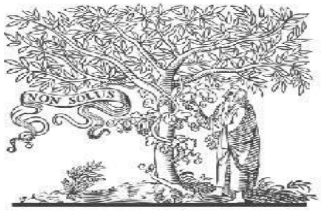
International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

COPY RIGHT



ELSEVIER SSRN

IJIEMR Transactions, online available on 31st Jan 2018. Link :http://www.ijiemr.org/downloads.php?vol=Volume-07&issue=Issue 01

10.48047/IJIEMR/V07/ISSUE 01/55

Title **Lossless and Reversible Data Hiding in Encrypted Images with Public Key Cryptography**

Volume 7, Issue 1, Pages: 464-471

Paper Authors
M. Nagaraju Naik

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

Lossless and Reversible Data Hiding in Encrypted Images with Public Key Cryptography

M. Nagaraju Naik[1]
[1]Professor of Department of ECE, CMR College of Engineering and Technology, Kandlakoya, Hyderabad, Telangana.

Abstract:

Here proposes a lossless, a reversible, and combined data hiding schemes for ciphertext images encrypted by public key cryptosystems with probabilistic and homomorphic properties. In the lossless scheme, the ciphertext pixels are replaced with new values to embed the additional data into several LSB-planes. Then, the embedded data can be directly extracted from the encrypted domain. The data embedding operation does not affect the decryption of original plaintext image. In the reversible scheme a pre- processing is employed to shrink the image histogram before image encryption. With the combined technique, a receiver may extract a part of embedded data before decryption, and extract another part of embedded data and recover the original plain text image after decryption.

Introduction

Due to increase in numerous crimes in present era, led to usage of digital multimedia almost everywhere, this in turn raises the issue of protecting personal information and has emerged as a much more important topic. Multitudinous researches and studies have been made to focus on safe guarding the images, such as facial images, where secrecy and privacy protection is needed. However, changes in the life environment caused by the rapid development of digital media techniques and communication media have changed users' emotional and sensual feelings. Consequently led to, the study on human senses and sensibility, in earnest to satisfy user needs through the convergence of many different fields. It is required to develop image obfuscation techniques which can minimize the infringement of user sensibility and simultaneously protect private life. Therefore, it is necessary to develop techniques to minimize the infringement of user sensibility and protect their privacy. Reversible De-Identification is a process which, while still concealing the identity of individuals, enables persons in possession of high security credentials to recover the original multimedia content containing private information.

The authors in encode the region of interest (ROI) and background in separate data layers using JPEG2000. On the other hand, the authors in employ encryption strategies directly on the pixel intensities of the ROI. However, these methods completely destroy the naturalness of the captured video. A ROI transform-domain scrambling technique was presented in for different image/video compression standards. The scrambling process better maintains the naturalness of the video. Non-reversible watermarking was adopted in to solve the latter issue and embed the information needed to recover the De- Identified region within the video itself. However, both these schemes are irreversible since the noise introduced by the watermark embedding process is permanent. Moreover, these schemes have registered a substantial reduction in compression efficiency. However, this method induces significant distortions within the obfuscated image themselves. This work presents a Reversible De-Identification method for lossless images. This approach adopts Reversible Watermarking to make the system reversible. The proposed solution is completely independent from the obfuscation process, and is thus generic.

Literature Review

Since lossless data hiding cannot reduce the amount of data needed to represent the image to the same degree as lossy data hiding, to achieve greater data hiding one must use a visually lossless data hiding technique. Visually lossless refers to data hiding techniques in which a scant amount of data is lost. It is important to note that the minute amount of data that is lost is visually imperceptible.

