Data Hiding In Encrypted Images Using Reversible Technique Based On Interpolation Method

Aishwarya R, Deeksha C,
Deepika G, Hephzibah Dayakar A
Dept of ISE, EPCET, Bangalore, India

Geetha R
Assistant Professor, Dept, of ISE, EPCET,
Bangalore, India

Abstract: Reversible data hiding in encrypted images (RDH-EI)based on progressive recovery. Three parties are involved in the framework, including the content owner, the data hider, and the recipient. The content owner encrypts the original image using a stream cipher algorithm and uploads cipher text to the server. The data hider on the server divides the encrypted image into three channels and respectively embeds different amount of additional bits into each one to generate a marked encrypted image. On the recipient's side, additional message can be extracted from the marked encrypted image, and the original image can be recovered without any errors. While most of the traditional methods use one criterion to recover the whole image, we propose to do recovery by a progressive recovery mechanism. Rate distortion of the proposed method out performs state-of-the-art RDH-EI methods

Keywords: RDH-EI; Data Hider; Encryption

I. INTRODUCTION

Idea of reversible data hiding in the encrypted images (RDH-EI) originates from reversible data hiding (RDH) in plain text images. It is feasible in the applications like cloud storage and the medical systems. Among them, digital image have been a popular choice as cover medium. RDH using digital images finds application. If the data hidden is some information related to cover medium itself, it is called watermarking. This is usually done for authentication and copyright in the protection.

Cover image wasn't protected by traditional RDH method. We need to hide additional data and add privacy to it. some of the examples are forensics, cloud storage, medical imaging etc. Reversible data hiding in encrypted images (RDH-EI) is used for this purpose. In this first cover image is encrypted and then additional data is hidden into it. One of the main properties of RDH-EI is severability of encryption and data hiding. RDH-EI uses three techniques first category uses differential expansion, second category is compression of cover medium to find room for additional data, third category uses histogram. Sometimes it uses combination of these three.

The operation can be done individually. The data hider can be kept out of viewing the cover image content. Similarly, image recovery and data extraction can be sought. This property can enhance the scope of RDH-EI. The proposed method hides additional data in suitable blocks. The selected blocks are not moved, Therefore the original structure of the cover image is unaffected. The LSB-planes of these blocks are extracted and reversibly embedded into remaining regions of the image using a traditional RDH method [20] it works for unencrypted images.it is encrypted and to remaining planes are used to hide additional data. Novel is used to select sufficient number of small-sized coarse blocks for hiding additional data, The method is made simpler by avoiding restructuring of the image. The reserved Blocks remain in their original positions in the cover image. To cope with feature, method [20] is modified and used in the proposed method.

II. PROPOSED SYSTEM

The proposed system is, including three parties: the content owner, the data hider, and the recipient. The content owner encrypts the original image and uploads the encrypted image onto a remote server. The data-hider divides the encrypted image into three sets and embeds messages into each set to generate a marked encrypted image. The recipient extracts message using an extraction key. Approximate image with good quality can be obtained by decryption if the receiver has decryption key. When both keys are available, the original image can be losslessly recovered by progressive recovery.

A. Pixel interpolation

The proposed method uses interpolation technique, it is a simplified adaption that suits our method for interpolation. There are two cases for current pixels in interpolation like interior pixel or a border pixel.

a) Interpolation of interior pixel

Interpolated value X' for X is used as a weighted average for horizontal and vertical neighbors of X. A 3 × 3 neigbourhood is shown in Fig. 2. Let the current pixel be X=C. Then,

$$X' = [W_o * NS + W_{90} * EW] \qquad (1)$$

KITE was held at Brindavan College of Engineering, Bengaluru, India on 4th May, 2018.

where W_0 and W_{90} are horizontal and vertical weights used in the same way as [21] using pixel variance in corresponding directions.

