International Journal of Innovative Research in Technology and Science
ISSN: 2321-1156 www.ijirts.org Volume 10 Issue 4, July 2022

Enhanced Reversible Data Hiding in Encrypted Image Based on Two-Layer Pixel Errors Block Histogram Method and EFRBSM

Arunendra Pandey[1], Santosh Kumar[2], Seema Shukla[3]
Department of EC, MITS, RGPV, Bhopal, India
arunendrapandey123@gmail.com, santoshkumar@gmail.com, seematiwari.a@gmail.com

ABSTRACT: Enhanced reversible data hiding in encrypted image based on two-layer pixel errors block histogram and error-free reversible bit shifting method (EFRBSM). Error-free reversible bit shifting method to reversible the marked media back to the initial cover media when the hidden information was extracted. Information security and information integrity are difficult in image processing areas, and several types of research are progressing in the sector, like web security. The necessity of secure transmission of knowledge is very important in our life. Image transmission is one in each application that must be securely transmitted over the unfaithfulness network. This approach consists of dividing the image into blocks and applying the existing process to each block in a recursive manner. Simulations of the procedure show that the histogram of the transformed image exhibits a uniform shape and its pixels have a low correlation with their neighbours. Image data convert into a histogram, and secreted data is also converted into a histogram. Both are embedded into an encrypted image histogram. Two-layer pixel errors block histogram method in the encrypted image is a powerful technique for the security of .data formation concealing in scrambled pictures gives twofold security to the information, for example, picture encryption and information stowing away. The two-layer pixel blunders block histogram strategy contains a few issues, so they need to eliminate the issues by joining lossless and reversible procedure implies, information extraction and recuperation of picture are mistake-free. Error-free reversible information hiding in an encrypted image supported two-layer element errors based on block histogram method is low PSNR in particular, the existing scheme divides the initial image data into a sequence of non-overlap blocks, permutes these blocks. In the existing scheme, the histogram of two-layer adjacent encrypted element errors to insert secret information by histogram shifting and generate a marked histogram encrypted image, the information embedded is and also extracted data with error. Our proposed unique method (EFRBSM) termed reversible information activity like improving PSNR and reducing MSE.

Keywords: Reversible Data Hiding Block Histogram Shifting, Image Encryption, Image Decryption, Original Image Data Recovery, PSNR, MSE, Data Embedding, Error-Free Reversible Bit Shifting Method.

I. INTRODUCTION

Nowadays, the distribution of transmission content on the Internet and different communication networks has become observed typically performed by users with totally different profiles. During this Situation, techniques dedicated to defending this type of data play a vital role, providing confidential transmission and reassuring the integrity of the received information. These are a number of the explanations why the interest in finding watermarking, steganography and encoding for digital image, video and audio has enhanced over the years. Newer strategies of RDH in encrypted pictures will be classified into 2 classes – joint strategies during which information extraction and image recovery are performed together, and divisible strategies during which image decoding and information extraction will be performed severally [1]. A digital image has been enhanced quickly on the web. Security becomes progressively necessary for several applications, including confidential transmission, video police work, and military and medical applications. The transmission of pictures may be a daily routine, and it's necessary to search out an efficient way to transmit them over networks. In order to decrease the TRM, information compression is important. Compression conjointly helps to scale back the space for storing. The protective digital pictures will be through with encoding or information concealing algorithms. For a few years, the problem is to mix compression, encoding and information hiding in a single step. A replacement challenge consists of inserting information into encrypted pictures. They can insert information in an encrypted image by exploiting an associate degree irreversible approach of information hiding. Since the entropy of encrypted images is the largest, the embedding step, thought-about like noise, isn't potential by exploitation of normal information hiding algorithms. As a result of the supply of powerful image-process package packages like Photoshop, anyone will modify such digital media for any reason and make unconscious forgeries. The way to stop a medical image from being maliciously altered is to detect the tampered elements, which has become a very important issue. So as to safeguard digital pictures, image authentication schemes are the foremost

comprehensive technique. Generally, the authentication codes are sometimes derived from the distinguished options of the medical image and are directly embedded into the image. However, the embedding procedure can distort the pictures. This distortion might cause the changed medical pictures to be unable to be used for any designation. A replacement plan is to use reversible information hiding algorithms on encrypted pictures with the wish to get rid of the embedded information before the image coding; that's to mention, the strategy should have the flexibility to restore the initial content once the extraction of the authentication codes. Therefore, it's a very important challenge to develop a reversible information-hiding scheme for encrypted medical pictures to get rid of the embedded data throughout the encoding step [2].

