Mathematical Statistician and Engineering Applications
ISSN: 2094-0343
DOI: https://doi.org/10.17762/msea.v70i2.2444

An Analysis of Reversible Data Hiding Techniques in Images

Richa Gupta
Asst. Professor, Department of Comp. Sc. & Info. Tech., Graphic Era Hill University, Dehradun, Uttarakhand India 248002

Article Info
Page Number:1549 - 1555
Publication Issue:
Vol 70 No. 2 (2021)

Article History
Article Received*: 05 September 2021*
Revised*: 09 October 2021*
Accepted*: 22 November 2021*
Publication*: 26 December 2021*

Abstract
The reversible data- hiding fashion conceals some sensitive information in an image for secure communication. Only an authorised party may decrypt the concealed communication and recreate the cover image. The strategies put forth by different experimenters haven't yet been suitable to reflect a picture with a high embedding rate and advanced reconstructed image quality. In this exploration, certain significant reversible data- caching strategies are addressed and a system is proposed that can enhance the quality of the reconstructed image, the embedding capacity, and the denoising of the image. This approach can offer a secret data transfer that's further authentic, private, and dependable. Keywords: Embedding rate, Encryption, Prediction error, PSNR, Reversible data-hiding, Steganography

I. Introduction

The development of technology has raised the significance of information transmission, especially digital images. The digital images can be used in colorful fields similar as military communication, medical field, advertising field, etc. These digital images have to be passed through the public sphere in a real- time script. The protection of this data from colorful conditioning that are illegal changing the content of the media, vicious uses of information, etc is of significant significance. Data concealing and the use of cryptography are the two primary methods that contribute most to improved communication security. In cryptography, the data that has been transformed into a form that cannot be deciphered is referred to as cypher data. This transformation takes place with the assistance of a secret key. During the process of data caching, the data is cloaked in some kind of cover train, such as an image, an audio recording, or a videotape, before being sent across the network. Cryptography pays attention to the security of the image while data hiding pays attention to the invisibility of the image. Hiding the actuality of secret data is the advantage that's main of hiding ways over cryptography. Certain operations use both encryption and data caching.

There are a few different methods for concealing sensitive information, the most common of which being digital watermarking, stenography, and reversible data hiding (RDH). The placement of a series of digital bits in a digital cover train is known as watermarking. This assists for the information regarding the brand. Steganography, also is a form of covert communication in which the image being transmitted is altered in such a way that only the person who sent it and the recipient to whom the message is addressed are able to recognise it.

The unnoticeability of hidden data makes the process of unearthing it significantly more difficult. In stenography, the cover train is meaningless after the birth of the secret data, but in RDH, the cover train also stores the information just like the secret data does. The RDH provides assistance

in embedding a relatively substantial quantity of data into an image in such a way that it is possible to reconstruct the initial image using the image that has been marked. Because of this, it is an excellent method for operations in which one wants to retrieve the original signal without suffering any loss after the data birth while simultaneously storing metadata in the cover train.

II. Literature Survey

W.Puechet.al in (1) proposed a reversible data caching system that can bed data in translated images which help us to recover the image that's original well as the retired data. Encoding and decoding processes are involved. The garbling algorithm consists of two way. Encryption and data embedding. Apply the AES encryption algorithm to the input image which is peak into certain blocks using a secret crucialk. Data can be bedded by using a bit negotiation system. The decoding algorithm also consists of two way. birth of the communication and decryption. To prize the communication, it's just enough to recoup the bits using the crucial k that's secret. But after the birth, the pixel that's original of the image can be lost. To avoid this, decryption can be done using original standard divagation function. The original standard divagation function of an translated image will be advanced than that of an image that's original. With this fact, the original image can be reconstructed. The advantage of this system is that it provides entropy that's high the information redundancy is veritably small which prevents several statistical attacks. The limitation of the system is that the embedding factor is 1 bit for 16 pixels.i.e, the cargo capacity is veritably lower and we can bed only a veritably quantum that's small of.

