6th International Conference on Multidisciplinary Research (ICMR-2019)
Osmania University Campus, Hyderabad (India)
30th-31st May 2019 www.conferenceworld.in
ISBN : 978-93-87793-89-7

Security Model For Secure Data Transmission Through Combination Of VC And DH

Prof. A.V. Deorankar[1], Pranali D. Kherde[2]

[1]*Department of Computer Science and Engineering,*
Government College of Engineering, Amravati, (India) (guide)
[2]*Department of Computer Science and Engineering,*
Government College of Engineering, Amravati, (India)

ABSTRACT

In this paper, Cryptography keeps the data of the message undisclosed and data hiding focuses on keeping the subsistence of the message undisclosed. A combination of this two techniques are used to increase data security. In encryption, the message is altered in such a way so that no data can be disclosed if it is received by an attacker. In Data hiding, the secret message is implanted into a cover carrier object, then transfer to the recipient which extracts the secret message in cover message.

Keywords: ***Cryptography, Data hiding, Feature extraction, Image processing, Security***

I. INTRODUCTION

Cryptography is a method which secures the secret data. The sender encrypts the data in a message using the secret key and then transfers it to the recipient. The recipient decrypts the data to get the secret data. Data hiding give attention to keeping the presence of the message secret [1]. Data hiding is the other method for safe communication. Data hiding involves hiding data so it appears that no data is secret at all. If no one knows that there is any hidden information or data, then automatically data is secure because no one will try to decrypt a message [2]. Data hiding is the method of hiding a secret message within a cover medium such as carrier object, video, text, audio. Now a day's hidden carrier object has many applications in our modern, high-tech world. Privacy and secrecy is a fear for most users on the internet. Hidden carrier object can make two parties to communicate secretly and covertly.

The strong point of data hiding is that it gets amplified if it combines with cryptography. The terms which are used in data hiding are cover-carrier object, hidden carrier object, secret message, secret key and embedding algorithm. Cover-carrier object is the carrier of the message such as carrier object, video or audio file. Cover-carrier object carrying the embedded secret data is the hidden carrier object. The secret message is the information that is to be hidden in a cover carrier object. The secret key is used to embed the message as per the hiding algorithm [2]. The embedding algorithm is used to embed the secret information in the cover carrier object.

The security of the makeover of hidden data can be done in two ways i.e. encryption and data hiding. A combination of the two techniques can be used to increase data security. In encryption, the message is converted so that no data

can be identified by an attacker. On the other hand in Data hiding, the secret message is embedded into a cover carrier object, and then sent to the receiver who extracts the secret message. When the undisclosed message is embedded into a cover carrier object then it is called a hidden carrier object [6]. The visibility of this carrier object should not be noticeable from the cover carrier object so that it will be almost impossible for the attacker to search any embedded message.

II. LITERATURE REVIEW

In [2], Fridrich et al. prepare gap by compressing a suitable bit-plane of a cover picture. To implant a 128-bit hash value, a bitplane is resolute as the lowest one that provides just an adequate amount of space for hash value embedding. Xuan et al. proposed a high capacity RDH technique based on integer wavelet transform (IWT). Their idea is to embed data into IWT coefficients of high-frequency sub-bands. Specifically, they proposed to lossless compress some selected middle bit-planes of IWT coefficients and make gap for data embedding.

After that, the researchers proposed two important strategies: difference expansion [4] and histogram shifting [6][7]. J. Tian in[4] introduced a DE method, which discovers supplementary storage space by exploring the idleness in the picture content. The DE technique implants a payload into digital images. The payload capacity limits as well as the visual quality of embedded images of this method are one of the best in the literature, along with low computational complexity.

Tian's difference-expansion technique is a high-powered, reversible method for data embedding. But this procedure face a problem of uninvited distortion at low embedding capacities and lack of capacity control due to the requirement for embedding a location map. The new reversible data hiding algorithm was introduced by Haoli Ge et al. in[7], which recover the original image with no deformation from the image. This algorithm can embed extra data than the other preceding reversible data hiding algorithms. This technique can be applied to nearly all types of images. It has been effectively experienced on different types of images such as some commonly used images, medical images, texture images, aerial images, and all of the 1096 images in CorelDRAW database. The calculation of this technique is fairly simple and the execution time is pretty short.