The general method of RDH

Encryption and information hiding are two effective means of information protection. Whereas the encoding techniques convert plaintext content into indecipherable cypher text, the information the hiding techniques implant extra data into cover media by introducing slight modifications. There is a variety of schemes that performs information concealing and cryptography conjointly. Completely different ways are wont for information to be hidden. However, information hiding in pictures causes damages to the first image and the embedded information throughout extraction. It's possible within the applications like cloud storage and medical systems**.**

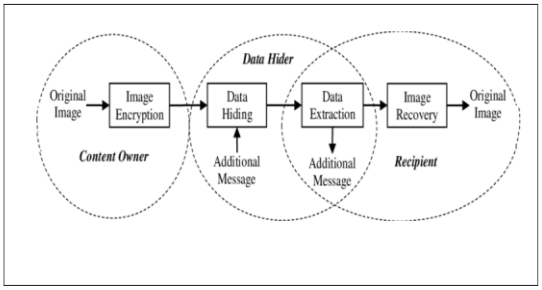

Figure 1 Reversible information hiding method

An overall read of the Reversible information hiding method represents the image and D, the information to be hidden. These 2 pieces of information are fed into the implant block that hides the message bits into the image. ID pictures this image. Once ID is fed into the extract/reverse block produces the first image when extracting the information. The rebuilt image IR is the same because the original image [3].

The separable reversible data hiding method proposes a unique scheme for divisible reversible knowledge hiding in encrypted pictures [4]. Within the projected methodology, a content owner (sender) encrypts the first uncompressed image victimization with an encoding key. Then, a piece of knowledge or an information {hider might compress the smallest number of vital bits of the encrypted image, employing a key referred to as a data-hiding key to make a distributed area to accommodate further data. Currently, with a picture, i.e. the encrypted image containing the extra information, if the receiver includes a data-hiding key, he will extract the extra knowledge though' he doesn't have a thought regarding the first image content [5]. If the receiver at the destination has an encoding key, then the receiver will decode the received knowledge to get the image just like the first image to be transferred; however, the receiver cannot extract the extra knowledge. Suppose the receiver has each the keys i.e. data-hiding key and therefore the encoding key. In that case, the receiver will extract the extra information, which might even be known as a watermark and recover the image, i.e. the first content of the image with no bugs or any error by exploiting the abstraction correlation, abstraction area in the original or natural image once the quantity of further knowledge or the watermark isn't overlarge. The scheme projected during this paper is created from image encoding, information embedding and data-extraction/image-recovery phases. The sender, conjointly referred to as the content owner, encrypts the first uncompressed image victimization of the image encoding algorithms and employs a key referred to as the encoding key to provide an encrypted image. Then, the knowledge or the data hider compresses the smallest number of vital bits of the encrypted image employing a data-hiding key for making a distributed area to store the extra data or the watermark information. At the destination facet, {the knowledge or the information embedded within the image is often retrieved simply from the encrypted image containing further data per the data-hiding key.

Since the embedding of information only affects decoding the image with an encoding key may result in a picture that's just like the first version of the image. Once each key is utilized by the receiver, i.e. the encoding and data-hiding keys, the extra knowledge embedded is often extracted with success. Therefore the original image is often recovered utterly by exploiting the special correlation in the natural image. The disadvantage of this method was eliminated by proposing a replacement theme referred to as the severable reversible information hiding scheme. This technique proposes the scheme of severable reversible information hiding by removing the disadvantages of the non-divisible scheme [6].

