© 2018 IJSRST | Volume 4 | Issue 10 | Print ISSN : 2395-6011 | Online ISSN : 2395-602X
Themed Section: Science and Technology

Unpredictable Information Covering Up in Encoded Pictures Using Interpolation-Based Distributed Space Reservation

B. N. Manjunadha Reddy[1], P. Viswanatha Reddy[2]
[1]Student, Department of Computer Science and Engineering, Sir Vishveshwaraiah Institute of Science & Technology, Madanapalle, India
[2]Assistant Professor, Department of Computer Science and Engineering, Sir Vishveshwaraiah Institute of Science & Technology, Madanapalle, India

ABSTRACT

Reversible data hiding (RDH) in encrypted pictures has earned additional attention recently in analysis community. Privacy protection of extra data yet as cover media makes it attractive for applications in medical imaging, cloud storage, forensics etc. during this paper, a brand new method for reversible data concealing in encrypted images (RDH-EI), is proposed. Our method adopts the approach of reserving sufficient space for the additional data before encrypting the duvet image. First we identify appropriate blocks for concealing data from numerous elements of the image. Before encrypting the image, one or additional LSB-planes of these blocks are backed-up into remaining elements of the image using a high-performing ancient RDH methodology that works on unencrypted pictures. Once encrypting the image, those LSB planes are accustomed hide extra knowledge. Recovery of original cover image and error-free extraction of extra knowledge is guaranteed perpetually. Moreover, the projected methodology is straightforward and intuitive. By experimentation results show that our methodology outperforms the progressive ways for reversible knowledge hiding in encrypted images.

Keywords: Reversible data concealing in encrypted images (RDH-EI), Reversible data hiding (RDH), and encryption

I. INTRODUCTION

Reversible data hiding (RDH) involves concealing information into a cover medium in an exceedingly manner that the first cowl medium will be recovered from the distorted stego medium. This has been attention space of analysis for many years. Technique proprietary by Barton is one amongst the earliest techniques in RDH. It absolutely was used for authentication of digital content exploitation digital signature embedded into the content. Theoretical analysis on capability limits of RDH is finished. RDH is performed using completely different styles of cover media comparable to pictures, videos, audio etc. Among them, digital image are a well-liked choice as cowl medium. RDH exploitation digital pictures finds application in military imaging, medical imaging, forensics etc. since permanent distortion to hide image is unacceptable in these areas.

In the event that the information covered up is some data identified with cover medium itself, it is called watermarking. This is normally done for verification and copyright insurance. A characterization of reversible watermarking plans is finished. This is for the most part appropriate to RDH moreover. Initially class employments strategy referred to as contrast development as if there should a rise an occurrence. These strategies for the most part work by growing little qualities, for example, neighboring pixel contrast, to implant extra bits. Second class of methods utilizes pressure of cover medium to discover space for extra information. Histogram moving is utilized as a part of the third class of methods. Some of the ongoing methods utilize a mix of the over three methodologies. There are two main approaches for RDH-EI as classified. First approach is to encrypt cover image and then find ways to hide additional data in the encrypted image. Methods fall in this category.

Limitations of these methods are low data hiding capacity and conditional reversibility. Since the entropy is maximized for encrypted images, it is difficult to find more space for additional using compression, pixel correlation etc. Also, error-free extraction of data and reversibility of cover image may not be possible at high embedding rates. Method improved embedding capacity and ensured true reversibility for all cases. Even then the achieved capacity is not significantly high for this approach, which limits the practical applications for these methods. The second approach is to reserve space for additional data in a lossless manner before encrypting the image. This space can be used to hide additional data after encrypting the image. The propose method that follows this approach which gives significant improvement in embedding capacity and also real reversibility in all cases. Also, Separability is ensured in both embedding and extraction process. In this paper we propose a method that adopts the second approach.

II. PROPOSED METHOD

This section describes the proposed method in detail. Let RB denote the set of blocks reserved and the remaining unreserved regions of the image together is denoted as UR. First we describe the interpolation technique used in our method. This is a simplified adaptation of the interpolation used in to suit our method. After that selection process for the blocks is explained. This is followed by the space reservation step.