Ariio van Leest et al. in[5] present a reversible watermarking method for digital images. There reversibility means the skill to re-establish the original image by the watermark detector. The method is related to a transformation function which introduces 'gaps' in the image histogram. The 'gaps' are used to encode the watermark. Several experiments exposed that a comparatively high embedding rate may be achieved.

Diljith M. Thodi & Jeffrey J. Rodriguez in[6] put forward a latest reversible watermarking algorithm for that they firstly investigate the drawbacks of Tian's algorithm and then put forward an enhanced approach that incorporates a histogram-shifting method and establish prediction-error expansion. This new algorithm exploits the relationship inherent between the flanking pixels using a predictor in an image region. The prediction-error at every location is deliberated and, depending on the total of information to be embedded, locations are preferred for embedding. Data embedding is finished by escalating the prediction-error values. A compressed location map of the embedded locations is also embedded along with the information bits.

Two innovative invertible watermarking methods was present by Jiri Fridrich et al. in[10] for authorization of digital images which are in the JPEG format. While nearly all earlier authentication watermarking schemes introduced several petite amount of non-invertible deformation in the image, the new methods are invertible in the good judgment that, if the image is deemed authentic, the deformation due to authentication can be absolutely detached to obtain the original image data. The fresh methods endow with new information pledge tools for integrity protection of sensitive imagery, such as medical images or high-importance military images viewed underneath non-standard circumstances when expected criteria for visibility don't apply.

Xuefeng Tong1 et al. in [13] presents a reversible data hiding scheme for medical images based on histogram-pair and prophecy inaccuracy. As the prediction-error histogram of medical images, compared with the gray level histogram of medical images, is more in line with quasi-Laplace distribution, histogram-pair and prediction-error based method could accomplish high performance.

W. Zhang et al. in[17] anticipated a process for RDH in encrypted images, for that they didn't "vacate room after encryption", but "reserve room before encryption". This method first making out room by embedding LSBs of several pixels into other pixels with a conventional RDH method and then encrypt the image, so that the positions of these LSBs can be inured to implant information in the encrypted picture. This technique split data extraction from image decryption as well as achieves admirable recital in two different scenario of 'Real reversibility is realized means that the data extraction of an image recovery is without any error' and 'For given embedding rates, the PSNRs of the decrypted image having the embedded data are drastically enhanced'.

III. PROPOSED METHODOLOGY

Data hiding provides an easy way of implementing the methods. The thought at the back of this design is to offer a good, efficient method for hiding the data from hackers and sent to the destination securely. This system would be mainly concerned with the algorithm ensuring the secure data transfer between the source and destination. For that, we first used encryption and then data hiding and vice-versa. In data hiding, we will use a cover carrier object for security purpose. The medium, in which information is to be hidden, is called a cover carrier object.

The secret key used for encrypting the carrier object and data hiding is the same. To resolve that problem we will use one secret key for encrypting the carrier object and another secret key for data hiding. A content holder encrypts the unique carrier object using an encryption key, and a information-hider can embed extra data into the encrypted carrier object using a hiding key. With an encrypted carrier object containing extra data, a receiver can first decrypt it according to the encryption key, and after that extract the embedded data and recover the original carrier object according to the data-hiding key. Thus, if both keys are different then there is a lot of security in data transmission.

Algorithm for data hiding:

1. Input an carrier Image (Ic)
2. Extract RGB Channels
3. Input Secrete Data (SD).
4. Convert Secrete Data to Binary (SDb)

5. Segment SDb into group of 6 bits
6. For i=1 to count seg(SDb)
   Read Pxi from Ic
   Extract R,G,B from Pxi
      Replace [R(0,5); seg(SDb)i]
      i= i+1;
      Replace [G(0,5); seg(SDb)i]
      i= i+1;
      Replace [B(0,5); seg(SDb)i]
      End// end of for
7. Save Result Image

Where,

Pxi= Pixel at i

R= Red component of pixel

G= Green component of pixel

B= Blue component of pixel

In this data hiding algorithm, firstly we take carrier image as an input for our system. Then its R,G,B components are extracted from each of its pixel. Secrete data is then converted into binary format and its segmentation will be done into 6 bits in each segment. For lope will be applied for each pixel starting from 1 to count of segment of binary secrete data. Then 6 bits from every component i.e R,G,B will be replaced by 6 bit segment of binary secrete data. After this the resulted image will contain the secrete data and it is known as stego image.

