iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** III **Month of publication:** March 2018

DOI: http://doi.org/10.22214/ijraset.2018.3635

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue III, March 2018- Available at www.ijraset.com

Comparative Study for Data Hiding Method using RDH Algorithms

A.Sindhiya[1], S. Sneha Raji[2], S.Sowmiya[3], G. Simi Margarat[4], K. Ravi kumar[5]
[1,2,3]*B.Tech, Department of Information Technology, RRASE College Of Engineering, Chennai, Tamilnadu, India*
[4]*Associate Professor, Department of Information Technology, RRASE College of Engineering, Chennai, Tamilnadu, India*
[5]*Professor & Head, Department of Computer Science and Engineering, RRASE College of Engineering, Chennai, Tamilnadu, India*

Abstract: Data Hiding is the process of hiding data in back of images or videos. The data hiding techniques mainly used in Military, Government and Medical Areas. Hiding process can be done in different types of algorithms. Mainly we are considering the RDH algorithm to hide the data. In this paper mainly focused on various works of Reversible data hiding algorithm and techniques.
Keywords: Data Hiding, RDH, Techniques.

I. INTRODUCTION

Information security is more important in the digital world. All things are shared only in digital format. The data are stored in Cloud. The data travel only through the medium of air. The internet only passes the data from one point to another. Effect of technology grow is hacking. In this situation, we must secure our data. Data secure done by lot of technologies.

For high security of data several approaches like steganography, Data Hiding and cryptography can be used. Data hiding is hide the data within a cover media. The data hiding process have two types. They

are embed data or cover media. In steganography, is to hide data in back of Visuals or Videos which help of pixels. These Steganography processes done in cover media.

Steganography methods have plenty of algorithms and techniques which are used to hide data. In mainly we are used REVERSIBLE DATA HIDING method. This RDH method contain some different compared to other hiding processes.

Reversible Data Hiding is image technique, by which aboriginal cover recovered by without ant lose of quality. In RDH, first select the pixels randomly with

Help of MCG. MCG means Mirroring Chipertext Group. Then vacate rooms and apply the mirroring concepts in those pixels. Next hide data in those selecting pixels. Then this process has encryption after that data hiding and image uploading.RDH has two encryption process, commonly we used only one encryption process. That's the specialty of the Reversible Data Hiding Process.

II. RELATED WORKS

In 2012, B. Macq [1] suggested this work proposes scheme of separable reversible data hiding for encrypted image using histogram modification. The sender is encrypt aboriginal image, the data-hider hides the secret data into the encrypted image by using histogram modification and *n*-nary data hiding scheme. On the receiver side, the secret message can be extracted by the embedding key, and the aboriginal image can be totally recollect by embedding and the encryption keys. If the embedding key is doesn't available for the receiver side, the aboriginal image can still be can't complete recollected using the encryption-key. This separable method doesn't require the sender to reserve embedding room by himself, and can perfectly recover the aboriginal image. In 2009, T. Bianchi, A. Piva, and M. Barni [2] they are suggested Signal processing modules working directly on encrypted data provides an elegant solution to solicitations scenarios where valuable signals must be protected from a malicious processing device. We enquire into the implementation of the Discrete Fourier Transform (DFT) in the encrypted domain, by using the homomorphic properties of the underlying cryptosystem. Some unique affairs are considered for the direct DFT, the radix-2, and the radix-4 fast Fourier algorithms, including the misconception scrutiny and the maximum size of the sequence that can be transformed. Also allocate computational complexity analyses and comparisons. The results show that the radix-4 FFT is best suited for an encrypted domain implementation in the proposed scenarios. In 2014, Z. Qian, X. Zhang, and S. Wang [3] this consistency proposes a framework of varying data obnubilating (RDH) in an encrypted JPEG bit stream. Unlike subsisting RDH for encrypted spatial domain images encrypting a JPEG bit stream into an opportunely organized structure, and embedding a secret data into the encrypted bit stream by scarcely modifying the JPEG stream. We identify utilizable bits congruous for data obnubilating so that encrypted bit stream

