International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2020 IJSRCSEIT | Volume 6 | Issue 2 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/IJSRCSEIT

Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption

Dr. K.V.V Kumar[1], K. Lavanya[2], P. Maria Kumar[2], M. Katyayani[2], T. Vinay Kumar[2], T. A. Rawindra Reddy[2]

[1]Associate.Professor, Department of ECE, Universal College of Engineering and Technology, Dokiparru, Guntur (DT), Andhra Pradesh, India.

[2]B. Tech Students, Department of ECE, Universal College of Engineering and Technology, Dokiparru, Guntur (DT), Andhra Pradesh, India

ABSTRACT

(RDH) in encrypted images, since it maintains the excellent property that the original cover can be loss less recovered after embedded data is extracted while protecting the image content's confidentiality. All previous methods embed data by reversibly vacating room. Recently, more and more attention is paid to reversible data hiding from the encrypted images, which may be subject to some errors on data extraction and/or image restoration. In this report, we propose a novel method by reserving room before encryption with a traditional RDH algorithm, and thus it is easy for the data hider to reversibly embed data in the encrypted image. The proposed method can achieve real reversibility, that is, data extraction and image recovery are free of any error. Experiments show that this novel method can embed more than 10 times as large payloads for the same image quality as the previous methods, such as for PSNR dB.

Keywords : - Image Encryption, Image Recovery, Reversible Data Hiding.

I. INTRODUCTION

1.1.1 Image

An image (from Latin: imago) is an artifact that depicts or records visual perception, for example a picture, that has a similar appearance to some subject usually a physical object or a person, thus providing a depiction of it. Image is a two-dimensional, such as a photograph, screen display, and as well as a three-dimensional, such as a statue. They may be captured by optical devices such as cameras, mirrors, lenses, telescopes, microscopes, etc. and natural objects and phenomena, such as the human eye or water surfaces. The word image is also used in the broader sense of any two-dimensional figure such as a map, a graph, a pie chart, or an abstract painting. In this wider sense, images can also be rendered manually, such as by drawing, painting, carving, rendered automatically by printing or computer graphics technology, or developed by a combination of methods, especially in a pseudo-photograph.

An image is a rectangular grid of pixels. It has a definite height and a definite width counted in pixels. Each pixel is square and has a fixed size on a given display. However different computer monitors may use different sized pixels. The pixels that constitute an image are ordered as a grid (columns and row s) each pixel consists of numbers representing magnitudes of brightness and color.

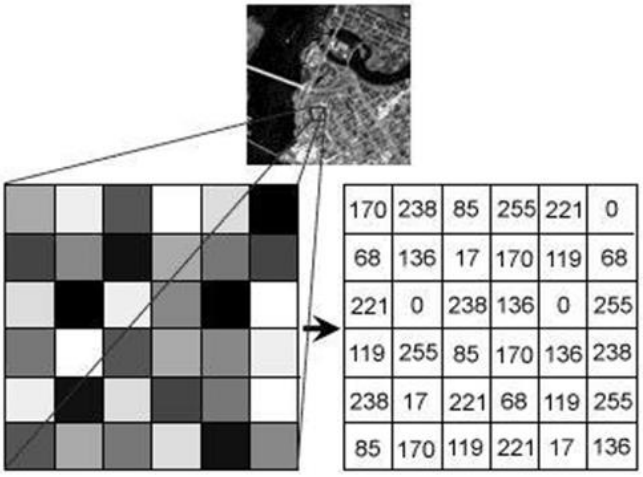

Figure 1. Image represented as rectangular grid pf pixels

Each pixel has a color. The color is a 32-bit in teger. The first eight bits determine the redness of the pixel, the next eight bits the greenness, the next eight bits the blueness, and the remaining eight bits the transparency of the pixel.

