International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 09 Issue 10 ǁ 2021 ǁ PP. 20-25

Reversible Data Hiding in Encrypted Image Based on Histogram Bit Shifting Method (RIEHM)

Abhishek Kushwaha
M. Tech. Scholar, All Saints' College of Technology, Bhopal, India

Sarwesh Site
Professor, Dept. of CSE, All Saints' College of Technology, Bhopal, India

Zuber Farooqui
Professor, Dept. of CSE, All Saints' College of Technology, Bhopal, India

***ABSTRACT**: Histogram shifting method using image data hiding or image encryption. This technology have advanced and almost of the people like using the internet because the primary medium to transfer information from one end to another end overall the world. The information or data transfer one end to another end using internet very easy, quick and correct. But different issues with sending information or data over the internet are that the security threat. In this process non-public or confidential information will be hacked are modified original information or data. Existing method block shifting histogram (BSH) based on block shifting so image are visible and low robustness. It is a very important requirement information security and it is also important requirement transfer information through internet and safety. There are several analysis process techniques related with internet security likes image data hiding, watermarking, cryptography, and steganography. Our proposed method a robust Image encryption histogram shifting method based on bit shifting (RIEHSM). .Proposed method a bit shifting histogram is the generalized ways for image data hiding and improves robustness of encrypted image.*

***KEYWORDS:** Image encryption, Image decryption,Data Hiding,image recovery, PSNR,Reversible data hiding, Privacy protection.*

Date of Submission: 09-10-2021 Date of acceptance: 23-10-2021

I. INTRODUCTION

Processing encrypted information will be quite helpful for several applications, like activity data within an encrypted image. a standard application may be a buyer-seller watermarking protocol during which the vendor of the transmission product encrypts the initial information using a public encoding key so embeds a novel fingerprint to spot the customer within the encrypted information. A lot of general case might be a thing during which the content owner has encrypted a picture however desires to infix quite one extra information stream. Reversible information activity in pictures may be a technique for embedding additional information into pictures such the initial cover image will be losslessly recovered once the embedded information are extracted. Uses the difference between two consecutive image pixels to infix an additional bit, use a lossless compression technique to make further area for carry in extra information bits [1].

Digital watermarking is one in every of the ways that to prove the possession and also the authenticity of the media. There are primarily two varieties of watermarking algorithms: visible watermarking and invisible watermarking. For invisible watermarking, the watermark ought to be perceptually clear and strength. For visible watermarking, the watermark ought to be perceptually visible and strength. Lossless information hiding has been wide studied as a well-liked and powerful technique to protect copyright in several sensitive situations, e.g., diagnosing, remote sensing and enforcement [1]. Information activity is stated as a method to hide information (representing some information) into cover media. Nowadays, the distribution of multimedia system content on the web and different communication networks became a follow typically performed by users with totally different profiles. In this scenario, techniques dedicated to shielding this type of data play a crucial role, providing confidential transmission and reassuring the integrity of the received information. This area number of the explanations why the interest in learning watermarking, steganography and encoding for digital image, video, and audio, has increased over the years [2].

Steganographic techniques have the most purpose of concealing a relevant info (a text or a picture, for example) behind an apparently unimportant image. in a very sensible steganographic technique, an unauthorized person shouldn't be ready to notice the presence of any hidden info [3]. A digital watermark may be a reasonably fingerprint introduced while not ever-changing visual and statistical aspects of a picture. Watermarking has application in eventualities wherever info may be maliciously changed by a listener. The licensed recipient ought to be ready to verify the presence of the referred fingerprint, ratifying the origin of the image the copyright holder, for example and determinant the kind of modification it should have suffered [4].
The visible digital watermarking the paper focuses on the following points:
1. The data hidden drawback may be solved exploitation histogram shifting algorithmic program for information concealing,
2. It concentrates on the restoration of image quality in order that the covered image may be totally retrieved.
3. For greatly enhancing the protection the cryptography of the covered image is completed in order that within the absence of the key, the illegal user cannot access the image info [5].