Non-degrading lossy or visually lossless (Exhibit E) data hiding technology attempts to eliminate redundant or unnecessary information, such as dots. Visually lossless data hiding produces a document that visually appears to be the same, but has minute differences. For example, an original document is scanned and stored. Through visually lossless data hiding the document is reproduced.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

However, instead of storing dot for dot, the data hiding scheme looks at the document and finds repeating patterns. Returning to the example of the duplicating the square, mentioned above, Paul is now asking Chris to draw several squares, triangles and circles on a page. Every now and then one of the squares to be duplicated has a single side with a line 0.5 millimeter longer than the others. They could save even more time in their duplicating process by just ignoring the 0.5 millimeter difference and calling it a square because the difference was probably an error in the original drawing of the square anyway. Even if it was not an error, a 0.5 millimeter extension on the line is pretty much imperceptible to a person looking at the picture.

This would work in document imaging as follows. The small letter "a" appears 50 times on the page of the original document. The visually lossless software will then store the small letter "a" once and use it again and again to replace the other 49 occurrences of the letter "a" on the page of the original document. If the last letter "a" on the page has an extra dot on the tail of the character, the extra dot will not be there when the character is printed. Why? Because the "a" that was stored in the system was not the one with the extra dot on the tail. The human eye will not perceive this minute detail. The name "visually lossless" arises from the fact that the human eye will not perceive these microscopic details.

Methodology

This paper proposes a lossless, a reversible, and a combined data hiding schemes for public-key-encrypted images by exploiting the probabilistic and homomorphic properties of cryptosystems. With these schemes, the pixel division/reorganization is avoided and the encryption/decryption is performed on the cover pixels directly, so that the amount of encrypted data and the computational complexity are lowered. In the lossless scheme, due to the probabilistic property, although the data of encrypted image are modified for data embedding, a direct decryption can still result in the original plaintext image while the embedded data can be extracted in the encrypted domain. In the reversible scheme, a histogram shrink is realized before encryption so that the modification on encrypted image for data embedding does not cause any pixel oversaturation in plaintext domain. Although the data embedding on encrypted domain may result in a slight distortion in plaintext domain due to the homomorphic property, the embedded data can be extracted and the original content can be recovered from the directly decrypted image. Furthermore, the data embedding operations of the lossless and the reversible schemes can be simultaneously performed in an encrypted image. With the combined technique, a receiver may extract a part of embedded data before decryption, and extract another part of embedded data and recover the original plaintext image after decryption.

ROI Extraction

For few decades digital X-ray imaging has been one of the most important tools for medical diagnosis. With the advent of distance medicine and the use of big data in this respect, the need for efficient storage and online transmission of these images is becoming an essential feature. Limited storage space and limited transmission bandwidth are the main challenges. Efficient image compression methods are lossy while the information of medical images should be preserved with no change. Hence, lossless compression methods are necessary for this purpose. In this paper, a novel method has been proposed to eliminate the non-ROI data from bone X-ray images.

Payload Generator

The Payload Generator Process receives the difference image D which is compressed using the predictive coding method followed by the Deflate algorithm. The original image I is authenticated using SHA-1 which generates a 20-Byte Hash.

Face Obfuscation

According to the development of digital devices and the release of many different smart phones and wearable devices including smart glass, the issue of protecting personal information has emerged as a much more important topic. Many studies and social interests have been concentrated on the protection of the images, such as facial images, where privacy protection is required. In this context, if the image currently playing on the screen is suddenly mosaicked or blurred at any moment for privacy protection, users can be irritated and have doubts about the use of the devices themselves. The existing compression techniques such as M-JPEG, M-JPEG 2000, MPEG-4, or AVC/H.264 are mainly used as these privacy protection techniques. This study is limited to the visualization method of "obfuscation techniques," the second method. With the fact that smart devices perform specific purposes and functions. For this, the method through the

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

convergence with artistic sensibility will be presented.

