IJARES/July 2014/Volume-2/Issue-7/1214-1219 **ISSN 2347- 9337**

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN ENGINEERING AND SCIENCE

ADVANCES IN RETRIEVAL OF IMAGE IN DATA HIDING SYSTEMS

B.S Kumar Reddy[1], Tirupati Reddy[2]

[1]M.Tech Student, Dept of CSE, Chilkur Balaji Institute of Technology, Hyderabad, T.S, India

[2]Assistant professor, Dept of CSE, Chilkur Balaji Institute of Technology, Hyderabad, T.S, India

ABSTRACT:

Reversible data hiding inside encrypted images is a novel topic fetching attention in the recent times because of privacy-preserving needs from managing of cloud data. Even though not many techniques of reversible data hiding in encrypted images were published yet, there are several promising applications if reversible data hiding can be functional to encrypted images. Few methods of reversible data hiding in encrypted images have been accessible in contrast; there are several capable applications if reversible data hiding can possibly be functional to encrypted images. We put forward a new method in support of reversible data hiding in encrypted images, intended for which we do not vacate room subsequent to encryption however reserve room earlier than encryption. In projected method, we initially empty out room by means of embedding least significant bits of several pixels into previous pixels with a conventional method of reversible data hiding and subsequently encrypt image, thus positions of least significant bits in encrypted image are used to embed information.

Keywords: Least significant bits, Encryption, Reversible data hiding, Privacy-preserving.

1. INTRODUCTION:

With consideration to providing privacy for images, encryption is an effectual as well as well-liked means since it converts original and significant content to inconceivable one. Several attempts on reversible data hiding in encrypted images were made. The provider of cloud service has no right to set up undeviating distortion during data colouring into encrypted information consequently, a reversible data colouring method based on encrypted data is chosen [4]. Server can

supervise image or authenticate its reliability devoid of having knowledge of original content, and consequently patient's confidentiality is protected. In realistic side, numerous reversible data hiding techniques have come out in recent years. The state-of-art methods typically combined difference expansion or else histogram shift to residuals of image, e.g., the expected errors, to attain improved performance [8]. More accepted method is based on difference expansion in which distinction of every pixel group is expanded, and consequently the least significant bits of difference are all-zero and used in favour of embedding messages. By initially removing compressible characteristics of original cover and subsequently compressing them losslessly, spare space is saved in support of embedding auxiliary information [1]. An additional promising strategy in support of reversible data hiding is histogram shift in which space is accumulated for data embedding through shifting bins of histogram of gray values. A reputation-based trust-management system was enhanced with data colouring as well as software watermarking, in which data encryption as well as colouring put forward potential for maintenance of content owner's confidentiality as well as data reliability [11]. We put forward a new method in support of reversible data hiding in encrypted images, intended for which we do not vacate room subsequent to encryption however reserve room earlier than encryption. In projected method, we initially empty out room by means of embedding least significant bits of several pixels into previous pixels with a conventional method of reversible data hiding and subsequently encrypt image, thus positions of least significant bits in encrypted image are used to embed information [3]. Not only does projected method divide data extraction from image decryption however achieves outstanding performance in two dissimilar prospects such as realization of real reversibility specifically data extraction as well as image recovery are open of any mistake [14]. For particular embedding rates, PSNRs of decrypted image contain embedded information are considerably enhanced; and in support of suitable PSNR, scope of embedding rates is very much enlarged.