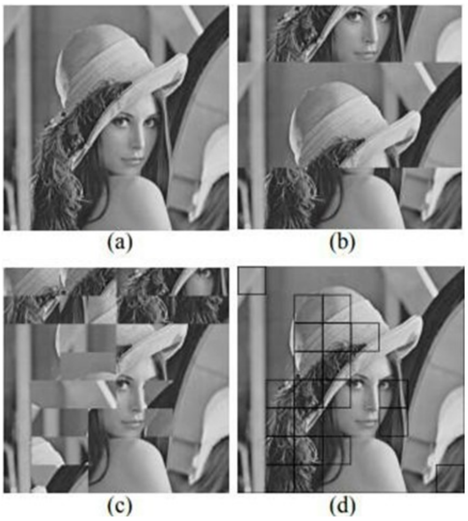

Fig 1. (a) original lena image. (b) partitioning in [21] (c)output of active block exchange in [22]. (d) DSR in proposed method

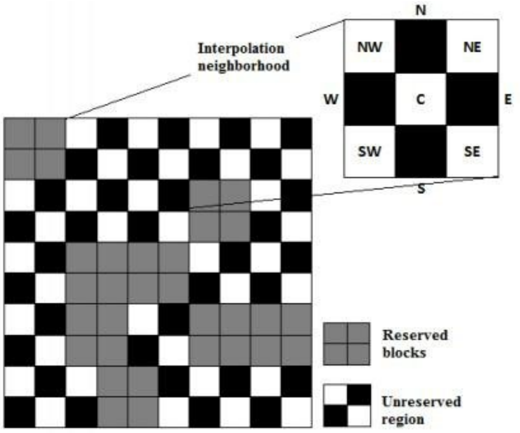

Fig 2. Blueprint of reserved blocks and unreserved blocks distribution in an image with interpolation neighbourhood highlighted

$$NS= (N+S)/2 \text{ and } EW= (E+S)/2 \qquad (2)$$

b) Interpolation of border pixel

All four neighbours are not present for a border pixel. Due to such case, interpolated value is used as a simple average for available horizontal and vertical pixel. For example, from Fig. 2, if X = E, then

$$X' = (NE + C + SE)/3$$

Once X' is computed, and interpolation-error e is computed as

$$e = X - X' \qquad (3)$$

As the number of pixels increases we can embed more bits in that region. So we use reserved blocks at RB that comprises the blocks that gives least number of pixels. The peak LP and RP will give better results in UR for [20].

B. Selection of blocks for data hiding

First the cover image IP*Q is split into blocks of size W*W. Interpolation-error histogram is applied to each blocks, based on number of pixels. Total pixels Np in the two peaks of histogram of a block is given by

$$Np=count(LP)+count(RP) \qquad (5)$$

here ( ) gives the count of pixels.np values for all the images are used in this way. The reserved blocks is given as

$$RB=DB \cup MB \cup IB \qquad (6)$$

DB are the set of blocks that are reserved for additional data, is set of blocks for metadata, and is set of blocks that store indices of blocks in sets and . Where n denotes the number of LSB planes that are used for space reservation. The number of blocks required set data is given by

$$n_{db} = \left\lceil \frac{l}{n \times w \times w} \right\rceil$$

here denotes the length of the additional data to hide. MB is considered as a singleton. Here metadata is of small length and hence n_{mb}= 1. Let N be the total number of blocks in the image, then the number of bits required to a represent block index is given by d= [log(N)].

Hence the total length li (in bits) of the indices of blocks in DB and MB is given by

$$li=d \text{ x } (n_{db} + n_{mb}) \qquad (7)$$

From this we can compute the number of blocks in set IB as

$$n_{ib} = \left\lceil \frac{li}{n \times w \times w} \right\rceil$$

The first n_{ib} blocks of cover image are selected as index block set IB. Usually the value of nib is 1 or 2. Apart from other blocks, n_{db}+n_{mb} blocks with least values for n_p are chosen as the data bock set DB and the meta block set MB. We choose blocks which contribute least no of pixels for the peak bins, for reserving space for additional data. This increases the interpolation-error histogram for the remaining unreserved region UR. hence it requires better performance for [20] when it is applied to UR.

C. Space Reservation for additional data

When the reserved blocks are chosen from previous step the LSB-planes of the block in the set, they are extracted and are reversibly embedded in a region by traditional RDH method.

a) Pixel interpolation

The border pixels of UR are also interpolated unlike original [20] and it is used to store additional data. Pixels that are adjacent to the pixel block can also be treated as border pixels.

b) Metadata storage

Metadata needed extraction process are stored into LSB-planes of border pixels, the proposed method stores in LSB-planes reserved blocks in MB.