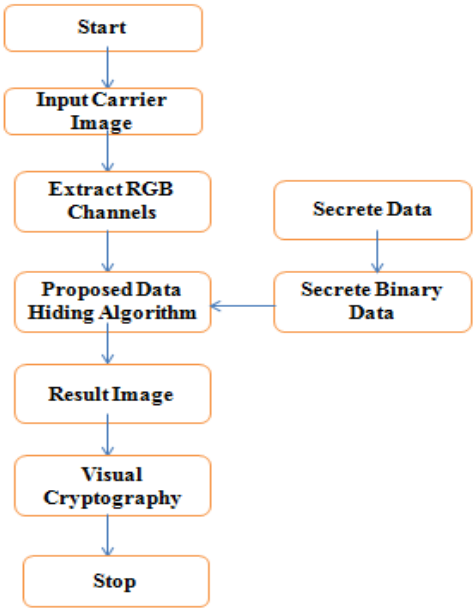

Fig 1: System Data flow diagram

Above includes the data flow of data hiding and encoding respectively. Input image which will work as an cover carrier image is choose, then its R,G,B channels are extracted each one of it is of 8 bit. Secrete data will be choose which we wish to embed into our cover carrier image, that secrete data is then converted into its binary format and this binary format of secrete data is then embed or hide in the image (R,G,B channels). after this process the resultant image which we get is known as stego image.

IV. RESULT ANALYSIS

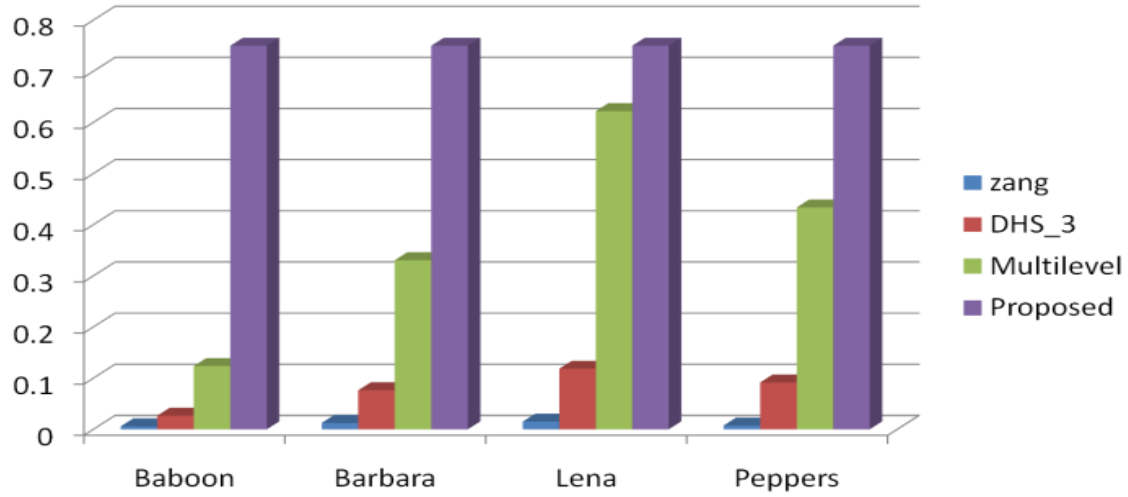

Fig 2: Embedding Capacity of previous and proposed work

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, AUG. 21, 2001.

[2] J. Fridrich, M. Goljan, and R. Du, “Invertible authentication,” Proc. SPIE, vol. 4314, pp. 197-208, Aug. 2001.

[3] G. Xuan, J. Zhu, J. Chen, Y. Q. Shi, Z. Ni, and W. Su, “Distortionless data hiding based on integer wavelet transform,” Electron. Lett., vol. 38, no. 25, pp. 1646-1648, Dec. 2002.

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

[5] van Leest, M. van der Veen, and F. Bruekers, “Reversible image watermarking,” in Proc. IEEE Int. Conf. Inf. Process., vol. 2. Sep. 2003, pp. II-731-II-734.

[6] D. M. Thodi and J. J. Rodriguez, “Prediction-error based reversible watermarking,” in Proc. IEEE Int. Conf. Inf. Process., Oct. 2004, pp. 1549-1552.

[7] Z. Ni, Y. Shi, N. Ansari, S. Wei, "Reversible data hiding, IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354362, 2006.

[8] 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.