Reversible Contrast Mapping

MOST of the reversible watermarking approaches proposed so far incorporate a lossless data compression stage . The use of an elaborate data compression stage increases the mathematical complexity of the watermarking. A simple integer transform defined on pairs of pixels. RCM is perfectly invertible, even if the least significant bits (LSBs) of the transformed pixels are lost. The data space occupied by the LSBs is suitable for data hiding. The basic RCM watermarking scheme was introduced in. Here, a modified version that allows robustness against cropping is proposed. It is shown that the RCM scheme provides almost similar embedding bit-rates when compared to the difference expansion approach, but it has a considerably lower mathematical complexity.

Let be image gray level range (for eight-bit gray level images), and let be a pair of pixels. The forward RCM transforms pairs of pixels into pairs of pixels.

$$x' = 2x - y, \quad y' = 2y - x. \qquad (1)$$

To prevent overflow and underflow, the transform is restricted to a sub domain defined by the equations.

$$0 \le 2x - y \le L, \quad 0 \le 2y - x \le L. \qquad (2)$$

As shown in Fig. 1(a), is a rhombic domain located along the diagonal of . The inverse transform is defined as follows:

$$x = \left\lceil \frac{2}{3}x' + \frac{1}{3}y' \right\rceil, \quad y = \left\lceil \frac{1}{3}x' + \frac{2}{3}y' \right\rceil \qquad (3)$$

where is the ceil function (the smallest integer greater than or equal to). As stated in Section I, the pair forward-inverse transform should give exact results. It immediately appears that if the LSB of was "1," the values inside the ceil functions for the computation of and decrease with 2/3 and 1/3, respectively. Similarly, if the LSB of was "1," the corresponding values decrease with 1/3 (for the computation of) and 2/3 (for the computation of). Except when both LSBs are "1," the ceil function recovers the correct results. An LSB of "1" means an odd integer number. From (1), it follows.

Threshold Selection

It is important in picture processing to select an adequate threshold of gray level for extracting objects from their background. A variety of techniques have been proposed in this regard. In an ideal case, the histogram has a deep and sharp valley between two peaks representing objects and background, respectively, so that the threshold can be chosen at the bottom of this valley . However, for most real pictures, it is often difficult to detect the valley bottom precisely, especially in such cases as when the valley is flat and broad, imbued with noise, or when the two peaks are extremely unequal in height, often producing no traceable valley. There have been some techniques proposed in order to overcome these difficulties. They are, for example, the valley sharpening technique , which restricts the histogram to the pixels with large absolute values of derivative (Laplacian or gradient), and the difference histogram method , which selects the threshold at the gray level with the maximal amount of difference.

The proposed Threshold Selection method is based on the observation that different sub-bands provide different levels of distortions. This work employs Differential Evolution (DE), which is a population based optimization algorithm, to derive the set of threshold which minimize a distortion criterion while ensuring that the capacity of the proposed system is sufficient to embed the messages.

ROI Replacement

Segmentation is very important to image retrieval process. The shape feature and the layout feature both depend on good segmentation technique. Thresholding, Region growing, Region splitting and Merging are examples of such methods in this category. In Region based segmentation the objective is to partition an image into regions. This paper explains the algorithms for finding Region of Interest from the facial images and extraction of features from the respective Region of Interest. In the proposed techniques, the different ROI's from the facial data are taken as Lips and Eyes of human facial image. These are detected from the face with the help of skin color and the knowledge based methods in concern with the human facial data. The ROI Replacement process replaces the region marked by the bounding box β with the recovered face image F. The image can be authenticated by comparing the hash derived by computing the SHA-1 on to the Hash value present in the tail of the packet.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

