verlag,Berlin,1996,pp.347-356.

[12] Yean- Kuhn Lea and Ling-Hew Cheng,"High capacity steganographic model" ,IEEE Proc.Visual Image Signal Process.,Vol.147,No.3,June 2000.

[13] Ross J.Anderson, Fabien A.P.Petitcols, on The limits of steganography, IEEE Journal of Selected Areas in Communication, 16(4);474-481,May 1998.

[14] M.Ashourian, R.C. Mainland Y.H.Ho, Dithered Quantization for Image Data Hiding In DCT domain, Proc.of IST2003, 2003, 171-175.

[15] C.C.lin, P.F.Shiu, High Capacity Data hiding scheme for DCT-based images. Journal of Information Hiding and Multimedia Signal Processing,1(3),2010,314-323.