Reversible information hiding Method : extra message are insert into some cover media, like military or medical pictures, in an exceedingly reversible manner so the first cover content are often absolutely repaired when extraction of the hidden message is termed reversible information hiding. General signal process generally takes place before encoding or when cryptography. generally the content owner doesn't believe the supplier of the service, in such cases ability to supply manipulating the plain content secret is undesirable. Thus manipulation on encrypted information once keeping the plain content is allowed. Because of the restricted channel resource a channel supplier with none data of the cryptography key might compress the encrypted information, once the key information to be transmitted. So as to confirm the privacy the content owner ought to cipher the information once it share a secret image with alternative person. Some info's like the origin information, image notation or authentication information, and is wish to be superimposed among the encrypted image by a channel administrator who doesn't understand the first image content. At receiver side it should be additionally expected that the first content are often recovered with none error when cryptography and retrieve of extra message. Meaning a reversible information hiding theme for encrypted image is desirable. Information hiding is that the method of concealing the information into covers media. That is, the information hiding method links a collection of the embedded information and a collection of the quilt media data. In most cases of information hiding, the first image becomes distorted because of information hiding and can't be inverted back to the first media. That is, cover media has permanent distortion even when the hidden knowledge is removed. In some applications, like diagnosis and enforcement it's desired that the first cover media are often recovered expeditiously with no loss. The marking techniques satisfying this demand arereferred to as reversible, lossless, distortion-free or invertible information hiding techniques [6].

Separable reversible information hiding Method: severable reversible information hiding, the name its self-indicates that it's a severable reversible information technique. That is its reversible information technique however that is severable. The severable means that that is ready to separate. The separation of activities i.e. extraction of original cover image and extraction of the payload is finished during this methodology. This separation needs some basic cause to occur. In dissociable information hiding key explained by Xinpeng Zhang the separation exists consistent with keys. At the receiver side, there are 3 completely different cases are encountered. The separation of extracting the information and obtaining the quilt media come back to exist. That's why it's known as-as dissociable reversible information hiding [6].

II.RELATED WORK

M.S Hwanga et al. [7] proposed a histogram shifting method for image reversible data hiding testing on high bit depth medical images. Among image local block pixels, the high correlation for smooth surface of anatomical structure in medical images are exploited. Thus a different value is applied for each block of pixels to produce a difference histogram to embed secret bits. During data embedding, the image blocks are divided into two categories due to two corresponding embedding strategies. Via an inverse
histogram shifting mechanism, the host image can be
accurately recovered after the hidden data extraction

T.Wang et al. [8] a new and reversible watermarking method is proposed to address this security issue. Specifically, signature information and textual data are inserted into the original medical images based on recursive dither modulation (RDM) algorithm after wavelet transform and singular value decomposition (SVD). In addition, differential evolution (DE) is applied to design the quantization steps (QSs) optimally for controlling the strength of the watermark. Using these specially designed hybrid techniques, the proposed watermarking technique obtains good imperceptibility and high robustness. Experimental results indicate that

the proposed method is not only highly competitive, but also outperforms the existing methods. Localization algorithms, e.g., the Dead Reckoning, the maximum likelihood estimation (MLE) and the Sequential Bayesian estimation (SBE). To the best of our knowledge, the reference is the first survey focusing on MWSNs localization.