1.1.2 Image File Sizes:

Image file size is expressed as the number of bytes that increases with the number of pixels composing an image, adepth of the pixels. The greater the number of rows and columns, the greater will be the image resolution, and the larger the file. Also, each pixel of an image increases in size when its color depth increases, an 8-bit pixel (1 byte) stores 256 colors, a 24-bit pixel (3 bytes) stores 16 million colors, the latter known as true color.

II. METHODOLOGY

EXSISTING METHOD:

CRYPTOGRAPHY:

The earliest forms of information hiding can actually be considered to be highly crude forms of private-key cryptography; the "key" in this case being the knowledge of the method being employed (security through obscurity). Steganography books are filled with examples of such methods used throughout history. Greek messengers had messages tattooed into their shave head, concealing the message when their hair finally grew back. Wax tables were scraped down to bare wood were a message was scratched. Once the tablets were re-waxed, the hidden message was secure. Over time these primitive cryptographic techniques improved, increasing both speed and capacity and security of the transmitted message. Today, crypto-graphical techniques have reached a level of sophistication such that properly encrypted communications can be assumed secure well beyond the useful life of the information transmitted. Of course the possibility exists that vulnerabilities could be found, or computing power breakthroughs could occur, but for most users in most applications, current cryptographic techniques are generally sufficient. Several good reasons exist, the first being that "security through obscurity" isn't necessarily a bad thing, provided that it is not the only security mechanism employed. Steganography for instance allows us to hide encrypted messages in mediums less likely to attract attention. A garble of random characters being transmitted between two users may tip off a watchful third party that sensitive information is being transmitted; whereas baby pictures with some additional noise present may not. The underlying information in the pictures is still encrypted, but attracts far less attention being distributed in the picture then it would otherwise. This becomes particularly important as the technological disparity between individuals and organizations grows. Governments and businesses typically have access to more powerful systems and better encryption algorithms then individuals. Hence, the chance of individual's messages being broken increases which each passing year. Reducing the number of messages intercepted by the organizations as suspect will certainly help to improve privacy.

Cryptographic techniques generally rely on the metaphor of a piece of information being placed in a secure "box" and locked with a "key". The information

itself is not disturbed and anyone with the proper key can gain access. Once the box is open, all of the information security is lost. Compare this to information hiding techniques where the key is embedded into the information itself. Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient. While cryptography is the science of securing data, cryptanalysis is the science of analyzing and breaking secure communication. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern hiding, patience, determination, and luck. Crypt analysts are also called attackers. Cryptology embraces both cryptography and cryptanalysis. Cryptography can be defined as the processing of information into an unintelligible (encrypted) form for the purposes of secure transmission. Through the use of a “key” the receiver can decode the encrypted message (decrypting) to retrieve the original message. Stenography improves on this by hiding the fact that a communication even occurred. The message m is imbedded into a harmless message c which is defined as the cover object. The message m is then embedded into c, generally with use of a key k that is defined as the stego-key. The resulting message is then embedded into the cover-object c, which results in stego-objects.

III. PROPOSED METHOD

Steganography

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. The word Steganography is of Greek origin and means "concealed writing" from the Greek words steganos meaning "covered or protected", and graphed meaning "writing" or simply Steganography means to hide secret information into innocent data or “Steganography is the art of hiding information in ways that prevent the detection of hidden messages”. Generally, messages will appear to be something else: images, articles, shopping lists, or some other cover text and, classically, the hidden message may be in invisible ink between the visible lines of a private letter. An image containing a secret message is called a cover image. Digital images are ideal for hiding secret information. First, the difference of the cover image and the stego image should be visually unnoticeable. The embedding itself should draw no extra attention to the stego image so that no hackers would try to extract the hidden message illegally. Second, the message hiding method should be reliable. It is impossible for someone to extract the hidden message if she/he does not have a special extracting method and a proper secret key. Third, the maximum length of the secret message that can be hidden should be as long as possible. The advantage of Steganography over cryptography alone is that messages do not attract attention to themselves. Plainly visible encrypted messages no matter how unbreakable will arouse suspicion, and may in themselves be incriminating in countries where encryption is illegal. Therefore, whereas cryptography protects the contents of a message, Steganography can be said to protect both messages and communicating parties. Steganography includes the concealment of information within computer files. In digital Steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size. As a simple example, a sender might start with an innocuous image file and adjust the color of every 100th pixel to correspond to a letter in the alphabet, a change so subtle that someone not specifically looking for it is unlikely to notice it. Hide Secret Files is the ultimate tool allowing you to have exclusive secured

