An Improved Reversible Data Hiding in Ciphered Images by using CHAOS Encryption

K C V RAGHAVACHARYULU[1],K RAMADEVI[2]

***Abstract*—Image encryption using chaotic function has been gaining popularity in recent years even though several methods for image encryption utilizing chaotic method emerging. This paper presents a new chaos based image encryption method which is based on series of confusion and diffusion processes guided by a user key based encryption and decryption. The proposed method generates large key space which results in bruit force attack. However, the extraction process has an additional method in comparison with general data hiding scheme. After the embedded secret data is extracted, the cover image can be completely restored to its original state. Extraction of data and image recovery can be achieved without any errors by using the proposed method explaining the flexible reversibility of the method.Based on the results, our method can embed the data and image in best quality and it can be calculated with the help of PSNR. Through Statistical analysis, it is confirmed that the proposed method is highly secure and is suitable for image encryption.**

***Index Terms*--Chaos algorithm, decryption,**

encryption,PSNR, reversible data hiding.

I. 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[2] 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 as secret. Steganography (Fig.1) is the method of hiding the information about the communication that occurs by hiding information in other information. It is the art of concealing a message in a shield without leaving a notable track on the original message. It can be pronounced as "ste-g&-'nä-gr&-fe" and derived from Greek words, "Steganos" means "covere" and "Graphie" means writing. Steganography is ancient art and its origins can be located back to 440 BC. The Greek historian Herodotus writes of a nobleman, Hostages, who had used steganography for the first time in history.

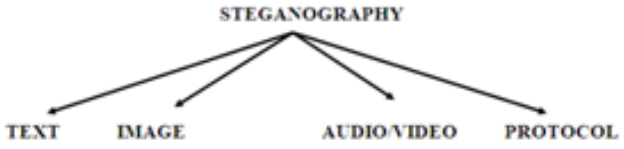


Fig. 1 Types of STEGANOGRAPHY

The goal of Steganography is to conceal the whole segments of communication making the true message not detectable to the observer. Although Steganography resembles Cryptography and its applications in some aspects, many principal differences exist. Cryptography[2] is about disguising the whole sections of the message whereas the encrypted data package is itself evidence of the existence of valuable information. Steganography[3][8] acts in advance and makes the encrypted text invisible to illegitimate users. Watermarking and finger printing are two other technologies that are closely related to Steganography; both of them are associated with safeguarding of intellectual property. But Steganography is associated with hiding of text in the form of information such as image, text, audio, and video. In the present paper, we propose a novel method for RDH in encrypted images, for which we do not "vacate room after encryption", but "reserve room before encryption". In the proposed method, we first empty out room by embedding LSBs of some pixels into other pixels with a traditional RDH method and then encrypt the image, so the positions of these LSBs in the encrypted image can be used to embed data.

II. EMBEDDING PROCESS

While displaying the different bands of a multispectral data set, images obtained in different bands are displayed in image planes (other than their own) the color composite is regarded as False Colour Composite (FCC). 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.Input image is converted into RED OR GREEN OR BLUE plane by RGB2 plane conversion. The encrypted secret data is embedded in any one of the plane to get the resultant image. The resultant image is nothing but stegno image

ISSN: 2278 – 7798

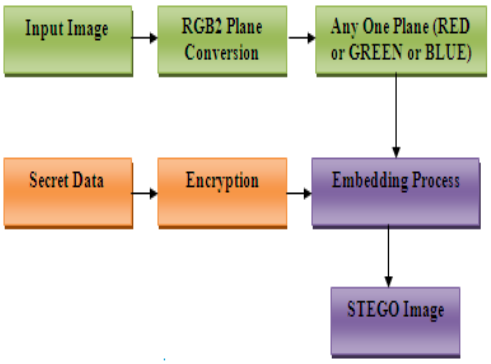
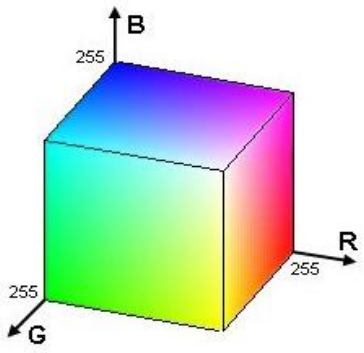


Fig. 2 Block Diagram: Embedding Process

A. Image

An image(ex. Lena Fig.3(a)) can be defined as a two-dimensional signal (analog or digital), that contains intensity (gray scale), or color information arranged along an x and y spatial axis[1].An image is also a collection of pixels, and each pixel has a particular color; that color is described by the amount of red, green and blue in it.