Proposed Enhancement Method

	Flag Values	
	A	e
Flag	0	0
Flag N_e e	0	1
Flag N_A A	1	0
Flag N_A A N_e e	1	1

As it was mentioned before, Image enhancement is an important feature in satellite imaging, which makes the image enhancement of such images to be of vital importance as increasing the enhancement of these images will directly affect the performance of the system using these images as input. The edge enhancement filtering is carried out with the help of traditional filters. But these filters do have some problems, especially while enhancing a noisy image. The effort on edge enhancement has been focused mostly on improving the visual perception of images that are unclear because of blur. Noise removal and preservation of useful information are important aspects of image enhancement. A wide variety of methods have been proposed to solve the edge preserving and noise removal problem. In order to increase the quality of the enhanced image, preserving the edges is essential. Mathematical morphology is the name given to a geometrical branch of nonlinear filters. It offers a unified and powerful approach to numerous image processing problems. One of the most appealing aspects of morphological image processing lies in addressing the image sharpening problem. In this paper, a new edge detected morphological filter is proposed to sharpen aerial images. The low contrast satellite input color images. DWT separates the input image into different sub band images, namely LL, LH, HL, and HH. DWT has been employed in order to preserve the high frequency components of the image. The input low contrast color image is decomposed into R,G,B. DWT is apply to each color(R,G,B) separately.

Experimental Results

The results presented in this section consider two different sets of images. The first set was composed of the standard test images Lena, Barbara, Aircraft and Mandrill while the second set consisted of 2000 frontal images from the color FERET dataset. All images considered in this work were converted in the YCbCr color space using 4:4:4 sampling. The proposed algorithm has set the maximum number of decompositions Mto 3 which ensures a single pass embedding capacity offered by the first level of watermarking of 0.9844 bpp. The Difference Expansion method was configured using values suggested in and thus adopted α= 0.5,NP = 100 and Γ= 0.3. This paper does not claim that this corresponds to an optimal configuration, but claims that it provides performance superior to state of the art IWT threshold selection schemes such as . These results clearly demonstrate that the proposed scheme manages to provide better quality of the stego image IθW at different capacities. Simulation results further demonstrate that the proposed scheme needs on average 20 generations to converge. This correspond to 2000 invocations of the fitness function which is significantly less than the 255NT invocations needed by exhaustive search. Fig. demonstrates the cumulative density function (CDF) of the capacity needed to embed packet swithin the obfuscated image using the set of 2000 frontal images from the color FERET dataset. It can be seen that a capacity smaller than 0.8 bpp is needed 99.8% of the time while they never require more than 1.1 bpp.

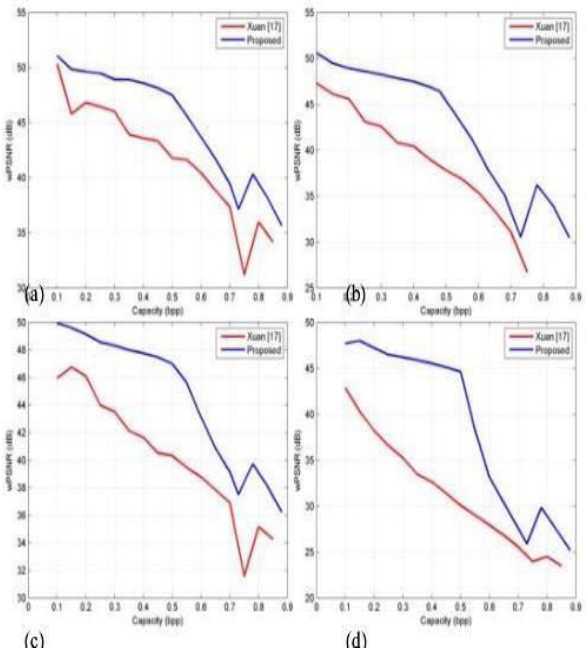


Figure Rate-Distortion performance using different threshold selection methods for (a)Aircraft (b) Barbara (c) Lena and (d) Mandrill test images

The images in Fig. demonstrate the superiority of the proposed method in relation to other state of the art methods. It can be seen that the encryption [5] and scrambling [8] processes provide images which are not natural.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