2. METHODOLOGY:

Most up to date schemes of reversible data hiding put together the strategy through

separate procedure of message embedding and feature compression. While few methods of reversible data hiding in encrypted images have been accessible on the other hand, there are several capable applications if reversible data hiding can possibly be functional to encrypted images [9]. Even though not many techniques of reversible data hiding in encrypted images were published yet, there are several promising applications if reversible data hiding can be functional to encrypted images. A novel method for reversible data hiding in encrypted images was implemented for which we do not vacate room after encryption as however reserve room before encryption [7]. The proposed means is open of inaccuracy in support of the entire kinds of images and can receive advantage of all conventional techniques of reversible data hiding intended for plain images and attain exceptional performance devoid of loss of perfect confidentiality [2]. Numerous methods may introduce several errors on extraction of data and/or restoration of image restoration, although the proposed means is open of inaccuracy in support of the entire kinds of images and can receive advantage of all conventional techniques of reversible data hiding intended for plain images and attain exceptional performance devoid of loss of perfect confidentiality [16]. The process of data embedding in encrypted images is intrinsically reversible for the data hider merely necessitates accommodating data into the spare space proceeding emptied out. The extraction of data and image recovery are indistinguishable to that of structure vacating room after encryption. If we overturn the order of encryption as well as vacating room, specifically reserving room preceding to the encryption of image at the side of content owner, the tasks of reversible data hiding in encrypted images would be additionally expected and to a large extent easier which shows the way to the novel structure such as reserving room before encryption as shown in fig1 [12]. This method divides data extraction from the decryption of image however moreover achieves exceptional performance in two dissimilar predictions. The content possessor initially reserves adequate space on original image and subsequently changes the image into its version of encrypted by means of the encryption key [5]. The standard algorithms of reversible data hiding are the ultimate operator intended for reserving room prior to encryption and can be effortlessly applied to

the structure of reserving room before encryption to accomplish enhanced performance when evaluated with procedures from structure of vacating room after encryption. In the framework of vacating room after encryption, owner of content encrypts the innovative image by means of a criterion cipher by means of a key of encryption [15]. Perceptibly, the standard algorithms of reversible data hiding are the ultimate operator intended for reserving room prior to encryption and can be effortlessly applied to the structure of reserving room before encryption to accomplish enhanced performance when evaluated with procedures from structure of vacating room after encryption [10]. This is for the reason that in this novel structure, we go after the customary thought that initially losslessly compresses the content of outmoded image and subsequently encrypts it regarding defensive privacy. In the framework of vacating room after encryption, owner of content encrypts the innovative image by means of a criterion cipher by means of a key of encryption [6]. Subsequent to producing the image of encryption, the owner of content surrenders it to a data hider and the data hider can possibly set in several auxiliary information into the encrypted image by means of losslessly vacating some room in proportion to a data hiding key [13]. Subsequently a receiver, possibly be the owner of content himself or an authoritative third party can take out the information of embedded by means of the key of data hiding and additionally make progress the original image from the version of encrypted in accordance with the encryption key.

3. RESULTS:

Reversible data hiding inside encrypted images is a novel topic fetching attention in the recent times because of privacy-preserving needs from managing of cloud data. A novel method for reversible data hiding in encrypted images was implemented for which we do not vacate room after encryption as however reserve room before encryption. Other methods may introduce several errors on extraction of data and/or restoration of image restoration, although the proposed means is open of inaccuracy in support of the entire kinds of images and can receive advantage of all conventional techniques of reversible data hiding intended for plain images and attain exceptional performance devoid of loss of perfect confidentiality. Our approach outperforms state-of-the-art algorithms of

reversible data hiding in images of encryption and can attain real reversibility, separate data extraction as well as to a great extent enhancement on excellence of noticeable decrypted images.