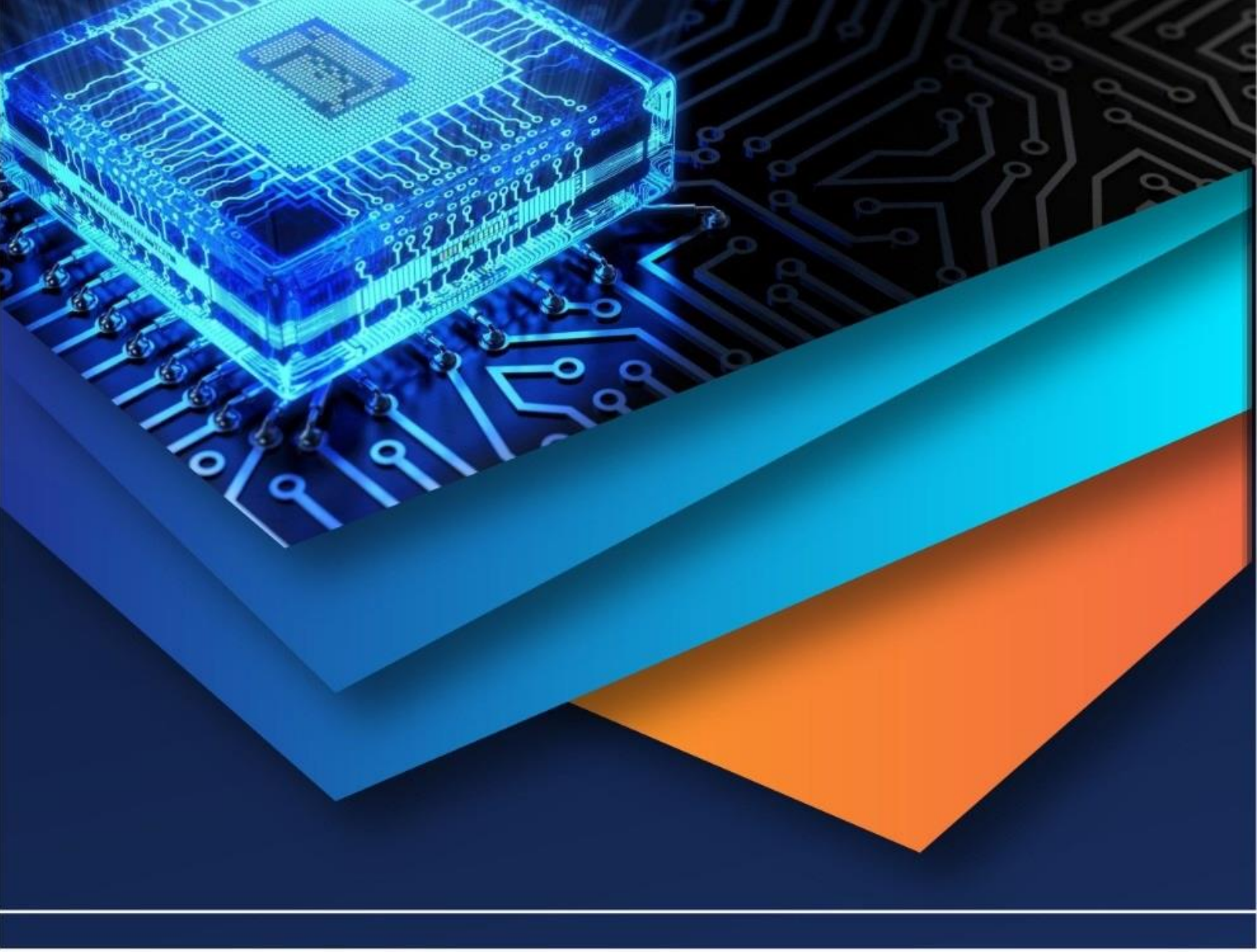
carrying private data can be correctly decoded. The private message bits are encoded with misconception rectification codes to achieve an impeccable data extraction and image recuperation. The encryption and embedding are controlled by encryption and insert keys properly. If a receiver has both keys, the secret bits can be extracted by analyzing the blocking artifacts of the neighboring blocks, and the pristine bit stream impeccably recuperated. In case the receiver only has the encryption key, he/she can still decode the bit stream to obtain the image with good quality without extracting the obnubilated data. In 2014, Z. Weiming Zhang n , Kede Ma, Nenghai Yu[4] A novel reversible data hiding technique in encrypted images is presented in this paper. Instead of embedding data in encrypted images directly, some pixels are estimated before encryption so that additional data can be embedded in the estimating misconception.. A benchmark encryption algorithm (e.g. AES) is applied to the rest pixels of the image and a special encryption scheme is designed to encrypt the estimating misconception. Without the encryption key, one can't get access to the aboriginal image. However, provided with the data hiding key only, he can embed in or extract from the encrypted image additional data without knowledge about the aboriginal image. Moreover, the data extraction and image recovery are free of misconceptions for all images. Experiments demonstrate the viability and efficiency of this method, in aspect of embedding rate versus Peak Signal-to-Noise Ratio (PSNR).In 2016, Z. Qian, X. Zhang [5] suggests With the popularity of outsourcing data to the cloud, it is vital to protect the privacy of data and enable the cloud server to easily manage the data at the same time. Under such demands, reversible data hiding in encrypted images (RDH-EI) attracts more and more researchers' attention. In this paper, we propose a novel framework for RDH-EI based on reversible image transformation (RIT). Different from all previous encryption based frameworks, in which the cipher texts may attract the notation of the curious cloud, RIT-based framework allows the user to transform the content of original image into the content of another target image with the same size. The transformed image, which looks like the target image, is used as the "encrypted image", and is outsourced to the cloud. Therefore, the cloud server can easily embed data into the "encrypted image" by any RDH methods for plaintext images. And thus a client-free scheme for RDH-EI can be realized, that is, the data embedding process executed by the cloud server is irrelevant with the processes of both encryption and decryption. Two RDH methods, including traditional RDH scheme and unified embedding and scrambling scheme, are adopted to embed watermark in the encrypted image, which can satisfy different needs on image quality and large embedding capacity respectively

