IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Special Issue-14, May 2019 E-ISSN: 2347-2693

Reversible Data Hiding in Encrypted Images

Narendra P[1*], N. Ganesh Kumar Reddy[2], N.Ramakrishna[3], O.Harikrishnareddy[4], Shashikala N[5]

[1,2,3,4,5]Dept. of Computing & Information Technology, REVA University, Bangalore, India

Corresponding Author: narendrap.2398@gmail.com

DOI: https://doi.org/10.26438/ijcse/v7si14.252255 | Available online at: www.ijcseonline.org

***Abstract*—** Reversible information concealing in scrambled pictures has achieved more consideration as of late in research network. Security assurance of extra information alluring for crime scene investigation. In this paper, another technique for reversible information stowing away in scrambled pictures. Our strategy embraces the methodology of holding adequate space for the extra information before encoding the spread picture. First we recognize reasonable squares for concealing information from different pieces of the picture. Before scrambling the picture, at least one LSB-plane of these squares are upheld up into residual pieces of the picture utilizing a high-performing customary RDH strategy that chips away at decoded pictures. In the wake of scrambling the picture, those least significant bits are utilized to conceal extra information. Recuperation of unique spread picture and blunder free extraction of extra information is ensured dependably. Also, the proposed technique is straightforward and instinctive. Tentatively outcomes demonstrate that our technique outflanks the cutting edge strategies for reversible information covering up in scrambled pictures.

***Keywords*—** Reversibledatahiding;interpolation;encryption;histogram;reservation

I. INTRODUCTION

Reversible information concealing includes concealing information into a spread medium in a way that the first spread medium can be recouped from the misshaped medium. Reversible information a center region of research for a considerable length of time. Strategy licensed is one of the soonest systems in Reversible data hiding. It was utilized for validation of computerized content utilizing advanced mark inserted into the substance. Hypothetical investigation on limit cutoff points of Reversible data hiding is finished by Kalker. Reversible data hiding is performed utilizing various types of spread media, for example, pictures, recordings, sound and so forth. Among them, computerized picture have been a well known decision as spread medium. Reversible data hiding utilizing advanced pictures discovers application in military imaging, therapeutic imaging, crime scene investigation and so on since lasting bending to cover picture is unsatisfactory in these territories.

On the off chance that the information covered up is some data identified itself with spread medium is called watermarking. This is generally accomplished for validation and copyright assurance. This is commonly relevant to Reversible data hiding moreover. First class utilizes system referred to as contrast extension as if there should arise an occurrence. These strategies by and large work by extending little qualities, for example, neighbouring pixel contrast, to install extra bits. Second classification of strategies utilizes pressure of spread medium to discover space for extra information. Histogram moving is utilized in the third classification. Some of the ongoing strategies utilize a blend of the over three methodologies.

Customary Reversible data hiding procedures don't ensure the security of the spread picture. At times it is important to guarantee security of spread picture and in the meantime conceal extra information into it. Therapeutic imaging, distributed storage, crime scene investigation and so forth are a portion of the application regions where such prerequisites are normal. Reversible information covering up in scrambled pictures is utilized for this reason. The spread picture is scrambled first and afterward extra information is covered up into it. An alluring property is the severability of encryption and information stowing away. It implies that these two activities should be possible by two unique people. Along these lines the information hider can be kept out of review the spread picture content. Additionally, distinguishableness in data extraction and picture recuperation is likewise very looked for. This property can upgrade the extent of RDH-EI.

First methodology is to scramble spread picture and afterward discover approaches to conceal extra information in the encoded picture. Techniques fall in this class. Restrictions of these strategies are low information concealing limit and contingent reversibility. Since the entropy is boosted for encoded pictures, it is hard to discover more space for extra utilizing pressure, pixel connection and so on. Additionally, mistake free extraction of information and reversibility of spread picture may not be conceivable at

high installing rates. Technique improved installing limit and guaranteed genuine reversibility for all cases. And, after it's all said and done the accomplished limit isn't fundamentally high for this methodology, which restrains the pragmatic applications for these strategies. The second methodology is to hold space for extra information in a lossless way before scrambling the picture. This space can be utilized to conceal extra information subsequent to encoding the picture. Mama et al. proposed a strategy that pursues this methodology which gives noteworthy improvement in installing limit and furthermore genuine reversibility in all cases. Additionally, detachability is guaranteed in installing and extraction process. We propose a technique that receives the second methodology.