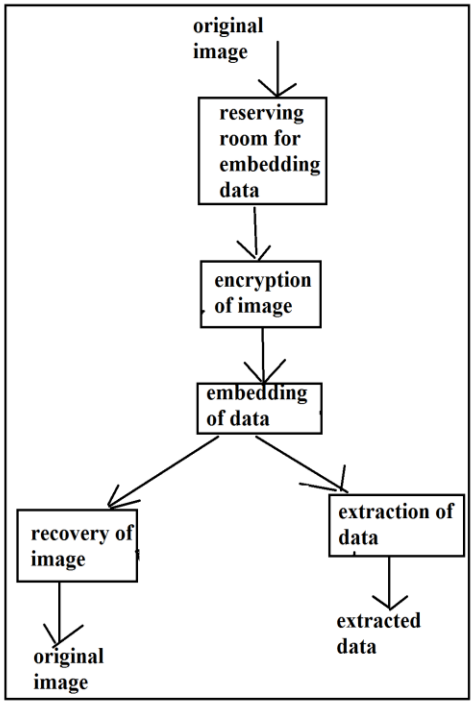

Fig1: An overview of reserving room before encryption

4. CONCLUSION:

In realistic side, numerous reversible data hiding techniques have come out in recent years. Most up to date schemes of reversible data hiding put together the strategy through separate procedure of message embedding and feature compression. More accepted method is based on difference expansion in which distinction of every pixel group is expanded, and consequently the least significant bits of difference are all-zero and used in favour of embedding messages. Novel method for reversible data hiding in encrypted images was implemented for which we do not vacate room after encryption as however reserve room before encryption. The proposed means is open of inaccuracy in support of the entire kinds of images and can receive advantage of all conventional techniques of reversible data hiding intended for plain images and attain exceptional performance devoid of loss of perfect confidentiality. Other methods may introduce several errors on extraction of data and/or restoration of image restoration, although the proposed means is open of inaccuracy in support of the entire kinds of images and can receive advantage of all conventional techniques of reversible data hiding intended for plain images and attain exceptional performance devoid of loss of perfect confidentiality. The standard algorithms of reversible data hiding are the ultimate operator intended for reserving room prior to encryption and can be effortlessly applied to the structure of reserving room before encryption to accomplish enhanced performance when

evaluated with procedures from structure of vacating room after encryption. The process of data embedding in encrypted images is intrinsically reversible for the data hider merely necessitates accommodating data into the spare space proceeding emptied out.

REFERENCES:

[1] W. Liu, W. Zeng, L. Dong, and Q. Yao, "Efficient compression of encrypted grayscale images," *IEEE Trans. Image Process.*, vol. 19, no. 4, pp. 1097–1102, Apr. 2010.

[2] Reversible Data Hiding in Encrypted Images by Reserving Room Before EncryptionKede Ma, Weiming Zhang, Xianfeng Zhao, *Member, IEEE*, Nenghai Yu, and Fenghua Li,2013

[3] W. Zhang, B. Chen, and N. Yu, "Improving various reversible data hiding schemes via optimal codes for binary covers," *IEEE Trans. Image Process.*, vol. 21, no. 6, pp. 2991–3003, Jun. 2012.

[4] P. Tsai, Y. C. Hu, and H. L. Yeh, "Reversible image hiding scheme using predictive coding and histogram shifting," *Signal Process.*, vol.89, pp. 1129–1143, 2009.

[5] Z. Ni, Y. Shi, N. Ansari, and S. Wei, "Reversible data hiding," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 16, no. 3, pp. 354–362, Mar.2006

[6] L. Luo *et al.*, "Reversible imagewatermarking using interpolation technique," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 1, pp. 187–193,Mar. 2010.

[7] T. Kalker and F.M.Willems, "Capacity bounds and code constructionsfor reversible data-hiding," in *Proc. 14th Int. Conf. Digital Signal Processing(DSP2002)*, 2002, pp. 71–76.

[8] 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.

[9] W. Zhang, B. Chen, and N. Yu, "Capacity-approaching codes for reversible data hiding," in *Proc 13th Information Hiding (IH'2011), LNCS 6958*, 2011, pp. 255–269, Springer-Verlag.

[10] X. L. 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

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

[12] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, "On compressing encrypted data," *IEEE Trans. Signal Process.*, vol. 52, no. 10, pp. 2992–3006, Oct. 2004.

[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] K. Hwang and D. Li, "Trusted cloud computing with secure resources and data coloring," *IEEE Internet Comput.*, vol. 14, no. 5, pp. 14–22, Sep./Oct. 2010.

[15] J. Tian, "Reversible data embedding using a difference expansion," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 890–896,Aug. 2003.

[16] 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.