(a)



(b)

Fig. 3 Input Image of Color Component

If each of these components has a range 0–255(fig .3(b)), 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 implies that every pixel corresponds to 3 values.

B. Plane Separation Process

It is essential to have high spectral resolution for color component production. In case of a true color composite, bits of red (Fig.4(a)), green (Fig.4(b)) and blue (Fig.4(c)) frame image processor buffer memory would be allocated for an image data from red, green and blue spectral region.

(a)

(b) **(c)**

Fig. 4 Plane Separation Process

A gray scale 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.

C. Secret Data Process

With the help of chaos algorithm[5] our secret data would be converted to ASCII Format.

Eg.:**RAGAVA**

Encrypted data: @#*&$

III. PROPOSED METHOD

A. Chaos Technique

Chaos [5] is a symmetric key algorithm which is used for both encryption and decryption as the data stream is simply XOR'ed with the generated key sequence(Fig.5). The key stream is completely independent of the plaintext used. It uses a variable length key from 1 to 256 bit to initialize a 256-bit state table.

ISSN: 2278 – 7798

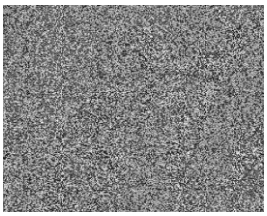


Fig. 5 Chaos encrypted image

The state table is used for generation of pseudo-random bits and then subsequently generates a pseudo-random stream which is XOR'ed[5][8] with the plaintext to give the cipher text shown in Fig.6.

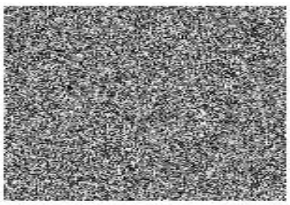


Fig. 6 Secret Data Hide in Chaos encrypted Image

B. Pixel processing

The matrix of a gray scale image of 8 bit consists of m × n pixels and a hidden message consisting of k bits[1].The first bit of message is embedded into the LSB of the first pixel of first bit and the second bit of message is embedded into the first pixel of second bit for Reversible Manner of secret data selection. The Stego-image generated that holds encrypted message also of 8-bit and difference between the cover image and the above is not visually detectable.

C. 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 of encrypted images, the cloud server scores the images by embedding into some notation, including the identity of the owner of the image, cloud server and time stamps, to handle the encrypted images[8][10]. In STEGNO image, the data and image are extracted by decryption process shown in Fig.7.

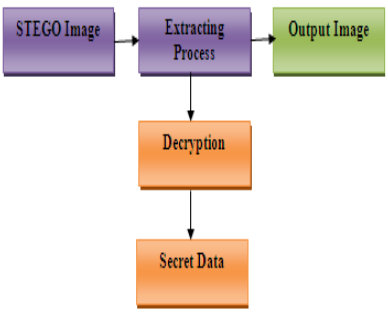


Fig. 7 Block Diagram: Extracting Process

Fig. 8 Image recovery

It is important to note that the cloud server cannot accomplish any persistent damage to the images.

D. Reversible Data Hide in 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[3]. By relaxing this constraint the size of each payload can vary between 1 and m. In such case, we showed that the mean residuals possess sufficient information to logically order the established payload[9] to recover the encrypted messages. The next two sub-sections establish this fundamental result for simple Steganography [4][5]and group parity steganography, respectively.

E. 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 also called reconstruction error variance σ_q^2. The MSE [3] between the original image f and the reconstructed image g at decoder equation given by

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

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[6]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:

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

The original and the reconstructed images are virtually identical to human eyes when PSNR is 20 dB or greater.

IV. Simulation Results

The data hiding key can be used to decrypt the chaos-planes and additional data would be extracted by directly reading the decrypted version. The information over encrypted images can be updated after replacing of Chaos and again encrypts the resulted updated information

ISSN: 2278 – 7798

according to the data hiding key. The whole process is leakage proof as it is entirely conducted on encrypted domain. Another case would be if 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. For e.g. Alice outsourced her images to a cloud server, images are encrypted into the mean square error and Peak signal to noise ratio that determines the image quality and also protects their contents.Fig.9 to Fig.14 are the steps of encryption and decryption process of chaos encryption. Table I and Table II are Tabular forms for Advanced Encryption Standard(AES) and CHAOS Encryption for different embedding rates.In Fig.15 is comparison between AES and CHAOS Encryption for different Embedding rates.when input image is converted in to chaos encrypted image , then secret data is places in the image resulting stegno image .Similarly in extraction process the image and secret data is obtained seperatley.