M.S. Lin et al. [9] presents a reversible data-hiding scheme for medical images. This method uses three neighboring pixels to predict the current pixel. For the prediction error, two histograms, *h1*and *h2*, are generated. The distribution in histogram *h1* and *h2* is more compact. The algorithm intends to embed secret data into the cover image by using the modification of the two histograms *h1*and *h2* instead of the original image histogram. The proposed method has the advantages like the stego-images have good visual image quality and has a higher pure payload**.**

L. Dong et al [10], proposed a novel reversible image data hiding method (RIDH). In this paper two class SVM classifier is designed to separate out encrypted and non-encrypted patches of images. This method provides higher embedding capacity and it also able to reconstruct original image and embedded message. Mainly, RIDH algorithm is designed for plaintext documents. In this message bits are embedded into the original image hence we can say that it works for lossless compression algorithm for compression certain features of images. The DE i.e. different expansion method improves the prediction error expansion (PEE)-based strategies which offers the state-of-the-art capacity distortion performance. The proposed two-class SVM classifier can efficiently separate outs the encrypted and non-encrypted patches of image.
Zhang et al. [11], discussed about separable reversible data hiding in encrypted images. There are two phases in which firstly, content owner encrypts the original uncompressed image using keys by which encryption is required. In this paper, proposed method content owner encrypts the original uncompressed image using encryption key.

Mark Johnson and et.al [12] has examined the possibility of first encrypting a data and then compressing it, such that the compressor does not have knowledge of the encryption key. The encrypted data can be compressed using distributed source coding principles, because the key will be available at the decoder. They showed that under some conditions the encrypted data can be compressed to the same rate as the original, unencrypted data could have been compressed.
Li Donget al. [13] proposed another reversible data hiding scheme over encrypted images. The data embedding is achieved through a public key modulation mechanism and so there is no need of a secret key. There is a powerful two class SVM classifier at the receiver side to distinguish between encrypted and non-encrypted image patches and it also allows to jointly decoding the embedded message and the original image. The data embedding is done by simple XOR operations, without the need of accessing the secret key.

Y. Shi et al.[14] have proposed a system that performs the Reversible Data hiding by using the histogram shift operation for RDH. In this system used the spare space for embedding the data by shifting the bins of gray scale values. The embedding capacity measured by the use of number of pixels in peak point. This system has some benefits such as it is simple and has constant PSNR ratio, capacity is high and distortion is very low. This system has some disadvantages such as more time consuming while searching the image number of times.
A. R. Gaykar et al. [15] a new reversible data hiding algorithm has been proposed with the property of contrast enhancement. The proposed method can take advantage of all traditional RDH techniques for plain images and achieve excellent performance without loss of perfect secrecy. For better visibility improving the algorithm and applying it to the medical and satellite images becomes the part of the system. Is a survey paper on Reversible Image Data Hiding The proposed algorithm has made the image contrast enhancement reversible.

III.PROPOSED METHDOLOGY

Our proposed method a robust image encryption histogram shifting method (RIEHM)based on bit shifting using data hiding in encrypted image based on bit shifting histogram and proposed method a is robustness is good as compare existing method block histogram shifting (BHS).our proposed method base on bit shifting through in histogram shifting method. Different image using jpg format and experimentation images like parrot image in jpg and size 75.2 KB as a host image and fifa image as data image in jpg size 28.1KB and experimentation images like road_forest_trees_nature image in jpg and size 259 KB as a host image and toyota-Logo-3D image as data image in jpg size 20KB.The proposed scheme consists of three steps. In the first step, the ownership of the host image encrypts the image by using a suitable encryption in bit change by histogram shifting. In the second step, the data image hides the data by host image by using another data image hiding through into host image. In the third step, host image and data image both are embedding well-built and generated the watermarked image. In the forth step, extract data image into watermarked image. The receiver

can access the data image as well as reconstruct the data image by using the respective decryption. Finally in the fifth step, generate output. The proposed framework aims to perform three main operations. Encrypted image generation, Data embedding in encrypted image, Data extraction and image recovery. First two operations will be performed at transmitter side and third will be at receiver side. The block diagram of the proposed work is shown in Figure1