Technique basically works by saving Least significant bit of a solitary substantial locale U the spread picture to shroud mystery information. Unique bits of these Least significant bit are reversibly installed into the mix of residual areas L utilizing. The rebuilt picture is scrambled and held biplanes of the picked area are utilized to conceal information. Strategy has a few faults. Truth be told performs better for a smooth picture. Yet, since a solitary huge locale is picked as U, a great deal of smooth territories becomes some portion of U and coarse zones in L as unmistakably found in Fig. 1(b). This impacts in L in a diminished exhibition of .Besides, rebuilding of the spread picture is must be performed in installing and extraction sides to get a significant steno picture and furthermore to recoup spread picture. This is fairly unintuitive. Another issue is that the strategy for choosing the area U is computationally serious as it works in a sliding-window way and figure smoothness factor on every window of pixels.

Strategy was improved by the creator utilizing a procedure alluded as dynamic square trade .In this strategy, a novel way is utilized of non-covering hinders in the picture. Very coarse squares are the moved to start of the picture coming about all coarse square collect in the top district of the picture as appeared in Fig. 1(c). The rest of the picture ends up being progressively reasonable for strategy to conceal more information with less weakening in PSNR. Technique is unpredictable in itself because of unintuitive adjustment of picture squares which includes additional means in sender and collector sides.

II. RELATED WORK

This section describes the reserve block and unreserved block. The reserve block we use to call RB and unreserved block we use to call UB**.** First The interpolation technique used in our method. This is a simple adaptation of the interpolation used in this method. After that selection process for the blocks is explained. This is followed by the Pixel interpolation process.

Fig. 1 (a)Original image (b) Partitioning image (c)Block exchange (d) Dynamic Super Resolution image

A. Pixel interpolation

The technique used in the proposed method is interpolation. Interpolation is a simplified adaptation of the interpolation used into our method. There are two cases of interpolation technique. One is interior pixel and second one is border pixel.

Interior pixel: Interior pixel is computed as a weighted average of vertical and horizontal neighbour. A 3 × 3 neighbourhood is shown in Fig. 2.

Let current pixel $X = C$.

Then $X = \lfloor w \times NS + w \times EW \rfloor$

Where w=horizontal and vertical weights

$NS = (N + S)/2$ and $EW = (E + S)/2$.

Border pixel: All the four neighbours are not present the border pixel. So it is computed as a simple average of the available vertical and horizontal pixels. For example

$X = (NE + C + SE)/2$.

|Interpolation-error e is computed as

$e = X - X'$

We can compute interpolation error for every pixel in the in the block. Two peak points LP and RP of this diagram are used for embed bits by a process of interpolation-error expansion. If the number of pixels in these bits are higher, we can embed more bits in that region. So we choose the reserved block set such that it comprises of the blocks that contribute least number of pixels to the peak bin sand which in turn results in a better.

B. Data *hiding for Selection of blocks*

The $I_{\times}$ cover image is divided into blocks of size $w \times w$. Interpolation-error is computed for each of these blocks. Total pixels n in the two peaks bins in a block is given by

$n = count(\mathrm{R}P) + count(\mathrm{LP})$

The count of pixel is given by the count().
The set of reserved blocks(RB)is

$$RB = IB \cup DB \cup MB$$

IB=set of blocks that store indices of blocks in sets DB & MB.
DB =set of blocks reserved for additional data.
MB =set of blocks for metadata.
Space reservation chosen by the Least significant bits. Least significant bits denote the value 'n'.