Vasiliy Sachnevet.al in(2) " Reversible watermarking algorithm using sorting and vaticination ", proposed a system that uses a rhombus pattern vaticination scheme for sorting. In this scheme, one- pixel value is prognosticated using the neighbouring pixels. A sorted row of vaticination crimes can be formed and these vaticination crimes can be expanded to hide a bit. The fashion that's sorting be used inorder to record the vaticination crimes with the help of the magnitude of original friction. There are two sets of pixels used. One is a fleck set for calculating predictors and another bone is cross set which is used for data caching. Variation in any set shall not affect another set. A histogram shift system is also incorporated then to ameliorate performance. The proposed system decreases position chart size, which increases the capacity. It can also avoid lapping problems caused by expansion and the histogram shift system enables low deformation. But the disadvantage is that the lack of encryption can lead to data loss.

X Zhanget.al in(3) proposed a scheme in which the content proprietor encrypts the image by using a XOR operation that's simple. also the translated image is divided into different blocks that arenon-overlapping each of them is again partitioned into 2 setss_0ands_1. The data hider also embeds fresh data into the translated image using a data- hiding key without knowing the original content. also three LSB bits ofs_0 will be flipped if the data to be bedded is 0. also flip three translated LSB bits ofs_1 and it'll be transmitted if the data to be bedded is 1. When the receiver receives the pronounced translated image, he may originally decipher it using the encryption key. According to the key that's data- caching he can further prize the bedded data with the help of a change function. Then, the lower the block size, the further fresh data can be bedded. still, the threat of the defeat of image bit and recovery birth is more.

Xiaolong Liet.al in(4) proposed a watermarking that's reversible by incorporating two new strategies in vaticination error discovery(PEE) which focuses on largely identified regions and pixels. Ie, Adaptive pixel and embedding selection. Conventional vaticination error discovery embeds data slightly, but then proposed a system that can adaptively bed 1 or 2 bits into expandable pixels according to the original complexity. This avoids pixel expansion with larger vaticination crimes and also it reduces the embedding impact by dwindling the outside revision to pixel values. In this, we elect pixels of smooth area for data embedding and leave pixels that are rough. A further sprucely distributed vaticination error histogram and a better visual quality of the watermarked image are the advantages of this system. The optimal embedding that's adaptive used for image partition is determined iteratively which is the limitation of the proposed system.

Xinpeng Zhanget.al in(5) " Divisible reversible data hiding in translated image ", uses a divisible reversible data caching system in which first the sender encrypts an image that's uncompressed an encryption key and it'll be transmitted. XOR operation is used then for Encryption. During transmission, a data hider can add secret data by compressing the Least Significant bits of the translated image which creates a space that's meager accommodate the data. In order to conceal the data, a data hiding key must be utilised. The receiver is able to recover the lost data and decipher the image by making use of the appropriate keys in the event of any loss. The benefit of using this method is that it employs data contraction that is lossless and can do data separation with no data being lost in the process. Due to this limitation, only a lower quantity of data can be loaded, and lossy compression must be utilised.

Zhenfei Zhaoet.al in (6) proposed a new reversible data hiding scheme grounded on orthogonal vaticination revision (OPT) and multilevel histogram shifting. Conclude fashion can give the stylish weights of a predictor. As a result, the utmost predictor error can be concentrated around zero. Then the error revision strategy uses the result of introductory pixels to prognosticate the values ofnon-basic pixels. Grounded on the sequence of vaticination crimes, a histogram can be constructed and a histogram that's multilevel medium can be designed for bedding secret data. At the receiver, we've to cipher the prognosticated value of the cover image that's recovered. also its difference that's pronounced will reckoned to gain the embedding position from the encoder. And therefore the original cover image and secret data can be impeccably reconstructed. This proposed scheme provides a better PSNR value and better embedding capacity. But the data loss can do during transmission due to the lack of proper security systems.

By reversing the order in which encryption is performed and leaving the room, the method proposed by W Zhanget.al in reference number 7 is able to considerably improve the general efficacy of data bedding in translated images. Before the encryption process begins, some of the pixels in the image are estimated, rather than the data being bedded in the images that have been translated. This allows for fresh data to be bedded in the offences that are estimating. Still, one can fill in or excerpt fresh data from the translated image with simply the data caching key, even without having knowledge of the image in its original form. Additionally, data creation and image retrieval are both error-free.