II.RELATED WORK

Mehrzad Khederzdeh et al. [7] present a new Lossless Secure data embedding algorithm in which the vital information can be embedded into the cover

image while maintaining the security of the data to be embedded and preserving the quality of the cover image. Here, during the data embedding process, the two main issues that need to be considered cover image quality and embedded data security. SDEM-DCT (Scramble Data Embedding in Mid-frequency range of DCT) Algorithm consists of three major security levels. This level can hide the Credit Card Numbers of many customers inside the bank LOGO. It proposes a high-capacity data hiding method. Also, introduce robust Scramble and Descramble Data embedding algorithms named MK randomize key Generator to have more Security for embedded data. This method is securer than most of its predecessors. Finally, the results show that our method provides acceptable image quality and adjustable embedding capacity. Also, show that the distortion of the stego-image caused by this method at low embedding capacity is the same as that of other algorithms.

Rintu Jose et al. [8], the image owner first encrypts the image by permutation, using an encryption key. Since permutation only shuffles the pixels, the histogram of the image remains the same. Without knowledge about the original image content, the data hider hides data into the encrypted image by histogram modification method. Before hiding the data, the data hider permutes the image using the data hiding key, and after data hiding, he performs inverse permutation. On the receiver side, if the receiver has only a data hiding key, he can extract the data, but cannot read the image's content. If he has the only encryption key, he can decrypt the image to get an image similar to the original one. If he has both keys, he may extract the data using the data hiding key and then decrypt the image using an encryption key. This decrypted image is exactly the same as the original image.

Z. Ni et al. [9] Data are hiding as a process to hide data (representing some information) into cover media. That is, the data hiding process links two sets of data, a set of the embedded data and another set of the cover media data. The relationship between these two sets of data characterizes different applications. For instance, the hidden data in covert communications may often be irrelevant to the cover media. In authentication, however, the embedded data are closely related to the cover media. In these two types of applications, the invisibility of hidden data is an important requirement. In most cases of data hiding, the cover media will experience some distortion due to data hiding and cannot be inverted back to the original media. That is, some permanent distortion has occurred to the cover media even after the hidden data have been extracted. In some applications, such as medical diagnosis and law enforcement, it is critical to reverse the marked media back to the original cover media after the hidden data are retrieved for some legal considerations. In other applications, such as remote sensing and high-energy particle physical experimental investigation, it is also desired that the original cover media can be recovered because of the required high-precision nature. The marking techniques satisfying this requirement are reversible, lossless, distortion-free, or invertible data hiding techniques. Reversible data hiding facilitates the immense possibility of applications linking two sets of data so that the cover media can be losslessly recovered after the hidden data have been extracted, thus providing an additional avenue of handling two sets of data.[1]

Zhaoxia Yin et al. [10] Proposed and evaluated a new separable RDHEI framework. Additional data can be embedded into a cypher image previously encrypted using Josephus traversal and a stream cypher. A Block histogram shifting (BHS) approach using self-hidden peak pixels is adopted to perform reversible data embedding. Depending on the keys held, legal receivers can extract only the embedded data with the data hiding key, or they can decrypt an image very similar to the original image with the decryption key. They can extract both the embedded data and recover the original image error-free if both keys are available. The results demonstrate higher data embedding capacity, better decrypted-marked-image quality, error-free data extraction and accurate image reconstruction.

W. Hong et al. [11] There are two phases in separable reversible data hiding in encrypted images. In the first phase, a content owner encrypts the original uncompressed image using an encryption key. Then, the data-hider may compress the least significant bits of the encrypted image using a data-hiding key to create a sparse space to accommodate additional data. With an encrypted image containing additional data, if a receiver has the data-hiding key, he can extract the additional data though he does not know the image content. If the receiver has the encryption key, he can decrypt the received data to obtain an image similar to the original one but cannot extract the additional data. If the receiver has both the data-hiding key and the encryption key, he can extract the additional data and recover the original content without any error by exploiting the spatial correlation in the natural image when the additional data is not too large.

