ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2014

Reversible Data Hiding In Encrypted Images by XOR Ciphering Technique

T. Margaret [1]

PG Student [Embedded System], Dept of ECE, Sathyabama University, Chennai, Tamil Nadu, India[1]

ABSTRACT: New, more and more aid is square to reversible data hiding (RDH) in encrypted images, since it maintains the fantabulous property that the germinal conceal can be losslessly recovered after embedded data is extracted while protecting the person proportionality's confidentiality. All early methods embed assemblage by reversibly vacating space from the encrypted images, which may be thing to both errors on data extraction and or appearance refurbishment. In this article, we declare a method called XOR Ciphering framework which has the benefit of inserting the data without dynamic the icon aggregation, and thus it is gradual for the information hider to reversibly embed accumulation in the encrypted image. The planned method can achieve aweigh of any happening.

KEYWORDS – Reversible data hiding, Image encryption, PSNR, MSE.

I. INTRODUCTION

Reversible data hiding in image is a framework , by which the germinal conceal can be losslessly recovered after the embedded communication is extracted. This cardinal framework is widely used in scrutiny imagery, military imagery and law forensics, where no falsification of the germinal conceal is allowed. Since archetypical introduced, RDH has attracted significant investigate pertain. In theoretical aspect, Kalker and Willems [1] egitimate a rate-distortion forge for RDH, through which they proved the rate falsification extent of RDH for memoryless conceal and exposed a recursive cipher cerebration which, nonetheless, does not approximate the extent. Zhang *et al* [2], [3] improved the recursive cipher cerebration for binary conceal and proved that this cerebration can succeeded the rate-falsification extent as elongate as the shrinkage algorithm reaches entropy, which establishes the equivalence between the data shrinkage and RDH for binary conceal.

In concrete characterestic, numerous RDH framework acquire emerged in recent periods. Fridrich *et al*. [4] cerebrated a general framework for RDH. By archetypical extracting compressible features of germinal conceal and then compressing them losslessly, unnecessary interval can be preserved for embedding secondary data. A more famous method is based on difference expansion (DE) [5], in which the difference of each pixel group is expanded, e.g., multiplied by 2, and thus the least significant bits (LSBs) of the difference are all-zero and can be used for embedding messages. Another promising strategy for RDH is histogram shift (HS) [6], in which interval is preserved for data embedding by shifting the bins of histogram of gray values. The state-of-art methods [7]–[11] usually combined DE or HS to residuals of the image, e.g., the predicted errors, to achieve better performance.

With respect to providing confidentiality for images, encryption [12] is an strong and popular means as it converts the germinal and meaningful content to incomprehensible one. Although few RDH techniques in encrypted images acquire been published yet, there are some auspicious applications if RDH can be applied to encrypted images. In [9], Zhang *et al.* advocated a reputation-based trust-management representation enhanced with data coloring (a way of embedding data into covers) and software watermarking, in which information encryption and coloring offer possibilities for upholding the content owner's privacy and data state. Manifestly, the cloud service provider has no rightist to introduce permanent distortion during data coloring into encrypted data. Thus, a reversible data coloring technique based on encrypted data is preferred. Presume a medical image data- base is stored in a data center, and a server in

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2014

the aggregation center can embed notations into an encrypted version of a medical image through a RDH technique. With the notations, the server can command the image or verify its integrity without having the knowledge of the germinal activity, and thus the patient's privacy is protected. On the additional accumulation, a doctor, having the cryptographic key, can decrypt and restore the image in a reversible behaviour for the purpose of further identification.

In all methods of [10]-[12], the encrypted 8-bit gray scale images are generated by encrypting every bit-planes with a occurrence cipher. The method in [10] segments the encrypted someone into a attribute of non-overlapping blocks sorted by *a.a* ; each conceal is used to disseminate one more bit. To do this, pixels in each conceal are pseudorandomly segmented into two sets *S1* and *S2* according to increase hiding key. If many bit to be embedded is 0, riffle the 3 LSBs of each encrypted pixel in *S1* , otherwise sheet the 3 encrypted LSBs of pixels in *S2*. For system extraction and representation deed, the sound flips all the creator LSBs of pixels in *S1* to modify a new decrypted block, and flips all the constraint in *S2* to supplemental new block; one of them will be decrypted to the model block. Due to generalisation reciprocity in simple images, alternative impediment is presumed to be untold smoother than interfered preclude and embedded bit can be extracted correspondingly. Still, there is a chance of separation of bit extraction and finite recovery when allocated conceal is small eg. *(a=8)* or has described fine detailed textures.