access to sensitive information based on a password. No one except you, who know the password, will be able to access the secured data. Not even your own operating system will have permission to alter the information. The latest, and one of the most annoying secondary products of the Internet evolution, is the spy-ware activity, and thankfully it is absolutely inoffensive against the protection guaranteed by Hide Secret Files. The hidden data won't be visible even for your own OS so the Safe Mode booting or moving the hard drive in another PC won't make it possible to reveal, the data protected by Hide Secret Files. For this to work you will need Win-RAR installed on your computer and Microsoft Windows with access to the command prompt. If you do not have Win-RAR installed on your computer you can find a link to download this program through our recommended download section. 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.

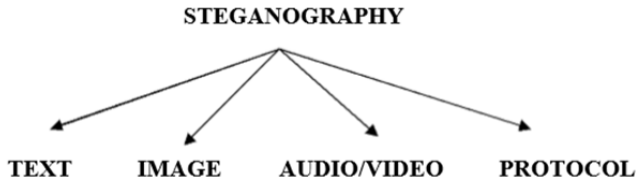

Figure 2. Different types of Steganography

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.

Text

While information can be hidden inside texts in such a way that the presence of the message can only be detected with knowledge of the secret key, for example when using the earlier mentioned method using a publicly available book and a combination of character positions to hide the message, most of the techniques involve alterations to the cover source. These modifications can be detected by looking for patterns in text or disturbing thereof, odd use of language and unusual amounts of whitespace.

Steganography in the Digital images

Steganography is the art of secret communication. Its purpose is to hide the very presence of communication as opposed to cryptography whose goal is to make communication unintelligible to those who do not possess the right keys. Digital images, videos, sound files, and other computer files that contain perceptually irrelevant or redundant information can be used as "covers" or carriers to hide secret messages. After embedding a secret message into the cover-image, a so-called stego-image is obtained. It is important that the stego-image does not contain any easily detectable artifacts due to message embedding. A third party could use such artifacts as an indication that a secret message is present. Once this message detection can be reliably achieved, the steganographic tool becomes useless. Obviously, the less information is embedded into the cover-image, the smaller the

probability of introducing detectable artifacts by the embedding process. Another important factor is the choice of the cover-image. The selection is at the discretion of the person who sends the message. The sender should avoid using cover-images that would be easy to analyze for presence of secret messages. For example, one should not use computer art, charts, images with large areas of uniform color, images with only a few colors, and images with a unique semantic content, such as fonts.

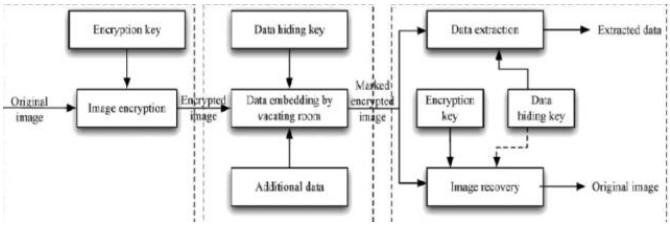

Figure 3. Block Diagram

$$O_i = \left[\sum_{j=0}^{i} N_j \right] \times \frac{\text{Max. Intensity Level}}{\text{No. of Pixels}}$$