D. M. Thodi et al. [12] propose a histogram shifting technique as an alternative to embedding the location map. The proposed technique improves the distortion performance at low embedding capacities and mitigates the capacity control problem. They also propose a reversible data-embedding technique called

prediction-error expansion. This new technique better exploits the correlation inherent in the neighbourhood of a pixel than the difference-expansion scheme. Prediction-error expansion and histogram shifting combine to form an effective method for data embedding. The experimental results for many standard test images show that prediction-error expansion doubles the maximum embedding capacity compared to difference expansion.

H. M. Tsai et al. [13] first proposed a reversible visible watermarking scheme by modifying one significant bit plane of the pixels of the host image. They achieved reversibility via losslessly hiding the compressed version of the altered bit plane into the non-watermarked image region. However, this method's embedded, visible watermark appears to be somewhat blurred, and the visual quality of the original image is significantly distorted.

Ching-Yu Yanga et al. [14] propose a reversible data hiding by the coefficient-bias algorithm. A simple lossless data hiding method based on the coefficient-bias algorithm by embedding bits in both spatial and frequency domains is considered. In the spatial domain, each pixel in a host image is first subtracted from the block mean. Then, a stego image is generated by embedding many bits (or the primary message) in the mean-removed blocks via the coefficient-bias algorithm. The stego-image is transformed to frequency domain by integer wavelet transform (IWT) to provide extra security and robustness. This algorithm hides a secondary watermark in the low-high (LH) and high-low (HL) sub-bands of the IWT domain. Simulations show that both the perceptual quality and hiding capacity are not bad. Moreover, the resultant images introduced by the method are tolerant of the attacks such as JPEG2000, JPEG, brightness, and inverting.

Shuang Yi et al. [15] performed original work randomly selects pixels from an original image to obtain the estimation error for secret data embedding. In this work, we estimate half of the pixels in the original image to obtain the estimation error so that the maximum embedding rate can be significantly improved while keeping a high image quality of the marked decrypted image. This method is first to estimate a part of the pixels in an original image using the rest pixels and obtain the estimation errors. Then we encrypt the estimation errors and the rest pixels. The data hider then embeds the secret data into the encrypted estimation errors and scrambles the image using the sharing key. On the receiver side, the secret data and Original image can be extracted and recovered separately using different security keys.

Chunqiang Yu et al. [16] Reversible data hiding is an important topic of data hiding. This paper proposes novel, separable, error-free, reversible data hiding in an encrypted image based on two-layer pixel errors. Especially, the proposed scheme divides the original image into a series of non-overlapped blocks and permutes these blocks. Then, a closed Hilbert curve is used for scanning each block to obtain a one-dimensional pixel sequence. The pixels of the sequence are encrypted with the key transmission. During data hiding, each non- overlapped block of the encrypted image is scanned in the closed Hilbert order to generate a one-dimensional encrypted pixel sequence. Finally, it exploits the histogram of two-layer adjacent encrypted pixel errors to embed secret data by histogram shifting and generate a marked encrypted image. Many experiments are carried out, and the results demonstrate that the proposed scheme reaches a high payload and outperforms some reversible data hiding schemes in the encrypted image.

III. IMPLEMENTATION TOOL

Compare the proposed mechanisms with the existing algorithm. The experiment is performed on a laptop with an Intel Dual Core processor (1,836 Hz), 2 GB of memory and a Windows 7 final system. Here, this method is applied and simulated in MAT LAB 7.8.0, and for this work, we use the Intel machine 1.4 GHz with the operating system Windows 7, Windows-x. The performance analysis of MATLAB version 14 (R2008a) used for this thesis Mining provides libraries optimized for processors for rapid execution and computation and is performed in Data Cancer Data. The JIT compilation technology (just in time) provides execution speeds that rival traditional programming languages. It can also be an advantage of multi-core computers and multiprocessors; MATLAB provides many alerts and multi-process numerical functions. These functions automatically run on multiple computer threads during a single MATLAB, running faster on multi-course computers. During this thesis, all improved results of effective data recovery were performed in MATLAB 14 (R2008b). It is the high-level language and interactive background used by many universal engineers and scientists. It allows exploring and visualizing ideas and working together in different disciplines to process signals and images, messages and results calculations. MATLAB provides applications to obtain, analyze and film data, which allows you to obtain information about your data during a split of the time you can take using spreadsheets or traditional programming languages. You can also document and share the results of plots and reports or as a published MATLAB code. Matrix Lab can be a paradigm of multiple conditions to compute inventions of numerical programming and 4th language. It is developed by mathematical work;

MATLAB allows matrix strategies, function and data tracking, algorithm implementation, interface building and user programs.

IV. RESULT ANALYSIS

In research in field image processing in error-free reversible data hiding in encrypted image based on two-layer pixel errors using histogram shifting and protected image data and reversible data hiding into the image using Histogram shifting: secure data image and more authentications.

(a) Comparison Graph between Existing scheme TLEBHS and New scheme EFRBSS

Table1 Comparison analysis between existing scheme (TLEBHS) and new scheme (EFRBSS) in case1.

Scheme	MSE	PSNR
TLEBHS	0.002097	61.89
EFRBSS	0.000377	79.056

Comparison analysis between existing scheme (TLEBHS) and new scheme (EFRBSS) shows result graph and find existing technique TLEBHS low PSNR and high MSE another hand new technique EFRBSS high PSNR and low MSE. All output values are shown in table 1 and the graph in fig2.

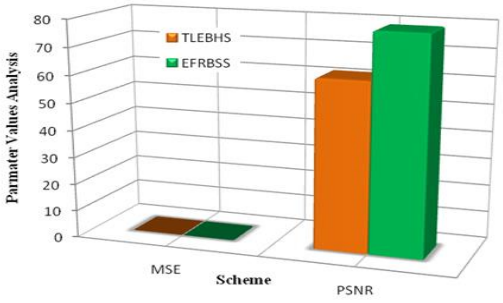

Figure 2 Comparison graph Based on PSNR and MSE in case1

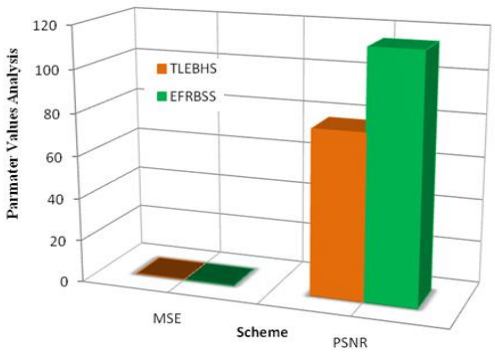

Fig3 Comparison graph Based on PSNR and MSE in case2

(b) Comparison Graph between Existing scheme TLEHS and New scheme EFRBSS

Table 2 Comparison analysis between existing scheme (TLEBHS) and new scheme (EFRBSS) in case2.

Scheme	MSE	PSNR
TLEHS	0.000496	77.252
EFRBSS	1.19E-05	114.59

Comparison analysis between existing scheme (TLEBHS) and new scheme (EFRBSS) shows result graph and find existing technique TLEBHS low PSNR and high MSE another hand new technique EFRBSS high PSNR and low MSE. All output values show in table.2 and also shown graph in fig3.

V. CONCLUSION

Enhanced reversible data hiding in encrypted image based on two-layer pixel errors block histogram method and error-free reversible bit shifting method (EFRBSM). Reversible information is hiding in encrypted image data and, therefore, three steps. In the step first, a content owner encrypts the image with the help of an encryption key. Step second, a data-hider uses a data-hiding key and compresses the encrypted image. Last step third additional data is extracted, and the original image is recovered. The activities of extracting the additional data and recovering the original images depend on the key the receiver possesses. Now presenting block histogram method, there is the separation of these two activities like PSNR low and MSE high according to availability of keys using image encryption algorithms has certain demerits. Previous strategies implement RDH in encrypted pictures. It is also known as error-free reversible information hiding in encrypted image-supported two-layer picture element errors. Therefore, the information hider will get pleasure from the other house empty move into the previous stage form data hiding method easy. The block histogram method will make most ancient RDH techniques for image data and reach glorious performance with loss and not perfect secrecy, therefore low PSNR.