Pixel interpolation

The interpolation technique used in the proposed method is a simplified adaptation of the interpolation used, to suit our method. There two cases for the interpolation of current pixel X based on whether X is an interior pixel or a border pixel. Interpolation of interior pixel: Interpolated value X' for X is computed as a weighted average of the horizontal and vertical neighbors of X. A 3×3 neighborhood. Let current pixel $X = C$. Then

$$X' = [w_0 * NS + w_{90} * EW]$$

Where w_0 and w_{90} are the horizontal and vertical weights computed in same way as using pixel variance in the corresponding directions.

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

Selection of blocks for data hiding

In this step, first the cover image I_{P*Q} is divided into blocks of size $w \times w$. Interpolation-error histogram is computed for each of these blocks. Total pixels n_p in the two peaks bins of the histogram of a block is given by

$$n_p = count(LP) + count(RP)$$

Where count() gives the count of pixels in the given bin. n_p values for all the image blocks are computed this way. The set of reserved blocks RB is

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

DB is the set of blocks reserved for additional data, MB is set of blocks for metadata, and IB is set blocks that store indices of blocks in sets DB and MB.

Space reservation for additional data

Once the reserved blocks are chosen using previous step, n LSB-planes of the blocks in set RB are extracted and reversibly embedded in region UR using modified version of traditional RDH method.

1) Pixel interpolation: Unlike original, the border pixels of UR are also interpolated and hence used to store additional data. The pixels which are adjacent to reserved blocks are also treated as border pixels.
2) Metadata storage: In metadata needed in extraction process are stored into LSB-planes of border pixels, whereas, the proposed method stores it in LSB-planes reserved blocks in set MB.
3) Two-pass embedding: To exploit all pixels in UR for bit embedding, one round of complete embedding into UR is split into two phases. In this first phase all the pixels marked as white ($(i + j) \ mod \ 2 = 0$) are used for bit embedding, followed by black ones $(i + j) \ mod \ 2 = 1$) in second phase.
4) Method generally works on rectangular image region, whereas, in our method region UR need not be rectangular, since reserved blocks (RB) are distributed across the cover image.

Encryption of cover image

After reserving space for additional data, the cover image encrypted. Encryption scheme is same as the one used where a stream cipher is used. Pseudo-random number sequence (r_{p*q}) is generated using an encryption key (K_E). Bitwise exclusive-OR operation of pixel values and corresponding pseudo-random number of the generated sequence is used for encryption.

Hiding additional data in reserved space

LSB-planes of the reserved blocks in set DB are now available to store additional data. The data is encrypted using a data-hiding key (K_E) before storing. If data-hider is different from content owner, he is provided with the indices of the reserved blocks, and number of LSB-planes(n) available.

Extraction process

Extraction process involves recovering the 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(K_H).

III. CONCLUSION

The proposed methodology is for reversible data activity in encrypted images(RDH-EI). By adopting the approach of reserving space for added knowledge before encryption, this method achieves higher performance than the present methods in terms of PSNR of the stego image and embedding capability. These attributes create this methodology appropriate for sensible applications in medical imaging, military imaging etc. Moreover, this methodology is easy and simple to implement compared to its predecessors. This is often as a result of we tend to are eliminating the necessity for restructuring the image in contrast to the other strategies in literature. For many of the images the embedding capability for added data is improved on the far side 10000 bits. At identical time, if we tend to compare the PSNR of stego image by keeping the information embedded constant, there are notable enhancements in PSNR for all the photographs over the state of the art methods.

IV. REFERENCES

[1]. J. B. Feng, H. C. Wu, C. S. Tsai, and Y. P. Chu, "A new multi-secret images sharing scheme using Lagrange's interpolation," Journal of

Systems and Software, vol. 76, no. 3, pp. 327–339, June 2005

[2]. J. Fridrich, J. Goljan, and Rui. Du, "Invertible authentication," in SPIE Proceedings of Security and Watermarking of Multimedia Content, pp. 197–208, San Jose, Jan. 2002.