ln= n X w X w

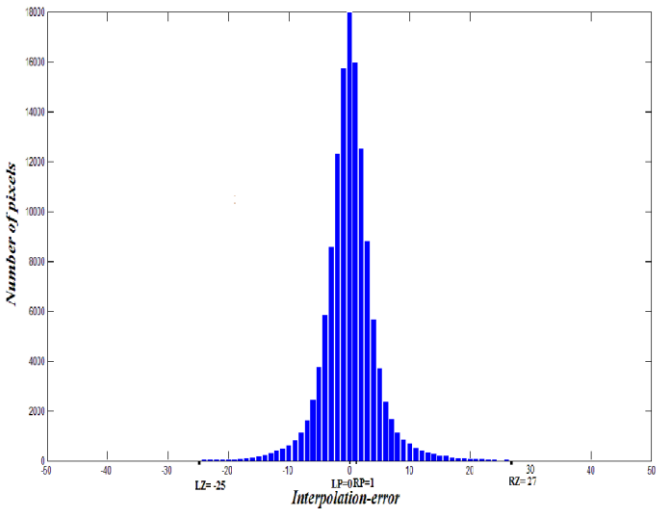

Fig. 3. Interpolation-error for Lena image

Interpolation of a pixel:
The border pixels of UR is used to store additional data. Interpolation of a pixel are adjacent to reserved blocks and also treated as border pixels.

Storage of Metadata:
Metadata are stored into Least Significant Bits-planes of border pixels. The method stores in Least Significant Bits-planes reserved blocks in set MB.The Meta data needed in extraction process.

III. METHODOLOGY

In reversible data hiding in encrypted using encrypted keys and data hiding key. In reversible data hiding in encrypted image is summarized in the following process.

- **Data Embedding Phase**: The image provider embed the data into the cover and encrypts it using encryption key. At the receiver receives encrypted image and decrypt it using the key and extracts the data to recovers original image.

- In an image a pixel is related with its neighbouring pixels, using this relation any pixel can be predicted from a its neighbour pixels. So we need to find the technique to deduce this relation.

- By Applying pixel permutation method the receiver decrypt the encrypted image.

- Now receiver extracts hidden data from decrypted image. The recipient extracts message bits from the decrypted stego-image by scanning the image in the same order as during the embedding.

IV. RESULTS AND DISCUSSION

The proposed method is tested using the publicly available standard test images aeroplane, wine, lean, Baboon from database. These test images represent the classes of natural images varying from smooth images to highly textured images.

The higher embedding rate blocks are more effectiveness of our mechanism to select the suitable blocks is more explicit. Special mention deserve by the Wine and Baboon image. Wine image gives highest Peak signal-to-noise ratio values for a given embedding rates. Peak signal-to-noise ratio image has plenty of smooth regions. Smooth regions gives more accurate interpolation. The textured image Baboon gives lowest Peak signal-to-noise ratio values for given embedding rate. The poor performance of method is textured images method.

V. CONCLUSION AND FUTURE SCOPE

This method is for reversible data hiding in encrypted images. This method achieves better performance than the existing methods because of adopting the approach of reserving space of image and embedding capacity. This method is suitable for applications in medical agencies, military security etc. This method is simple and easy to implement compared to other methods. we are eliminating the need for reconstructing the image unlike the other methods in general. At the same time, if we compare the clarity of image by keeping the data constant, there are notable improvements in images over the long time.

This method is used for various applications like military, medicine, data security etc.

REFERENCES

[1] L. Zhou, V. Varadharajan, M. Hitchens, Achieving secure role-based access control on encrypted data in cloud storage, IEEE Trans. Inf. Forensics Secur. vol. 8, no.12, pp.1947– 1960, 2013.
[2] H. Wang, S. Wang, Cyber warfare-steganography vs. steganalysis, Commun. ACM, vol. 47, no. 10, pp. 76–82, 2004.
[3] F.A.P. Petitcolas, R.J. Anderson, M.G. Kuhn, Information hiding-a survey, Proc. IEEE, vol. 87, no. 7, pp.1062–1078, 1999.

[4] J. Fridrich, D. Soukal, Matrix embedding for large payloads, IEEE Trans. Inf. Secur. Forensics, vol. 1, no. 3, pp. 390–394, 2006.
[5] C. Munuera, Steganography and error-correcting codes, Signal Process. vol. 87, no. 6, pp. 1528–1533, 2007.
[6] J. Mielikainen, LSB matching revisited, IEEE Signal Process. Lett. vol. 13, no. 5, pp. 285–287, 2006. [7]. X. Zhang, S. Wang, Efficient steganographic embedding by exploiting modification direction, IEEE Commun. Lett. vol. 10, no. 11, pp. 781–783, 2006.
[7] J. Tian, Reversible data embedding using a difference expansion, IEEE Trans. Circuits Syst. Video Technol. vol. 13, no. 8, pp. 890–896, 2003.

.