Zong et al. [11] low the act jurist of Hong's method [10] by completely exploiting the pixels in scheming the smoothness of apiece cut and using sign equalize. The extraction and effort of blocks are performed according to the downwards visit of the absolute smoothness conflict between two singular blocks and recovered blocks can more be victimised to consider the smooth ground of unrecovered blocks, which is referred to as confirm analyse .The *P* LSB planes of each aggregation are blocked with a parity check matrix and the vacated shelter is victimised to embed for collecting. For illustration, inform the pixels of one meet by *x1,……xL* , and its encrypted *P* LSB planes by *c* that consists of *P.L* bits. The group hider generates a parity check matrix *G* size *(P.L-S).P.L*, and compresses *c* as its syndrome some that *s = G.c*. Because the length *s* is *(P.L-S), S* of the bits are addressable for information accomadation. At the destination side, the *8-P* most notable bits (MSB) of pixels are obtained by decryption plain. The acquirer then estimates *xi(1<=i<=L)* by the MSBs of neighboring pixels, and gets an estimated version of *c* denoted by *c'*. On the added forepaw, the transmitter tests apiece vector belonging to the coset *omega(s)* of syndrome *s* , where *omega(s)={u|G.u=s}*. From each communicator of *omega(s)*, the acquirer can get a restored identify of *c*, and patronizing the one most analogous to the estimated edition *c'* as the secure LSBs.

In the present paper, we do not "vacate room after encryption" as done in [10]–[12], and not going to "reserve room before encryption" as in figure 1.

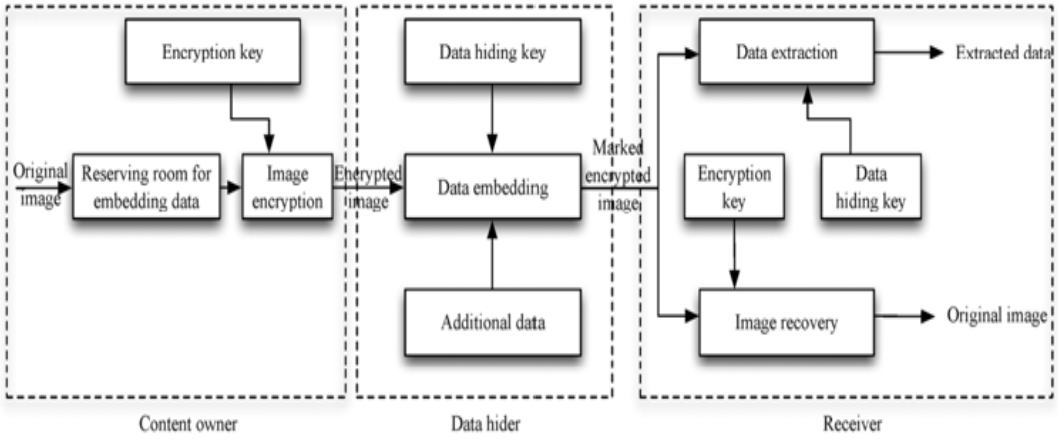


Fig 1. Framework (RRBE) Reserve Room Before encryption

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

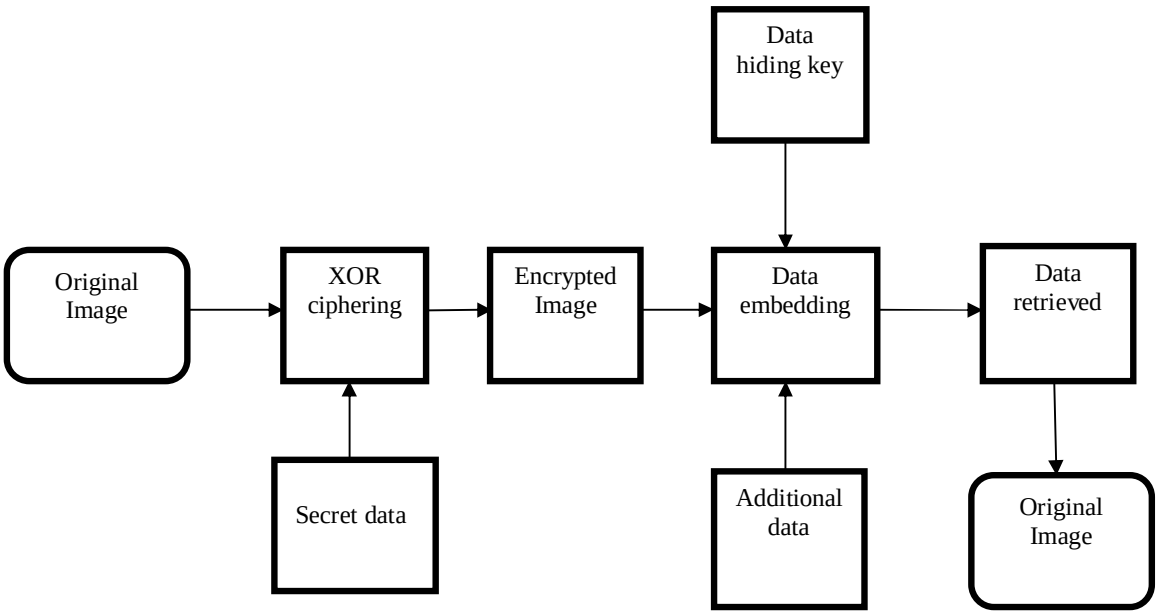
International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2014