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

[4]. J. Fridrich, M. Goljan, Q. Chen, and V. Pathak, "Lossless data embedding with file size preservation," in SPIE Proceedings of EI, San Jose, Jan. 2004.

[5]. J. Fridrich, M. Goljan, and R. Du, "Lossless data embedding-new paradigm in digital watermarking," EURASIP Journal of Signal Processing, vol. 2002, no. 2, pp. 185–196, Feb. 2002.

[6]. J. Tian and R. O. Wells, "Reversible data-embedding with a hierarchical structure," in Proceedings of the ICIP International Conference on Image Processing, vol. 5, pp. 3419–3422, Genova, Oct. 2004.

[7]. C. L. Tsai, K. C. Fan, C. D. Chung, and T. C. Chung, "Reversible and lossless data hiding with application in digital library," in Proceedings of the 38th Annual International Carnahan Conference on Security Technology, pp. 226–232, Albuquerque, USA, Oct. 2004.

[8]. C. S. Tsai and C. C. Chang, "A repeating color watermarking scheme based on human visual model," Eurasip Journal on Applied Signal Processing, vol. 13, pp. 1965–1972, 2004.

[9]. 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.

[10]. G. Xuan, J. Zhu, J. Chen, Y. Q. Shi, Z. Ni, and W. Su, "Circular interpretation of bijective transformations in lossless watermarking for media asset management," IEE Electronics Letters, vol. 38, no. 25, pp. 1646–1648, Dec. 2002.

[11]. Zhang X (2011) Reversible data hiding in encrypted images, IEEE Signal Process. Lett., 18(4):255–258 10. Hong W, Chen T, Wu H (2012) An improved reversible data hiding in encrypted images using side match, IEEE Signal Process. Lett., 19(4):199–202

[12]. Zhang X (2012) Separable reversible data hiding in encrypted image, IEEE Trans. Inf. Forensics Security, 7(2):826–832 12. Ma K, Zhang W, et al. (2013) Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption, IEEE Trans. Inf. Forensics Security, 8(3):553-562

[13]. Kalker T, Willems F M (2002) Capacity bounds and code constructions for reversible data-hiding, Proc. 14th Int. Conf. Digital Signal Processing (DSP2002), 71–76 2. Sachnev V, Kim H J, Nam J, et al. (2009) Reversible watermarking algorithm using sorting and prediction, IEEE Trans. Circuits Syst. Video Technol. 19(7): 989–999

[14]. Fridrich J, Goljan M (2002) Lossless data embedding for all image formats, Proc. SPIE Proc. Photonics West, Electronic Imaging, Security and Watermarking of Multimedia Contents, 4675: 572–583, San Jose, CA, USA

[15]. G. Xuan, J. Zhu, J. Chen, Y. Q. ShL Z. Ni, and W. Su, "Distortionless data hiding based on integer wavelet transform", lEE Electronics Letters, vo1.38, no.25, pp.l646-1648, December 2002.

[16]. J.Tian, "Reversible watermarKing by difference expansion," Proceedings of Workshop on Milltimedia arId Security, 19•22, Dec. 2002.

[17]. M.Veen, EBroekers, A.Leest, and S.Cavin, "High capacity reversible watermarking for audio,"

Proceedings of the SP/E, Volume 5020, pp. 1•11,2003.

[18]. B.Yang; M.Schmucker; W.Funk; C.Busch; S.Sun, Integer DCT•based reversible walermarking for images using companding technique. SPIE Electronic hnaging 2004.

[19]. Z. Ni, Y. Q. Shi, N. Ansari and W. Suo "Reversible data hiding," IEEE Proceedings of /SCAS'03, vo1.2, pp.II•912 - II-915, May 2003.

[20]. G. Plonka and M. Tasche, "Invertible integer DCT algorithms" Applied and Computational Harmonic Analysis. 15, pp.70•88, 2003.