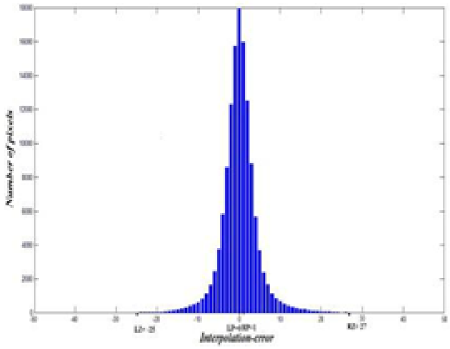

Fig 3. Interpolation-error histogram for Lena image with peak points LP = 0 and RP=1.

Two-pass embedding

c) *One round of complete embedding into UR* is split into two phases to exploit all pixels in UR for bit embedding. In first phase pixels are marked as white ((i+j)mod 2=0)are used for bit embedding ,which is followed by black((i+j)mod 2=1) ,second phase is similar to [21].

d) *Method[20]* works on rectangular image region, In our method region UR need not to be rectangular because reserved blocks are distributed in cover image.

Here we use additive interpolation-error expansion in [20] to reversibly embed original LSB-planes of reserved blocks into UR.

$$\hat{e} = \begin{cases} e + SIGN(e) \times b, & e = LP \text{ or } RP \\ e + SIGN(e) \times 1, & e \in (LZ, LP) \cup (RP, RZ) \\ e, & otherwise \end{cases} \quad (9)$$

Pixel interpolation-error e computed using (3). LZ and RZ are the first zero bins towards left and right of LP and RP which is showed in fig (3) It is clear that only those pixels belongs to two peak bins of LP and RP.

$$SIGN(e) = \begin{cases} -1, & e \leq LP \\ 1, & e \geq RP \end{cases} \qquad (10)$$

The stego pixel is obtained from interpolated pixels value x' as x''=x'+e^ which replaces original image x in the cover image.

Bit embedding of multiple round can be done in UR , taking the output image of one round as the cover image for next round. Overflow and underflow scenarios are handled using boundary map as in [20]. Values of LP,RP,LZ,RZ and number of embedding rounds form the metadata. The image obtained as the result of this step is given as I'$_{P*Q}$.

D. Encryption of cover image

The cover image is encrypted after reserving space for additional data. Encryption scheme used here is [18]-[21]. Pseudo random and bitwise exclusive-OR operation is used for encryption.

$$E_{i,j,k} = I'_{i,j,k} \oplus r_{i,j,k} \quad k = 0, 1, \ldots, 7. \qquad (11)$$

where $I'_{i,j,k}$ is the k^{th} bit of pixel $I'_{i,j}$.

E. Hiding additional data in reserved space.

LSB-planes of reserved blocks are available to store additional data .The data is encrypted using data hiding key (KH).If the data hider is different from content owner will be provided with the indices of reserved blocks and LSB-planes will be available. This information will be required in the extraction process to identify the reserved blocks.

F. Extraction process

Extraction process involves recovering additional data and restoring the original cover image. The steps are more-or less the reverse of embedding process as summarized below.

1) Data-extractor extracts indices of the reserved blocks stored in LSB-planes index blocks IB to identify the blocks in which additional data is stored.

2) Hidden additional data is extracted from the reserved data blocs (DB) and decrypted using data-hiding key(H).

3) Decrypted stego image is obtained using the exclusive- OR operation using the same pseudo-random sequence used in embedding side on the encrypted image p^{h}×Q as shown.

$$D^{H}_{i,j,k} = \begin{cases} E^{H}_{i,j,k} \oplus r_{i,j,k}, & k = 0, \ldots 7 \text{ , if } E^{H}_{i,j} \in UR \text{ or } MB \\ E^{H}_{i,j,k} \oplus r_{i,j,k}, & k = n, \ldots 7, \quad otherwise. \end{cases} \qquad (12)$$

LSB-planes of blocks in RB and IB excepted while decrypting to preserve the additional data and block indices. Decrypted image is used to measure the distortion introduced on the original image PXQ by the embedding process. n LSB-planes of blocks in RB and IB excepted while decrypting to preserve the additional data and block indices. Decrypted image ph×Q is used to measure the distortion introduced on the original image P×Q by the embedding process.

III. CONCLUSION

A new RDH-EI Protocol for three parties is Proposed, Main improvement is extending the traditional recovery to the progressive based recovery. The progressive recovery based RDH-EI provides a better prediction way for estimating the LSB layers of the original image using three rounds, which outperforms state-of-the-art RDH-EI methods. Since RDH-EI is equivalent to a rate-distortion problem, capability of the method should be evaluated by both the distortion and the embedding rate. For a fair comparison, it limits the distortion to three LSB-layers, and accordingly improves the embedding rate.