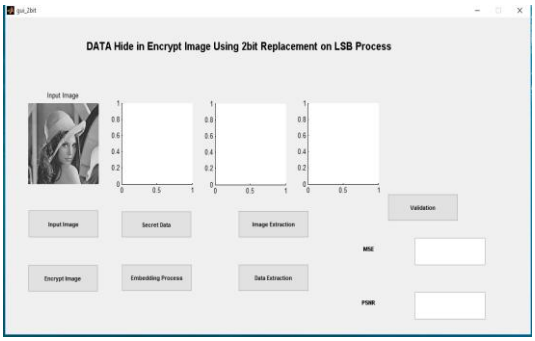


Fig. 9 Initial process by taking Lena image

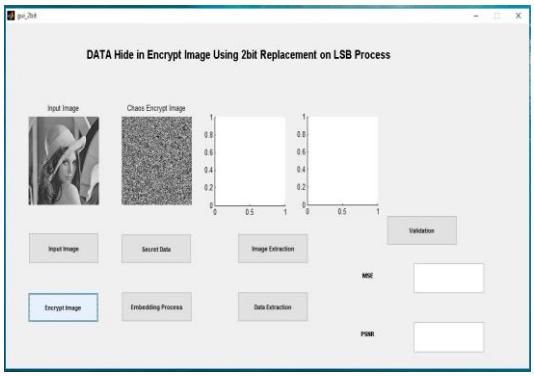


Fig. 10 Chaos Encrypted Image

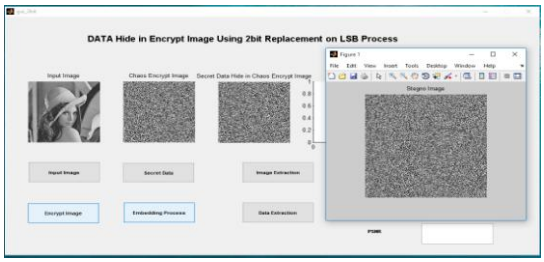


Fig. 11 Secret Data in Chaos Encrypted Image

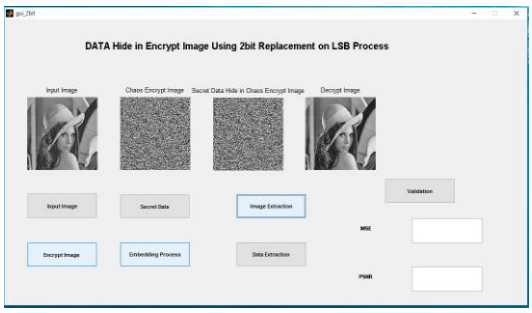


Fig. 12 Decrypted Lena Image

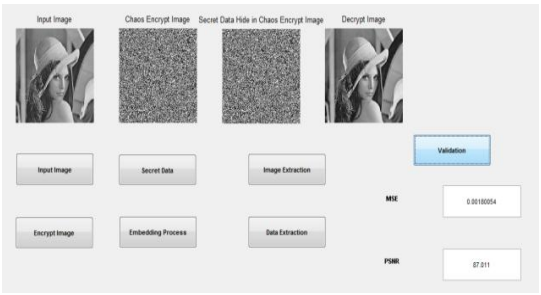


Fig. 13 MSE& PSNR Values of Lena Image

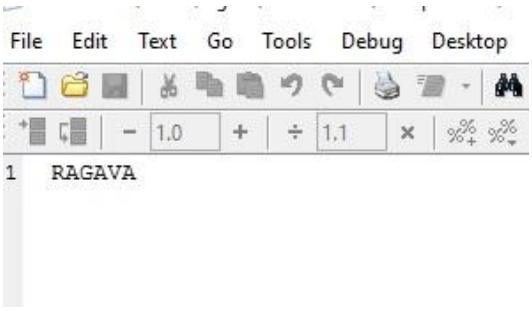


Fig. 14 Secret Data

Table I PSNR(dB) values of AES Encryption

Input	0.05	0.1	0.2	0.3	0.4	0.5
Lena	54.72	52.56	48.79	46.52	42.68	39.04
Flower	57.08	54.30	51.98	49.20	48.67	40.78
Hills	57.70	54.78	51.56	49.26	48.56	42.78
Mountain	54.78	51.45	46.26	44.56	41.23	32.80
Nature	56.87	53.63	50.36	43.69	40.76	31.69

Table II PSNR(dB) values of CHAOS Encryption

Input	0.05	0.1	0.2	0.3	0.4	0.5
Lena	65.72	61.56	57.79	53.52	52.68	47.04
Flower	68.08	64.07	61.98	58.20	55.97	51.78
Hills	65.70	62.68	60.56	59.26	54.86	49.18
Mountain	62.89	60.75	57.96	54.26	53.56	49.80
Nature	64.97	62.25	61.69	59.53	57.16	45.69