The meaning of Max. Intensity Levels maximum intensity level which a pixel can get. For example, if the image is in the grayscale domain, then the count is 255. And if the image is of size 256x256 then, the No. of pixels is 65536. And the expression is the bracket means that the no. of pixels having the intensity below the output intensity level or equal to it. For example, if we are calculating the output intensity level for 1 input intensity level, then that means that the no. of pixels in the image having the intensity below or equal to 1 means 0 and 1. If we are calculating the output intensity level for 5 input intensity level, then the it means that the no. of pixels in the image having the intensity below or equal to 5 means 0 , 1 , 2 , 3 , 4 , 5. Thus, if we are calculating the output intensity level for 255 input intensity level, then the it means that the no. of pixels in the image having the intensity below or equal to 255 means 0 , 1 , 2 , 3 , ... , 255. That is how new intensity levels are calculated for the previous intensity levels. The next step is to replace the previous intensity level with the new intensity level. This is accomplished by putting the value of Oi in the image for all the pixels, where Oi represents the new intensity value, whereas i represent the previous intensity level.

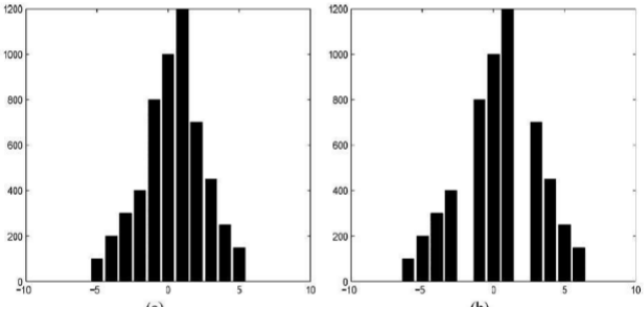

Figure 4. Selection of proper points (a) Original histogram, (b) shifted histogram. (In this figure, length of messages is 1000 bits)

The gray-scale histogram of an image represents the distribution of the pixels in the image over the gray-level scale. It can be visualized as if each pixel is placed in a bin corresponding to the color intensity of that pixel. All of the pixels in each bin are then added up and displayed on a graph. This graph is the histogram of the image. The histogram is a key tool in image processing. It is one of the most useful techniques in gathering information about an image. It is especially useful in viewing the contrast of an image. If the gray-levels are concentrated near a certain level the image is low contrast. Likewise if they are well spread out, it defines a high contrast image.

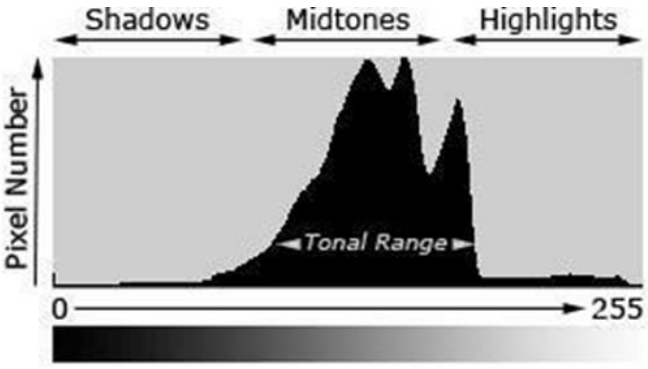

Figure 5. Sample histogram

Contrast Stretching

Contrast stretching enables the spacing of some of the output values so that they are further apart, thereby making them more easily distinguishable. This can be done manually by choosing the upper and lower bound of the histogram and adjusting the graph to fit. It can also be done automatically by implementing the histogram-equalized stretch. Histogram Equalized Stretch This stretch assigns more display values to the frequently occurring portions of the histogram. In this way, the detail in these areas will be better enhanced relative to those areas of the original histogram where values occur less frequently. The aim is to maximize the overall contrast as shown below ; a nearly uniform (i.e. flat) distribution is produced.