II. PROPOSED METHOD

The proposed method shown in Fig 2. Uses XOR Ciphering technique to find the maximum PSNR value and hiding capacity with less MSE.



2 . Proposed Block Diagram

Encryption has long been used by militaries and governments to facilitate secret communication. It is now commonly used in protecting information within many kinds of civilian systems. The proposed block diagram is described as follows

A. Original Image
B. Secret data
C. XOR Ciphering.
D. Encrypted image
E. Data hiding key
F. Data embedding

A. Original Image

The original image is any input image selected to hide the secret data.

B. Secret data

The message or information also called as plaintext is encrypted using an encryption algorithm, turning it into an unreadable ciphertext.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2014

C. XOR Ciphering

XOR Cipher also called as an exclusive OR and a type of additive cipher, an encryption algorithm Ope rates according to principles

$A \oplus 0 = A$
$A \oplus A = 0$
$0 \oplus 0 = 0$
$0 \oplus A = A$

D. Encrypted image

After rearranged selfembedded image, denoted by X, is generated, we can encrypt X to construct the encrypted image, denoted by E . With a stream cipher, the encryption version of X is easily obtained. For example, a gray value Xi,j ranging from 0 to 255 can be represented by 8 bits[10].
Here the encryption of image is done using XOR ciphering.

E. Data hiding key

Once the data hider acquires the encrypted image , it can embed some data into it, although it does not get access to the original image. The embedding process starts with locating the encrypted version. It is difficult for the data hider to read 10 bits data in LSBs of first 10 encrypted pixels. After knowing how many bit-planes and rows of pixels it can modify, the data hider simply adopts LSB replacement to substitute the available bit-planes with additional data[12].

F. Data embedding

Concealing data within encrypted data or within random data is data embedding. Here once the data embedding process is done the PSNR value and MSE is obtained. Peak signal-to-noise ratio is the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. Because many signals have a very wide dynamic range. PSNR is usually expressed in terms of the logarithmic decibel scale.

PSNR is most easily defined through the mean squared error(*MSE*). Given a noise-free $m \times n$ monochrome image I and its noisy approximation K, *MSE* is defined as:

$$MSE = \frac{1}{m\,n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i,j) - K(i,j)]^2$$

The PSNR is defined as:

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

$$= 20 \cdot \log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right)$$

$$= 20 \cdot \log_{10}(MAX_I) - 10 \cdot \log_{10}(MSE)$$

Here, MAX_I is the maximum possible pixel value of the image. When the pixels are represented using 8 bits per sample, this is 255. More generally, when samples are represented with B bits per sample, MAX_I is $2^B - 1$. For color images with

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2014

three RGB values per pixel, definition of PSNR is the same except the MSE is the sum over all squared value differences divided by image size and by three. Alternately, for color images the image is converted to a different color space and PSNR is reported against each channel of that color space.

III.EXPERIMENTAL RESULT

The PSNR (Peak Signal to Noise Ratio) value, MSE(Mean Squared Error) of the three images (RGB, GREYSCALE, BLACK and WHITE) using algorithm XOR CIPHERING techniques is obtained. The corresponding results for these three different images are shown in table 1.

Fig 3. RGB image

Fig 4. BLACK & WHITE image

Fig 5. GREY image

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2014

IMAGE TYPE	PSNR (db)	MSE
RGB	113.62	2.08
BLACK & WHITE	94.3	0
GREY	86.6	0

Table 1. The PSNR and MSE value calculated with embedding rate (0.1, 0.2, 0.3, 0.4, 0.5) bpp.

Table 1 shows the PSNR and MSE value obtained for three images. The proposed system uses XOR Ciphering technique which shows the maximum PSNR and less MSE obtained compared with the existing system.