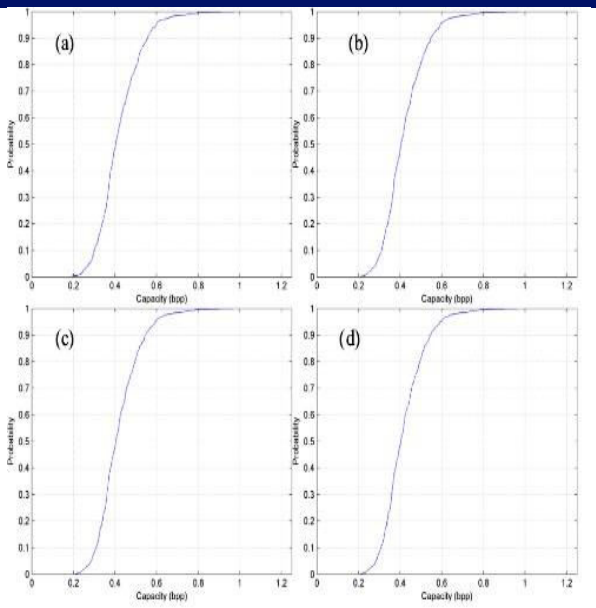


Figure CDF of the capacity needed to embed s at different obfuscation levels (a) k-2, (b) k-5, (c) k-10 and (d) k-20

Figure comparing the resulting reversible de-identified images (a) original image, (b) scrambling of DCT coefficients, (c) encryption of pixel values, (d) proposed method

This work presents a novel Reversible De-Identification method for lossless compressed images. The proposed scheme is generic and can be employed with other obfuscation strategies other than k- Same. A two-level Reversible-Watermarking scheme was adopted which uses Differential Evolution to find the optimal set of thresholds and provides a single-pass embedding capacity close to 1.25 bpp. Simulation results have shown that this method is able to recover the original image if the correct encryption key is employed. It further shows that 0.8 bpp were sufficient to cater for 99.8% of the frontal images considered and none of the image needed more than 1.1 bpp. Future work will focus on the extension of this algorithm for lossy image and video compression standards.

CRYPTOGRAPHY
BLOCK DIAGRAM OF CRYPTOGRAPHY

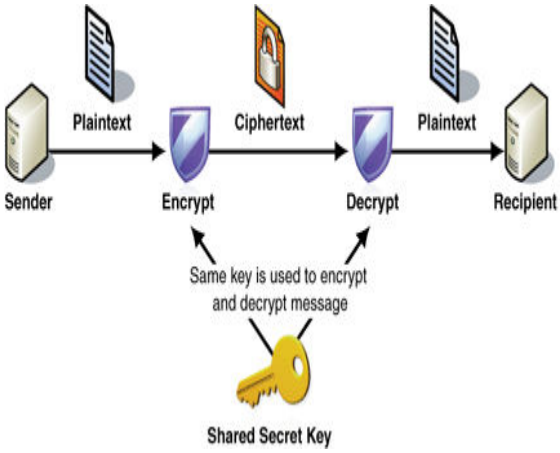


Figure Block diagram of cryptography

It is the art and science of embedding secret messages like a file, message, image or video within another cover(duplicate) like file, message, image or video.

Cryptography technique have high security.

LOSSLESS SCHEME
BLOCK DIAGRAM OF LOSSLESS SCHEME

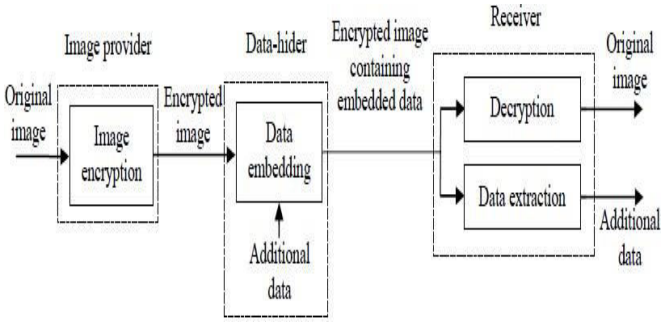


Figure: sketch of lossless data hiding scheme for public key encrypted image

- A lossless data hiding scheme for public-key-encrypted images is proposed.
- Encryption and data hiding are two effective means of data protection. While the encryption techniques convert plaintext content into unreadable ciphertext,
- The data hiding techniques embed additional data. Data hiding may be performed with a lossless
- In this lossless scheme we perform the encryption technique. So that

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

the data will be hided.
After that the hidden information is transmitted to the receiver with out any loss.