III. CONCLUSION

Reversible data hiding in encrypted image is getting more attention these days because of security maintaining requirements. In this paper five different types of reversible data hiding techniques for digital images: LSB Modification Based Technique**,** Difference expansion technique, Histogram modification technique and Interpolation technique are studied, analyzed and compared. The comparative results show each technique has its own advantage and disadvantages.

REFERRENCES

[1] B. Macq, "Lossless multiresolution transform for image authenticating watermarking," in Proc. Eur. Signal Process. Conf., pp.533–536, 2000
[2] T. Bianchi, A. Piva, and M. Barni, "On the implementation of the discrete Fourier transform in the encrypted domain," IEEE Trans. On Information Forensics and Security, 4(1), pp.86–97, 2009
[3] Z. Qian, X. Zhang, and S. Wang, "Reversible data hiding in encrypted jpeg bit stream," IEEE Trans. on Multimedia, 16(5), pp.1486–1491, 2014
[4] W. Zhang, K. Ma, and N. Yu,"Reversibility improved data hiding in encrypted images by reserving images," Signal Processing, 94, PP.174–182, 2014.
[5] Z. Qian, X. Zhang, "Reversible data hiding in encrypted image with distributed source encoding," IEEE Trans. on Circuits and Systems for Video Technology, 26(4),pp. 636–646, 2016
[6] K. Ma, W. Zhang, et al., "Reversible data hiding in encrypted images by reserving room before encryption" IEEE Trans. on Information Forensics and Security, 8(3),pp.553–562, 2013
[7] P. Zheng, and J. Huang, "Discrete wavelet transform and data expansion reduction in homomorphic encrypted domain," IEEE Trans. Image Processing, 22(6), pp.2455–2468, 2013.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY