International Journal of Current Trends in Engineering & Technology
www.ijctet.org, ISSN: 2395-3152
Volume: 07, Issue: 01 (January-February, 2021)

Review on Error-Free Reversible Data Hiding in Encrypted Image Based on Two-Layer Pixel Errors block Histogram Shifting Method

Arunendra Pandey, Santosh Kumar, Seema Shukla
Department of Electronic Communication
MITS, RGPV, Bhopal, India
arunendrapandey123@gmail.com

***ABSTRACT**:* Reversible information hiding may be a method to reverse the marked media back to the initial cover media when the hidden information was extracted. Information security and information integrity are the 2 difficult areas for analysis. Numerous researches are progressing on the sector like web security. The necessity of secure transmission of knowledge is very important in our life. Image transmission is one in each of the applications that must be securely transmitted over the fraudulence network. During this, technical data to be transferred is embedded into an encrypted image. This paper proposes unique severable and error-free reversible information hiding in an encrypted image supported two-layer element errors. Especially, the projected scheme divides the initial image into a series of non-overlapped blocks and permutes these blocks. The bar graph of two-layer adjacent encrypted element errors to insert secret information by bar graph shifting and generate a marked encrypted image; the information embedded is extracted with none error.

Additionally, the cover image is remodelled error-free. This kind of techniques is termed Reversible information activity. Here may be a review on completely different information hiding techniques in the encrypted image, and our projected methodology (EFBHSM) improves PSNR and Minimize MSE.

Keywords: Reversible data hiding block Histogram Shifting, Image encryption, Image decryption, original image data recovery, PSNR, MSE, data embedding.

I. INTRODUCTION

Nowadays, the distribution of transmission content on the Internet and different communication networks became a observe 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 out 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 enhanced quickly on the web. Security becomes progressively necessary for several applications, confidential transmission, video police work, 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. 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 in encrypted pictures. They can insert information in an encrypted image by exploitation the associate degree irreversible approach of information hiding. Since encrypted image entropy is the largest, the embedding step, thought-about like noise, isn't potential by exploiting normal information hiding algorithms. As results 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, detection of the tampered elements, has become a very important issue. To safeguard digital pictures, image authentication schemes are the foremost wide used technique. Generally, the authentication codes are sometimes derived from the medical image's distinguished options 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 uses reversible information hiding algorithms on encrypted pictures to eliminate the embedded information before the image coding. That's to mention, and the strategy should have the flexibility to restore the initial content once the authentication codes are extracted. Therefore, it's a very important challenge to develop a reversible information-hiding scheme for medical pictures encrypted pictures to eliminate the embedded data throughout the encoding step [2].

The general method of RDH

Encryption and information hiding are two effective means that of information protection. Whereas the encoding techniques convert plaintext content into indecipherable ciphertext, 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 to information hide. However, general information hiding in pictures causes damages to the first image and the embedded information throughout extraction. It's possible within applications like cloud storage and medical systems.

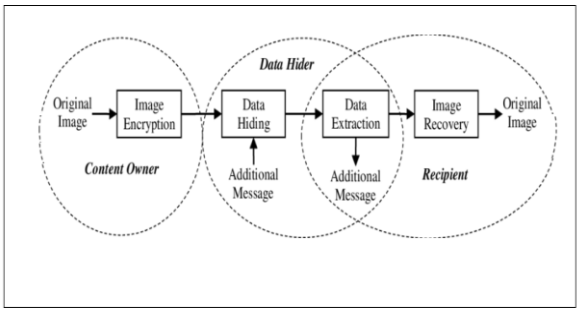

Figure 1 Reversible information hiding method

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

Separable reversible data hiding Method: this method proposes a unique scheme for divisible reversible knowledge hiding in encrypted pictures [4]. A content owner (sender) encrypts the first uncompressed image victimization an encoding key within the projected methodology. A 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. 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. However,' he doesn't think regarding the first image content [5]. Suppose the receiver at the destination has an encoding key. In that case, the receiver will decode the received knowledge to get the image just like the first image that's to be transferred. However, the receiver cannot extract the extra knowledge. Suppose the receiver has each of the keys, i.e., the data-hiding key and the encoding key. In that case, the receiver will extract the extra information, which might even be known as watermark and recover the image, i.e., the first content of the image with none 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 the image encoding algorithms and employing a key referred to as the encoding key to provide an encrypted image. 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 are often retrieved simply from the encrypted image containing further data per the data-hiding key. Since the embedding of information only affects, a decoding of the image with an encoding key may result in a picture 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 are often extracted with success. Therefore, the original image is often recovered utterly by exploiting the special correlation in natural image. This method's disadvantage 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] this paper presents a new algorithm of 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. During the data embedding process, the two main issues of cover image quality and embedded data security need to be considered. SDEM-DCT (Scramble Data Embedding in Mid-frequency range of DCT) Algorithm consists of three major security levels. This level can be used to 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 called 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 indeed provides acceptable image quality and adjustable embedding capacity. Also, showing the distortion of the stego-image caused by this method at low embedding capacity is similar to that of other algorithms.

Rintu Jose et al. [8]. The owner of the image first encrypts the image by permutation, making use of an encryption key. Since permutation only shuffles the pixels, the histogram of the image remains the same. Without any knowledge about the original image content, the data hider hides data into the histogram modification method's encrypted image. 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 first extract the data using the data hiding key and then decrypt the image using an encryption key. This decrypted image is the same as the original image.

Z. Ni et al. [9] Data were 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 another set of the cover media data. The relationship between these two sets of data characterizes different applications. For instance, in covert communications, the hidden data 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 data hiding cases, 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 out. 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 is retrieved for 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 applications' immense possibility to link two sets of data so that the cover media can be losslessly recovered after the hidden data have been extracted out, thus providing an additional avenue of handling two different 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 decrypt an image 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] Inseparable reversible data hiding in encrypted images; there are two phases. 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 some 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. Suppose the receiver has both the data-hiding key and the encryption key. In that case, 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 amount of additional data is not too large.

D. M. Thodi et al. [12] proposes 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 of the host image's pixels. They achieved reversibility via losslessly hiding the compressed version of the altered bit plane into the non-watermarked image region. However, the embedded, visible watermark with this method appears to be somewhat blurred, and the visual quality of the original image is significantly distorted.

Ching-Yu Yanga et al. [14] propose reversible data hiding by a coefficient-bias algorithm. A simple lossless data hiding method based on the coefficient-bias algorithm by embedding bits in both the spatial and frequency domain 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 a large number of bits (or the primary message) in the mean-removed blocks via the coefficient-bias algorithm. The stego-image is transformed into the frequency domain by integer wavelet transform (IWT) to provide extra security and robustness. A secondary watermark is hidden 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 method's resultant images are tolerant of the attacks such as JPEG2000, JPEG, brightness, and inverting.

Shuang Yi et al. [15]. The 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 original image's pixels to obtain the estimation error. 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. The secret data and Original image can be extracted and recovered separately using different security keys at the receiver side.

Chunqiang Yu et al. [16] Reversible data hiding is an important topic of data hiding. This paper proposes a novel separable and 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 pixel sequence is 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.EXPECT OUTCOME

In research in field image processing in error-free reversible data hiding in the 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.

IV. CONCLUSION

Reversible information hiding in encrypted pictures and, therefore, the privacy-preserving needs from cloud information management. 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 additional house empty move into the previous stage form data hiding method easy. The planned technique will make most ancient RDH techniques for pictures and reach glorious performance with loss and not excellent secrecy, therefore low PSNR.

Moreover, these novel techniques can do real changeability, separate information extraction, and greatly 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 planned technique (EFBHSM) improves PSNR and Minimize 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 on, 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 International Conference on, pp. 225-229, 2015.

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