ISSN: 2278 – 7798

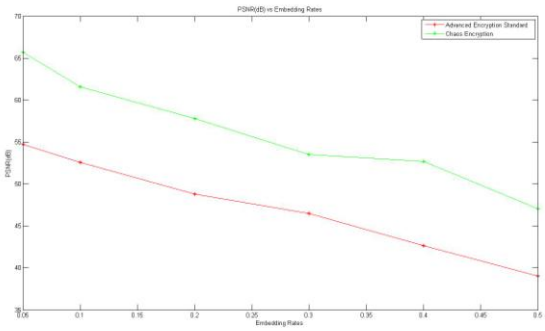


Fig. 15 Comparision of PSNR and Embedding Rates for Lena image

Advantages

a. The size of key used by this algorithm is random.
b. The size of the key and data cannot be predicted by other illegitimate or sub user as the size is random.
c. The number of times the loop has to be executed is non-static thus more secures the algorithm.
d. This algorithm is easy to implement.

V.Conclusions

From the experimental results, it was found that the hidden secret knowledge creates token changes within the media while not compromising its quality. Moreover, the key of this knowledge itself is that it is successfully hidden and extracted without distortion. Presently the chaos-based scheme was designed for stagnant images. The chaos-based image encryption method can be applied to moving in the society has promoted digital images and videos images as well. The prevalence of multimedia technology to play a more significant role than the traditional texts, which demands a serious protection of users' privacy. To fulfill such security and privacy needs in various applications, encryption of images and videos is very important to frustrate malicious attacks from unauthorized parties.

REFERENCES

[1] S.Janakiraman, "Pixel Bit Manipulation for Encoded Hiding-An Inherentstego,"*IEEE*, vol. 978, pp.351-457, 2012.

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

[3] W.Zhang, B. Chen, and N. Yu, "Capacity-approaching codes for reversible data hiding," Proc 13th Information Hiding(IH'2011),LNCS, vol. 6958, pp. 255–269, Springer-Verlag, 2011.

[4] A.Cheddad, J. Condell, K. Curran and P. Mc. Kevitt"Digital Image Steganography:Survey and Analysis of Current Methods,"

[5] W.Zhang, B. Chen, and N. Yu, "Improving various reversible datahiding schemes via optimal codes for binary covers," *IEEE Trans.Image Process.*, vol. 21, no. 6, pp. 2991–3003, Jun. 2012.

[6] Z. Ni, Y.Shi, N. Ansari, and S. Wei, "Reversible data hiding," IEEE *Trans.Circuits Syst. Video Technol.*, vol. 16, no. 3, pp. 354–362, Mar.2006.

[7] P.Tsai, Y. C. Hu, and H. L. Yeh, "Reversible image hiding scheme using predictive coding and histogram shifting," Signal Process., vol. 89, pp. 1129–1143, 2009.

[8] W. Liu, W. Zeng, L. Dong, and Q. Yao, "Efficient compression of encrypted grayscale images," IEEE Trans. Image Process., vol. 19, no. 4, pp. 1097–1102, Apr. 2010.

[9] X.Zhang, "Reversible data hiding in encrypted images," IEEE Signal *Process. Lett.*, vol. 18, no. 4, pp. 255–258, Apr. 2011.

[10] W.Hong, T. Chen, and H.Wu, "An improved reversible data hiding in encrypted images using side match", IEEE Signal Process. Lett.,vol. 19, no. 4, pp. 199–202, Apr. 2012.

BIOGRAPHY

Mr. K C V Raghavacharyulu received his B.Tech Electronic Communication Engineering from Sai Aditya Institute of science and technology, Surampalem, Andhra Pradesh, INDIA in 2012 and pursuing M.Tech Instrumentation and control system from university college of Engineering, JNTUK, Kakinada, Andhra Pradesh, in the year of 2013-2015. His Interested areas include Image Segmentation, Image processing and network security.

Mrs. K.RamaDevi obtained M.Tech degree in Microwave and Radar Engineering from Osmania University College of Engineering, Hyderabad in 2003. She is presently working as Assistant Professor in the Department of Electronics and Communication Engineering, University College of Engineering, JNTUK, Kakinada, A.P., INDIA. She is presently pursuing Doctoral degree from J.N.T.U. College of Engineering, Kakinada. She presented many research papers in various national and international journals and conferences. Her research interests include Micro Strip Patch Antennas, slot antennas simulated in MATLAB and HFSS.

ISSN: 2278 – 7798