EVERSIBLE SCHEME
BLOCK DIAGRAM OF REVERSIBLE SCHEME

- Reversible data hiding is a widely used technique on the basis of watermarking. The host image can be recovered exactly.
- Reversible Data Hiding technique is applied at medical and military applications. The data embedding process will usually introduce permanent loss to the cover medium.
- Reversible Data Hiding which enables images to data in hidden form and restored to their origin by removing digital hidden data.
- Here we use histogram shrinking to avoid oversaturation. And the embedded data will be reversed. Therefore the security increases.

BLOCK DIAGRAM FOR COMBINED SCHEME

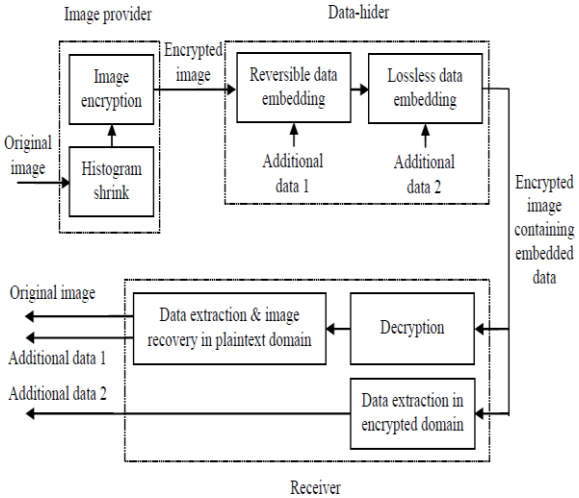


Figure: sketch of combined scheme

Here we combine both lossless & reversible schemes and transmit the required information with high security.

WORKING

i. First an input image (original) is given from the sender. The image is encrypted by the encryptor and the encrypted image is then transmitted to data hider.

ii. In Data hider, we are using both lossless and reversible schemes. In lossless scheme, cyphertext pixels are replaced with the new values to embedded data into several LSB planes of cyphertext pixels. The embedded data can be directly extracted from an encrypted domain. The data embedding operation doesn't affect the decryption of the original plaintext image.

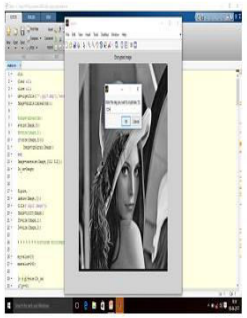
iii. In Reversible scheme, preprocessing is employed to shrink the image histogram. Due to the compatibility of both lossless and reversible schemes, the data embedding operation in two manners can be simultaneously performed in an encrypted image.

iv. With this combined technique, receiver may extract a part of embedded data before decryption and extract another part of embedded data after decryption and recover the original plain text image.

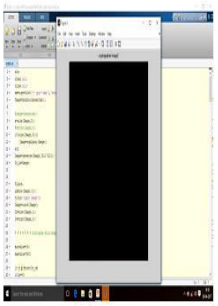
v. This project has been implemented using MATLAB software.