REFERENCES

[1] C. W. Honsinger, P. W. Jones, M. Rabbani, and J. C. Stoffel, “Lossless recovery of an original image containing embedded data,”U.S. Patent 6 278 791, 2001.

[2] J. M. Barton, “Method and Apparatus for Embedding Authentication Information Within Digital Data,” U.S. Patent 5 646 997, 1997.

[3] Z. Ni, Y. Q. Shi, N. Ansari, and S. Wei, “Reversible data hiding,” in ISCAS Proceedings of the 2003 International Symposium on Circuits and Systems, vol. 2, pp. II–912–II–915, Thailand, May 2003.

[4] T. Kalker and F.M. Willems, “Capacity bounds and code constructions for reversible data-hiding,” in Proc. 14th Int. Conf. Digital Signal Processing (DSP2002), 2002, pp. 71–76

[5] J. B. Feng, I. C. Lin, C. S. Tsai, and Y. P. Chu, “Reversible watermarking: Current status and key issues,” Int. J. Netw. Security,vol. 12, no. 3, pp. 161–171, 2006.

[6] A. M. Alattar, “Reversible watermark using the difference expansion of a generalized integer transform,” IEEE Transactions on Image Processing, vol. 13, no. 8, pp. 1147–1156, Aug. 2004.

[7] J. Tian, “Reversible data embedding using a difference expansion,”IEEE Transactions on Circuits Systems and Video Technology, vol.13, no. 8, pp. 890–896, Aug. 2003.

[8] D. M. Thodi and J. J. Rodriguez, “Reversible watermarking byprediction-error expansion,” in Proceedings of the 6th IEEE Southwest Symposium on Image Analysis and Interpretation, vol. 3,pp. 21–25, LakeTahoe, USA, Mar. 2004.

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

[10] J. Fridrich and M. Goljan, “Lossless data embedding for all imageformats,” in SPIE Proceedings of Photonics West, Electronic Imaging, Security and Watermarking of Multimedia Contents, vol.4675, pp. 572–583, San Jose, Jan. 2002.

[11] G. Xuan, C. Yang, Y. Zhen, Y. Q. Shi, and Z. Ni, “Reversible data hiding based on wavelet spread spectrum,” in Proceedings of the IEEE 6th Workshop on Multimedia Signal Processing, pp. 211–214,Italy, Sept. 2004.

[12] C. D. Vleeschouwer, J. E. Delaigle, and B. Macq, “Circular interpretation of histogram for reversible watermarking,” in Proceedings of the IEEE 4th Workshop on Multimedia Signal Processing, pp. 345–350, France, Oct. 2001.

[13] B. Yang, M. Schmucker, X. Niu, C. Busch, and S. Sun, “Reversible image watermarking by histogram modification for integer dct coefficients,” in Proceedings of the IEEE 6th Workshop on Multimedia Signal Processing, pp. 143–146, Siena, Italy, Sept. 2004.

[14] 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.

[15] [15] 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 Technol., vol. 19, no. 7, pp. 989–999, Jul. 2009.

[16] X. Zhang, “Reversible data hiding in encrypted images,” IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255–258, Apr. 2011.

[17] 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.

[18] X. Zhang, “Separable reversible data hiding in encrypted image,”IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 826–832, Apr. 2012.

[19] N. S. Nair, T. Mathew, Neethu A.S., Viswajith P. Viswanath, Madhu S. Nair, M. Wilscy, "A Proactive Approach to Reversible Data Hiding in Encrypted Images", Procedia Computer Science, Elsevier,Vol.46, pp.1510-1517, 2015

[20] L. Luo et al., “Reversible image watermarking using interpolation technique,” IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp.187–193, Mar. 2010

[21] K. Ma, W. Zhang, X. Zhao, N. Yu, and F. Li, “Reversible data hiding in encrypted images by reserving room before encryption,” IEEE Trans. Inf. Forensics Security, vol. 8, no. 3, pp. 553–562, Mar. 2013.

[22] T. Mathew, M. Wilscy, “Reversible Data Hiding in Encrypted Images by Active Block Exchange and Room Reservation,” in Proc. Int.Conf. Contemporary Computing and Informatics (IC3I), 2014, pp.839-844, Nov. 2014

[23] Miscellaneous Gray Level Images [Online]. Available: http://decsai.ugr.es/cvg/dbimagenes/g512.php.