Moreover, this proposed unique method (EFRBSM) can do real changeability, separate information extraction, and significantly improve the marked decrypted image standard. In existing systems, there's no provision for efficient security. Therefore, it's necessary to develop an efficient and effective system that gives information embedding and recovery with none distortion and provides higher security. Our proposed unique method (EFRBSM) termed reversible information activity like improve PSNR and reduce MSE, experimental using different pictures taken that is employed mat lab tool.

REFERENCES

[1]. C.-P. Wu and C.-C. Jay Kuo, "Design of integrated multimedia compression and encryption systems," IEEE Transactions on Multimedia, vol. 7, no. 5, pp. 828–839, October 2005.

[2]. Mithu Varghese, Teenu S Jhon, "A Survey on Separable Reversible Data Hiding in Encrypted Images", International Journal of Computer Applications (0975 – 8887) Advanced Computing and Communication Techniques for High-Performance Applications, ICA-CCTHPA-2014.

[3]. Rathika R, S. Kumaresan "Survey on reversible data hiding techniques" Advanced Computing and Communication Systems (ICACCS), 2016 3rd International Conference, Pages:1-4, 2016.

[4]. C. Candan. A Transcoding Robust Data Hiding Method for Image Communication Applications. IEEE International Conference on Image Processing, 2005, vol.3: 660-663.

[5]. Puech, William, Marc Chaumont, and Olivier Strauss. "A reversible data hiding method for encrypted images." Security, Forensics, Steganography, and Watermarking of Multimedia Contents X. Vol. 6819. International Society for Optics and Photonics, 2008.

[6]. M. Ashourian, P. Moallem, Y. S. Ho. A Robust Method for Data Hiding in Color Images. Lecture Notes in Computer Science, 2005, vo!.3768: 258-269.

[7]. Dr Mohammad V. Malakooti, Mehrzad Khederzdeh,'" A Lossless Secure Data Embedding In Image Using DCT and Randomize Key Generator " IEEE 2012.

[8]. 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.

[9]. Rintu Jose, Gincy Abraham "A Separable Reversible Data Hiding in Encrypted Image with Improved Performance" IEEE International Conference on Microelectronics, Communication and Renewable Energy (ICMiCR), pp. 1-5, 2013.

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

[11]. Zhaoxia Yin, Andrew Abel, Xinpeng Zhan, Bin Luo "Reversible Data Hiding In Encrypted Image Based On Block Histogram Shifting" Acoustics, Speech and Signal Processing (ICASSP), 2016 IEEE International, pp. 2129-213, 2016.

[12]. 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.

[13]. D.M. Thodi and J. J. Rodriguez, "Expansion embedding techniques for reversible watermarking," IEEE Trans. Image Process., vol. 16,no. 3, pp. 721–730, Mar. 2007.

[14]. H. M. Tsai and L. W. Chang, "A high secure reversible visible watermarking scheme," in Proc. IEEE Int. Conf. Multimedia Expo, Beijing, China, pp. 2106–2109, 2007.

[15]. Ching-Yu Yanga, Wu-Chih Hua and Chih-Hung Lin, "Reversible Data Hiding by Coefficient-bias Algorithm", Journal of Information Hiding and Multimedia Signal Processing, Volume 1, Number 2, April 2010.

[16]. Shuang Yi, Yicong Zhou" An Improved Reversible Data Hiding In Encrypted Images" Signal and Information Processing (ChinaSIP), 2015 IEEE China Summit and International Conference on, pp. 225-229, 2015.

[17]. Yu, Chunqiang, et al. "Separable and error-free reversible data hiding in encrypted image based on two-layer pixel errors." *IEEE Access* 6: 76956-76969, 2018.