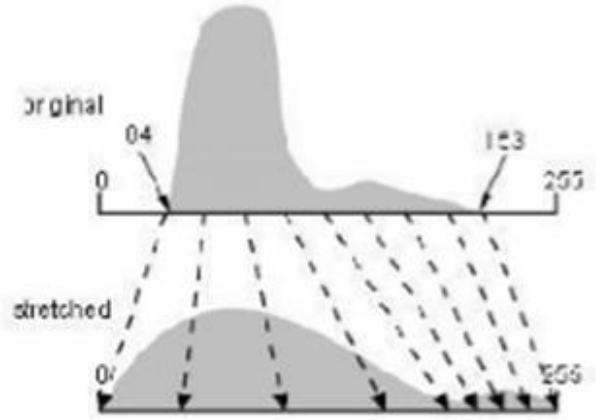

Figure 6. Histogram Equalization

After an image has been equalized the feature s become much more defined and easier to identify for the viewer

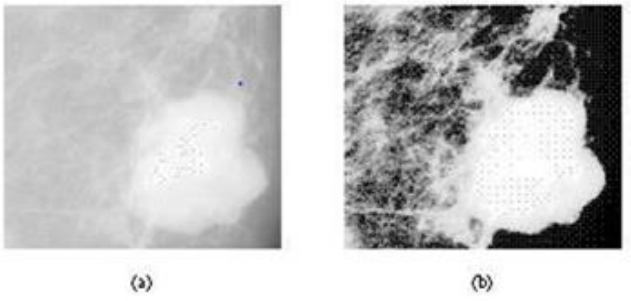

Figure 7. Image before and after equalisation

Arithmetic Encryption Process

Encryption is the standard method for making a communication private. Anyone wanting to send a private message to another user encrypts (enciphers) the message before transmitting it. Only the intended recipient knows how to correctly decrypt (decipher) the message. Anyone who was "eavesdropping" on the communication would only see the encrypted message. Because they would not know how to decrypt it successfully, the message would make no sense to them. As such, privacy can be ensured in electronic communication.

1.Plaintext (Clear text)

The intelligible message which will be converted into an unintelligible (encrypted) message

2. Cipher text

A message in encrypted form

3. Encryption

The process of converting a plaintext message into a cipher text message

4. Decryption

The process of converting a cipher text message into a plaintext message. 5. Cryptosystem A system to encrypt and decrypt information.

5. Cryptosystem

A system to encrypt and decrypt information

6. Symmetric Cryptosystem

A cryptosystem that uses the same key to encrypt and decrypt information.

7. Asymmetric Cryptosystem

A cryptosystem that uses one key to encrypt and a different key to decrypt.

Secret Data Encryption Process

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

Format. For example: 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] Based on this we can get Data for (Encrypted Data) as eXi\j_

Least Significant Bit (LSB) Substitution

The principle involved in this method is to replace all LSB bits of pixels of the cover image with secret bits. This method embeds the fixed-length secret bits in the same fixed length LSBs of pixels.

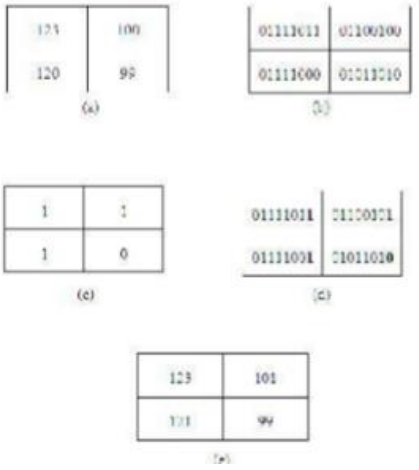

Fig: 7 LSB Substitution (a) Image having size 2*2, (b) Binary format of image (a), (c) Binary secret data, (d) LSB substitution-embedding (c) into (b), (e) Final image after substitution

Although this technique is simple, it generally causes noticeable distortion when the number of embedded bits for each pixel exceeds three.

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. For example let us consider this 8-bit 11111000. It is converted to 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.