RESULT

At Transmitter side

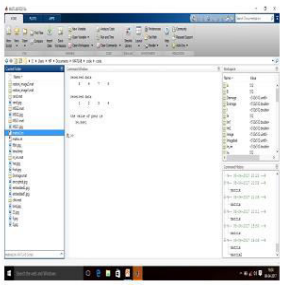


(a) Encrypted image image

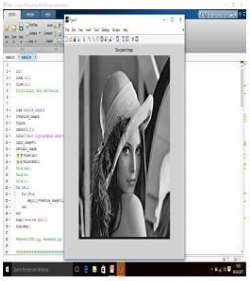


(b) Cryptography

At Receiver side



(a) Received data



(d) Decrypted image

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

CONCLUSION

Comparison of results make between conventional algorithms and the proposed algorithm. Proposed algorithm produces individually advanced embedded quality of images provided with a same embedding capacity. In proposed research a Symmetric image encryption algorithm based upon SSI S-Block and chaotic sequence is proposed. The unique BSSI s-block performs the change on the chaotic encoded image initially and then pixel matrix is completed by shuffling columns and rows of cipher. After simulation of the algorithm it shows that faster execution time. The proposed technique is studied in terms of key space analysis, statistical analysis, brute-force attack. in future the technique can be verified on various attacks. And this proposed work also explore the use of dynamic S- box for improved computing security.

FUTURE SCOPE

- Machine learning techniques may be used to improve the results.
- The proposed work may be extent for video compression and cryptography.

REFERENCES

[1] Xinpeng Zhang, Jing Long, Zichi Wang, and Hang Cheng "Lossless and Reversible Data Hiding in Encrypted Images with Public Key Cryptography" 1051-8215 (c) 2015 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.

[2] Shamim Ahmed Laskar and Kattamanchi Hemachandran "High Capacity data hiding using LSB Steganography and Encryption" Department of Computer Science International Journal of Database Management Systems (IJDMS) Vol. 4, No. 6, December 2012.

[3] Ashwak Mahmood Alabaichi "Color Image Encryption using 3D Chaotic Map with AES key Dependent S-Box" JCSNS International Journal of Computer Science and Network Security, VOL.16 No.10, October 2016

[4] M. Ushanandhini and D. Chitra "Optimal Prediction Scheme Using Reversible Information Hiding" International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE) ISSN: 0976-1353 Volume 23 Issue 4 –August 2016.

[5] Patil K. U. 1 & Nandwalkar B. R. "GA Based Reversible Data Hiding in Encrypted Images by Reserving Room before Encryption" IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) e-ISSN: 2278-2834, p-ISSN: 2278-8735

[6] X. L. Li, B. Yang, and T. Y. Zeng, "Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection," IEEE Trans. Image Process., vol. 20, no. 12, pp. 3524–3533, December. 2011.

[7] Lokesh Kumar, Novel Security Scheme for Image Steganography using Cryptography Technique, Volume 2, Issue 4, April 2012.

[8] Z. Ni, Y. Shi, N. Ansari, and S. Wei, ―Reversible data hiding, IEEETrans. CircuitsSyst. VideoTechnol.,vol.16,no.3,pp.354–362,Mar. 2006.

[9] Anchal Jain, Navin Rajpal, "A Two Layer Chaotic Neural Network based Image EncryptionTechnique", IEEE National conference on computing and Communication systems, ISBN 978-1-4673-1952-2, 2012.

[10] Grasha Jacob, A. Murugan, "An Encryption Scheme with DNA Technology and JPEG Zigzag Coding for Secure Transmission of Images", arXiv: 1305.1270v1, 2013.

[11] Grasha Jacob, Murugan A, "A Hybrid Encryption Scheme using DNA Technology", IJCSCS Vol 3, Feb 2013.

[12] Zhang Yunpeng, Zhu Yu, Wang Zhong, Richard O.Sinnott, "Index-Based Symmetric DNA Encryption Algorithm", IEEE (4th CISP), DOI 10.1109/CISP.2011.6100690.

[13] C. E. Shannon, "Communication theory of secrecy systems, Bell System" Technical Journal 28–4 (1949) 656–715.

[14] Xingyuan Wang · Qian Wang "A novel image encryption algorithm

based on dynamic S- boxes constructed by chaos", Nonlinear Dyn (2014) 75:567-576.