First, some pixels are aimlessly named according to the encryption key. Also the values were

estimated with the help of the neighboring pixels. The estimating crimes that can do in these pixels are calculated with the help of these values. The named pixels that are arbitrary replaced by estimating crimes. also the content proprietor can produce embedding space by modifying the histogram of estimating crimes with the help of two loftiest lockers and two smallest lockers. The content proprietor can give the shifted error to the data hider for bedding data after the histogram shift. But during transmission leakage of information can do. To avoid this, a special encryption algorithm can be used for cracking the estimating crimes and a standard algorithm like AES for cracking the rest of the pixels. It shall be arranged successionally. For decryption and data recovery, this system can work on two schemes. Data birth before image decryption and data birth after image decryption. The proposed scheme provides better performance in complete reversibility, separability between data birth and in image decryption as well as advanced PSNR under given embedding rate.

Cao Xet.al in(8) proposed a data caching system by patch position representation. Then the correlations between the neighbour pixels are explored and a patch position representation that's meager used to hide the secret data. The patch is regarded as a whole and represented them using a small number of portions for which capacity that's high be attained. Due to this large room that's vacated a data hider can bed further secret bits in the translated images. By this system, for a certain embedding rate, the reconstructed image quality can be bettered. Then, the embedding that's average reached1.7 times as large as that of the other embedding schemes.

In the paper (9), Nour Kittawie et al suggested an algorithm that may conceal two watermarks within a given translated image. The primary watermark is embedded in the translated image by exchanging part of the pixels that are grounded on the data caching key. The secondary watermark is embedded in the watermarked translated image through the utilisation of the histogram shifting reversible data caching method.

In order to keep data confidentiality first, the image will be translated using a sluice cipher with the help of a secret key. also the first watermark is bedded using the bit negotiation system in which one watermark bit will be substituted at the MSB position per each block that'snon-overlapping. The image size and the size of the block both play a role in determining the maximum amount of bits that can be embedded into an image. Before adding an alternative watermark, the translation image is cut into four equal corridors, and the histogram stirring process is carried out on each section of the image separately. This is done so that the bits of the alternate watermark may be accounted for. This split is carried out in order to circumvent the result of the sluice cypher encryption producing a histogram that is horizontal. The data caching key is derived from both the point at which the component is at its maximum and the point at which it is at its minimum. By increasing the total number of bits that are embedded in the translated image, the introduction of a different type of watermark can help to boost the embedding capacity of an image. In order to win the retired alternate watermark utilising the inverse histogram shifting system, the watermarked translated picture that was entered into the receiver is first divided into four equal corridors. This is done in order to award the retired watermark. The image can be deciphered using the same secret key matrix bits that were used during the encryption phase to obtain an analogous image that includes bits that are the same as the original image with the

exception of the bits that are in the named embedding positions. This allows the original image to be recovered. Using the data caching key, select the positions of the bedded bits in each block. The receiver makes the assumption that the original bit that was replaced by the replacement bit is both zero and one in their own right, which results in the formation of two new blocks, one of which is the original block with the original bit for each block. The original block can be identified by computing the pixel change values included within the blocks and comparing those results to a change function that has already been established. In most cases, the change that occurs in the original block is noticeably less than that which occurs in an obtruded block. The approach that has been proposed offers a large embedding capacity, a high visual image quality, and a high entropy. Incorporating fashions other than histogram stirring is one way in which bedding capacity can be improved further.

Anushiadeviet.al in(10) proposed a new idea for lossless data caching using proximity pixel difference and histogram stirring. Then first divide the image into several 2 × 2sub-images and have to calculate the absolute pixel differences. Neighbouring pixel value in an image is largely identified and hence, the maximum proximity pixel difference is nearly equal to zero. also draw the histogram for the pixel that's absolute and the data can be bedded after shifting the histogram. If the value 'd' represents the peak point of the histogram, then the process of adding 'n' to each difference with a value that is lower than 'd' is referred to as "histogram stirring." After the data has been embedded and the histogram has been stirred, the next step is to reacquire the data and reconstruct the image. With the use of this plan, a high PSNR value can be incorporated into a quantum that has reliable data. However, it does not provide any guarantee that the data and images will remain secure.