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

Figure 8. Change in pixel values

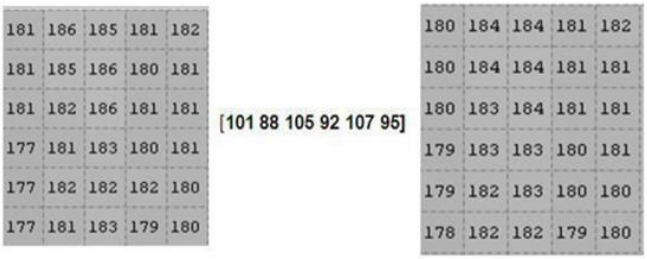

Figure 9. Data Hidden in Input Image

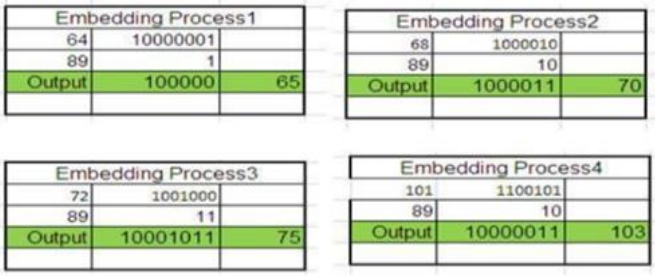

Fig: 10 Change in pixels due to embedding

Advantages of LSB Insertion

A major advantage of the LSB algorithm is it is quick and easy. There has also been steganography software developed which work around LSB color alterations via palette manipulation. LSB insertion also works well with single-scale imagess