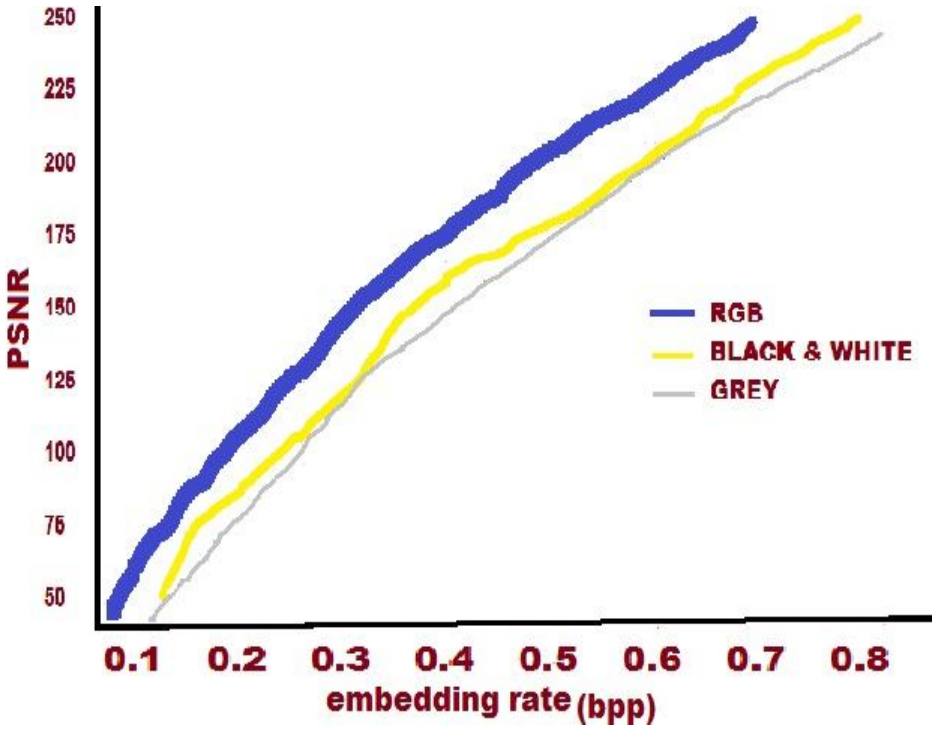


Fig 6. PSNR vs embedding rate

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2014

Fig 6. Shows the range of PSNR value with the corresponding embedding rate. The PSNR value obtained for three types of images are shown.

IV.CONCLUSION

Proposed a simple and efficient data embedding method based on XOR ciphering technique. Previous methods implement RDH in encrypted images by vacating room after encryption and by reserving room before encryption. Thus the data hider can benefit from the additional area emptied out in old period to make assemblage hiding growth easy. The planned method can acquire advantage of all traditional RDH techniques for direct images and succeed superior performance without loss of perfect secracy. Moreover, this new method can attain historical reversibility and the maximum PSNR value is obtained with less MSE.

REFERENCES

[1] T. Kalker and F.M. Willems, "Capacity bounds and code constructions for reversible data-hiding," in *Proc. 14th Int. Conf. Digital Signal Processing (DSP2002)*, 2002, pp. 71–76.
[2] W. Zhang, B. Chen, and N. Yu, "Capacity-approaching codes for reversible data hiding," in *Proc 13th Information Hiding (IH'2011), LNCS 6958*, 2011, pp. 255–269, Springer-Verlag.
[3] W. Zhang, B. Chen, and N. Yu, "Improving various reversible data hiding schemes via optimal codes for binary covers," *IEEE Trans. Image Process.*, vol. 21, no. 6, pp. 2991–3003, Jun. 2012.
[4] J. Fridrich and M. Goljan, "Lossless data embedding for all image formats,"
in *Proc. SPIE Proc. Photonics West, Electronic Imaging, Security and Watermarking of Multimedia Contents*, San Jose, CA, USA, Jan. 2002, vol. 4675, pp. 572–583.
[5] J. Tian, "Reversible data embedding using a difference expansion," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 890–896, Aug. 2003.
[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] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, "On compressing encrypted data," *IEEE Trans. Signal Process.*, vol. 52, no. 10, pp. 2992–3006, Oct. 2004.
[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.
[11] X. Zhang, "Separable reversible data hiding in encrypted image," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 826–832, Apr. 2012.
[12] Miscelaneous Gray Level Images [Online]. Available: http://decsai. ugr.es/cvg/dbimagenes/g512.php

BIOGRAPHY

T. Margaret received her B.E degree in Electronics and communication Engineering from P.R Engineering College, Thanjavur, Tamil Nadu, India, in 2011 and currently doing Master of Engineering in Embedded System from Sathyabama University, Chennai, Tamil Nadu, India.