[9] M. Fallahpour and M. H. Sedaaghi, "High capacity lossless data hiding based on histogram modification," IEICE Electron. Exp., vol. 4, no. 7, pp. 205-210, 2007.

[10] H. J. Hwang, H. J. Kim, V. Sachnev, and S. H. Joo, "Reversible watermarking method using optimal histogram pair shifting based on prediction and sorting," KSII Trans. Internet Inf. Syst., vol. 4, no. 4, pp. 655-670, Aug. 2010.

[11] X. Zhang, "Reversible data hiding in encrypted image," IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255-258, Apr. 2011.

[12] H.-T. Wu and J. Huang, "Reversible image watermarking on prediction errors by efficient histogram modification," Signal Process., vol. 92, no. 12, pp. 3000-3009, Dec. 2012.

[13] G. Xuan, X. Tong, J. Teng, X. Zhang, and Y. Q. Shi, "Optimal histogram pair and prediction-error based image reversible data hiding," in Proc. Int. Workshop Digit.-Forensics Watermarking, 2012, pp. 368-383.

[14] J. Yu, G. Zhu, X. Li, and J. Yang, "An improved algorithm for reversible data hiding in encrypted image," in Proc. Int. Workshop Digit.-Forensics Watermarking, 2012, pp. 384-394.

[15] X. Zhang, "Separable reversible data hiding in encrypted image," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 826-832, Apr. 2012.

[16] X. Chen, X. Sun, H. Sun, Z. Zhou, and J. Zhang, "Reversible watermarking method based on the asymmetric-histogram shifting of prediction errors," J. Syst. Softw., vol. 86, no. 10, pp. 2620-2626, 2013.

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

[18] W. Zhang, K. Ma, and N. Yu, "Reversibility improved data hiding in encrypted images," Signal Process., vol. 94, no. 1, pp. 118-127, Jan. 2014.

[19] X. Liao and C. Shu, "Reversible data hiding in encrypted images based on absolute mean difference of multiple neighboring pixels," J. Vis. Commun. Image Represent., vol. 28, pp. 21-27, Apr. 2015.

[20] X. Li, W. Zhang, X. Gui and B. Yang, "Efficient Reversible Data Hiding Based on Multiple Histograms Modification" IEEE Trans. Inf. Forensics Security., vol. 10, no. 9, pp. 2016-2027, Sept. 2015.

[21] Z. Qian and X. Zhang, "Reversible data hiding in encrypted images with distributed source encoding," IEEE Trans. Circuits Syst. Video Technol., vol. 26, no. 4, pp. 636-646, Apr. 2016.

[22] Y. Q. Shi, X. Li, X. Zhang, H. T. Wu and B. Ma, "Reversible data hiding: Advances in the past two decades" IEEE Access, vol. 4, no. , pp. 3210-3237, 2016.

REFERENCES

[1] Hall D. L. and Llinas J., 1997, An introduction to multisensor data fusion, Proc. IEEE, Jan. 85:6–23

ISBN : 978-93-87793-89-7

[2] Zhou J, Civco D L,Silander J A. 1998, A wavelet transform method to merge LandsatTM and SPOT panchromatic data [J]. International Journal of RemoteSensing, 19(4):743-757

[3] Zhang Z and Blum R.S., Mar. 1997, A region-based image fusion scheme for concealed weapon detection, in Proc. 31st Annu. Conf. Information Sciences and Systems, Baltimore, MD, pp.168-173.

[4] Piella G., 2002, A general framework for multiscale image fusion:from pixels to regions. Technical report PNA-R0211, ISSN 1386-3711, CWI, Amsterdam, The Netherlands, May 31

[5] Unser M., 1995, Texture classification and segmentation using wavelet frames. IEEE Transactions on Image Processing, 4(11),1549-1560.

[6] P. J. Burt and R. J. Kolczynski, Enhanced Image Capture Through Fusion [J], in Proc. 4th Int. Conf. Computer Vision, Berlin, Germany 1993, 171□182

[7] D.R.Barron and O. D. J. Thomas, Image Fusion Through Consideration Of Texture Components [J]. Electronics Letters, 2001,37 (12) : 746□748

[8] Xydeas. C.S, Petrovic. V, Objective image fusion performance measure, [J], Electronics Letters, v36, n 4, p. 308-309, 2000.

[9] Eric W. Weisstein “K-Means Clustering Algorithm from MathWorld”.