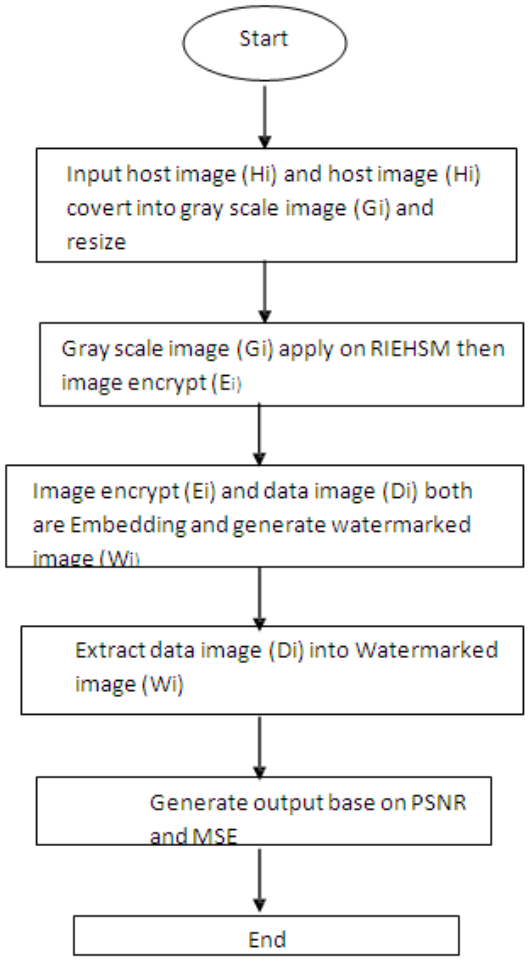

Figure 1 : Proposed methodology block diagram

IV .RESULT ANALYSIS

A proposed method represent mathematical model to improve privacy of secret data. In this method, security model work between data sender and data receiver. Even though, server is not trusted then also data sender secret message will be in safe during data transmissions. It displays following model separately such as Mean Squared Error (MSE) and Peak Signal Noise Ratio (PSNR).

Different image using jpg format and experimentation images like parrot image in jpg and size 75.2 KB as a host image and fifa image as data image in jpg size 28.1KB

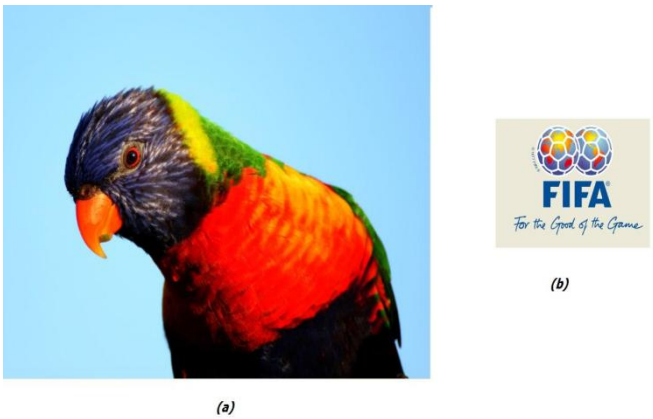

Figure 2 : (a) PARROT host image, (b) FIFA image data image

The PSNR (Peak Signal to Noise Ratio) value, MSE (Mean Squared Error) of the three images (RGB, GREYSCALE, BLACK and WHITE) using pervious work and proposed work techniques is obtained. The corresponding results for these parrot image and fifa image are shown in table 1 shows the PSNR and MSE value obtained for parrot image and fifa image. The proposed system uses RIEHSM technique which shows the maximum PSNR and less MSE obtained compared with the existing system