IV. RESULTS

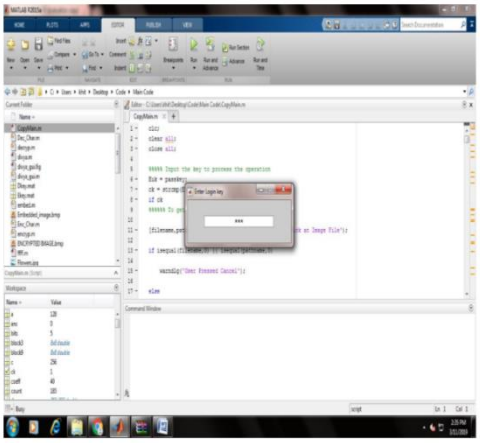

Fig: 11 After clicking the run button

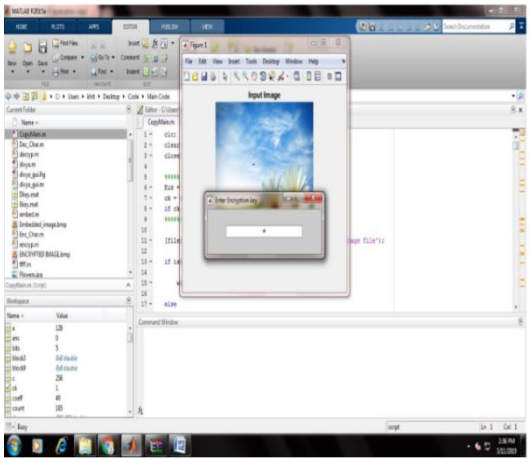

Fig: 12 Giving an Input Image and encryption key

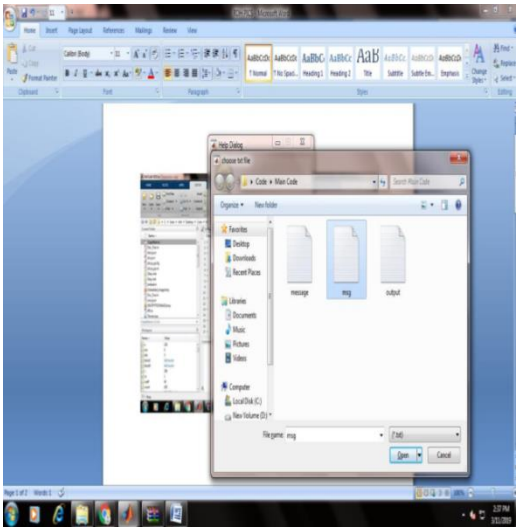

Fig:13 .Giving message

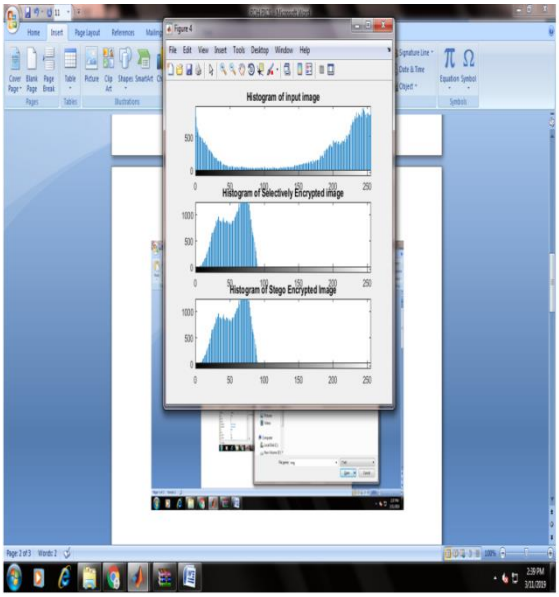

Fig:14.Histogram representation

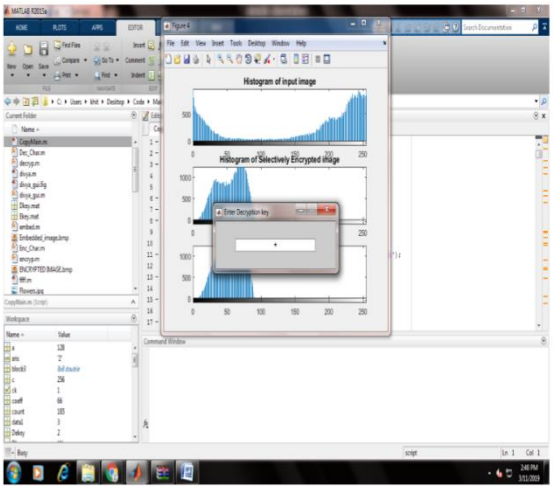

Fig: 15. Decryption key

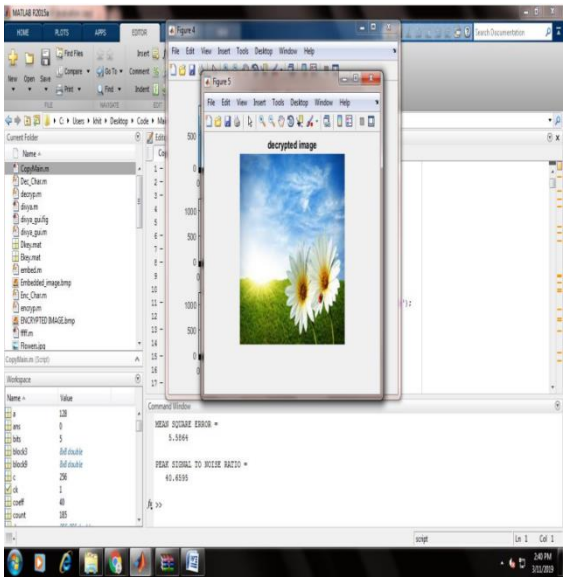

Fig: 16. Resulted Decrypted image

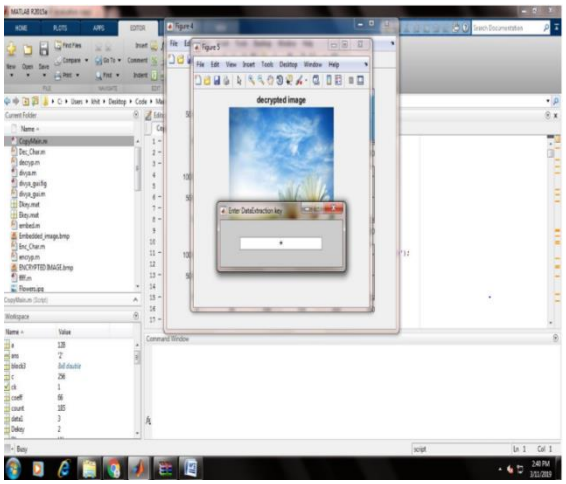

Fig: 17. Giving Data extraction key

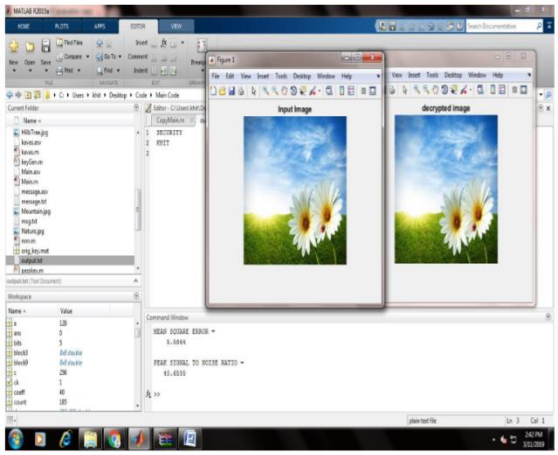

Fig: 18 resulted output image and PSNR

V. ADVANTAGES AND APPLICATIONS

5.1. Advantages

- This method can achieve real reversibility, that is, data extraction and image recovery are free of any error.
- It is easy for the data hider to reversibly embed data in the encrypted image.
- This method can embed more than 10 times as large payloads for the same image quality as the previous methods

5.2. Applications

- Secret Data Communication in Defense.
- Research institute.
- Medical information protection.

VI. CONCLUSION

Reversible data hiding in encrypted images is a new topic drawing attention because of the privacy-preserving requirements from cloud data management. Previous methods implement RDH in encrypted images by vacating room after encryption, as opposed to which we proposed by reserving room before encryption. Thus the data hider can benefit from the extra space emptied out in previous stage to make data hiding process effortless. The proposed method can take advantage of all traditional RDH techniques for plain images and achieve excellent performance without loss of perfect secrecy.

VII. 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 increased. This is mainly used in military applications and defence applications.