Paulineet.al in(11) proposed reversible data hiding in translated images by MSB negotiation. Then first, descry all the crimes that can be passed at MSB positions and preprocessing of the image will be done inorder to minimize the error. also the image shall be translated and data will be hidden at the MSB positions. The secret data will be recaptured and MSB values will be prognosticated to reconstruct the cover image at the receiver. A combination can be handed by this system of high PSNR and high bedded capacity.

III. Comparison

Table-1 Comparison between related works

Methods	Advantages	Disadvantages
[1]	High Entropy and less information redundancy	Payload capacity is very less
[2]	Improves capacity and can avoid overlapping problems	Data loss can occur
[3]	Improvement in embedding capacity and less distortion	Risk of the defeat of image recovery and bit extraction is more
[4]	Better visual quality of the watermarked image	Optimal adaptive embedding threshold determined iteratively
[5]	Lossless compression	Embedding capacity is less
[6]	Better reconstructed image	Loss of data can occur

[7]	Complete reversibility and separability	Not much satisfactory embedded capacity
[8]	Better embedding capacity	Embedding capacity according to the PSNR values cannot be achieved
[9]	Better entropy and visual quality	Embedding capacity according to the PSNR values cannot be achieved
[10]	Capacity is more	No guarantee for the secrecy of image
[11]	Better PSNR and better embedding capacity	Noise can be affected during transmission

IV. Conclusion

Reversible data hiding ways came an ineluctable part of secure communication. In this paper, colorful styles put forward by the experimenters were bandied and it has been set up that some styles enable us to hide a quantum that's large of while some of them can hide only a many quantities of data. There's also a change that's significant embedding capacity and reconstructed image quality which gets bettered over the time. By combining certain named styles, the capacity can be increased by us of the system. In order to further ameliorate the embedding capacity, two-bit MSB positions can be used for hiding the data and to ameliorate the reconstructed image quality a median edge discovery algorithm can be used. Noise elimination can be incorporated in this two- bit MSB grounded negotiation system in order to avoid the essential noise that can be passed during transmission.

References

[1] W. Puech, M. Chaumont, and O. Strauss, “A reversible data hiding method for encrypted images,” in Electronic Imaging 2008. *International Society for Optics and Photonics, 2008, pp. 68191E–68191E.*

[2] V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y.-Q. Shi, “Reversible watermarking algorithm using sorting and prediction*,” IEEE Trans. Circuits Syst. Video Techno l., vol 19, no.7, pp.989–999, Jul.2009.*

[3] X. Zhang, “Reversible data hiding in encrypted image,” *IEEE Signal Processing Letters, vol. 18, no. 4, pp. 255–258, 2011.*

[4] Xiaolong 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, Dec. 2011*

[5] X. Zhang, “Separable reversible data hiding in encrypted image,” *IEEE Transactions On Information Forensics And Security, Vol. 7, No. 2, April 2012*

[6] Zhenfei Zhao, Guangyu Kang and Ruixu Guo, “Reversible Data Hiding Based on Orthogonal Prediction Error Modification and Multilevel Histogram Shifting,” *Information Technology Journal,2012, 11: 1077-1083*..7, no.2, pp. 826–832, Apr.2012.

[7] W. Zhang, K. Ma and N. Yu, “Reversibility improved data hiding in encrypted images*,” Signal Processing, vol. 94, pp. 118–127, 2014.*

[8] Cao X, Du L, Wei X, Meng D and Guo X**. "**High Capacity Reversible Data Hiding in Encrypted Images by Patch-Level Sparse Representation" *IEEE Transactions On Cybernetics,2015*

[9] Nour Kittawi and Ali Al-Haj, "Reversible Data Hiding in Encrypted Images," *2017 8th International Conference on Information Technology (ICIT),978-1-5090-6332-1/17/$31.00 ©2017 IEEE*

[10] R.Anushiadevi,Padmapriya Praveenkumar, John Bosco Balaguru Rayappan and Rengarajan Amirtharajan, 2017. "Reversible Secret Data Hiding Based on Adjacency Pixel Difference," *Journal of Artificial Intelligence, 10: 22-31.*

[11] Pauline Puteaux, and William Puech, "An Efficient MSB Prediction-Based Method for High-Capacity Reversible Data Hiding in Encrypted Images" *IEEE Transactions on Information Forensics and Security, 2018*