Table 1 :MSE and PSNR value of existing method and proposed method

METHOD	MSE	PSNR
BHS	0.0304	35.22
RIEHSM	0.0116	44.82

V. CONCLUSION

Our proposed method an image encryption histogram shifting method (RIEHSM) based on bit shifting using data hiding in the encrypted image based on bit shifting histogram and proposed method a is robustness is good as comparing existing method block histogram shifting (BHS). The technique should be part of a complete image encryption system and its aim is to eliminate the effectiveness of attacks which explore the frequency of occurrence of the pixels values. This kind of attack may be useful against encryption techniques based on changes on pixels positions or transformations which do not alter significantly the histogram of an image. Simulations which indicate that the proposed scheme has potential applicability in practical scenarios were presented. Procedures dependent on a histogram shifting method with the purpose of implementing a complete image encryption method. This work proposes an improved robustness in the data hiding in encrypted images by RIEHM (image encryption histogram shifting method) based on bit shifting. This work provides full protection for the image as well as the data by using histogram shifting.. Compared to the other existing BHS methods, the proposed method highly improves the embedding rate, as well as the PSNR of the image, is also good.

REFERENCES

[1]. M.U. Celik, G. Sharma, A.M. Tekalp, and E. Saber, "Lossless generalized-lsb data embedding," Image Processing, IEEE Transactions on, vol. 14, no. 2, pp. 253–266, Feb 2005.

[2]. M. A. Suhail and M. S. Obaidat, "Digital watermarking-based DCT and JPEG model," IEEE Trans. on Instrumentation and Measurement, vol. 52, no. 5, pp. 1640–1647, October 2003.

[3]. J. Fridrich, Steganography in Digital Media: Principles, Algorithms, and Applications, Cambridge University Press, 1st edition, 2009.

[4]. I. J. Cox, M. L. Miller, and J. A. Bloom, Digital Watermarking and Steganography, Morgan Kaufmann, 2nd edition, 2007.

[5]. NutanPalshikar, Prof. Sanjay Jadhav, " Lossless Data Hiding using Histogram Modification and Hash Encryption Scheme",International Journal of Emerging Technology and Advanced Engineering,ISSN 2250-2459, Volume 4, Issue 1, 2014.

[6]. MithuVarghese,Teenu S Jhon, " A Survey on Separable Reversible Data Hiding in Encrypted Images", International Journal of Computer Applications Advanced Computing and Communication Techniques for High Performance Applications ,0975 – 8887,2014.

[7]. M.S Hwanga , L.Y. Tsengb ,LC Huang, "A reversible data hiding method by histogram shifting in high quality medical images", Journal of Systems and Software, Vol. 86, (3), pp. 716–727, 2013.

[8]. B.Lei, E.L.Tan, S.Chen, D.Ni, T.Wang, H.Lei, "Reversible watermarking scheme for medical image based on differential evolution", Expert Systems with Applications, Vol. 41, (7), pp. 3178–3188, 2014.

[9]. S.C. Huang, M.S. Lin, "A High-capacity Reversible Data hiding Scheme for medical images", Journal of Medical and Biological Engineering, Vol. 30, (5), pp. 289-296, 2010.

[10]. J. Zhou, W. Sun, L. Dong, et al., "Secure reversible image data hiding over encrypted domain via key modulation," IEEE Trans. on Circuits and Systems for Video Technology, vol. 26, no. 3, pp. 441-452, Mar. 2016.
[11]. X. Zhang, "Separable reversible data hiding in encrypted image," IEEE Trans. on Information Forensics and Security, vol. 7, no. 2, pp. 826-832, Apr. 2012.
[12]. M. Johnson, P. Ishwar, V.M. Prabhakaran, D. Schonbergand K. Ramchandran, "On compressing encrypted data," IEEE Trans. Signal Process., vol. 52, no. 10, pp. 2992-3006, Oct. 2004.
[13]. Jiantao Zhou, Weiwei Sun, Li Dong,Xianming Liu, Oscar C. Au,and Yuan Yan Tang, "Secure Reversible Image Data Hiding over Encrypted Domain via Key Modulation", IEEE transactions on circuits and systems for video technology,2015.
[14]. 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.
[15]. Ashwini R. Gaykar and Prof. S. M. Rokade, "Data Hiding with contrast enhancement by using RDH Algorithm", International Journal of Engineering Development and Research, Vol.4, Issue-1, pp.145-149, May-June 2016.