VIII. 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 substitution Chi-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, MCAUST.

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

[8]. Waugh & Wang, S,"Cyber Warfare: Steganography vs Stegoanalysis", Communications of the AC M, 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.

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

AUTHORS BIBLOGRAPH

K. V. V. Kumar born in India 1987. Obtained his B.Tech, from VRS&YRN College of Engineering and Technology Chirala. During 2007-2010. & M.Tech from K.L University in the Specialization of Communication and Radar systems during 2010-2012.He is having More than 7 years teaching experience and having 8 international and national journals / Conference papers Like IEEE and SPRINGER. He is Associate member of I.E.T.E and ISSE other bodies Like I.S.T.E. His research interested areas includes Image processing and Signal Processing. and Video Processing.

K.LAVANYA obtained her B.Tech from Universal College of Engineering And Technology, Dokiparru, Guntur Dt, AP in Electronics and Communication Engineering Stream.

P.MARIA KUMAR obtained him B.Tech from Universal College of Engineering And Technology, Dokiparru, Guntur Dt, AP in Electronics and Communication Engineering stream.

M.KATYAYANI obtained her B.Tech from, Universal College of Engineering And Technology, Dokiparru, Guntur Dt, AP in Electronics and Communication Engineering stream.

T.VINAY KUMAR obtained him B.Tech from Universal College of Engineering And Technology,

Cite this article as :

Dr. K.V.V Kumar, K. Lavanya, P. Maria Kumar, M. Katyayani, T. Vinay Kumar, T. A.Rawindra Reddy, "Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 6 Issue 2, pp. 100-110, March-April 2020.
Journal URL : http://ijsrcseit.com/CSEIT206220