International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 5 | Issue 1 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT1951102

Reversible Data Hiding in Homomorphic Encrypted Domain by Monitoring Ciphertext Group

V. Santhi [*1], M. Abinaya [2]

[*1] Assistant Professor, Dept. of Computer Applications, Bon Secours College for Women Tamil Nadu, India
[2] M.Sc Computer Science, Bon Secours College for Women, Thanjavur, Tamil Nadu, India

ABSTRACT

Since few years, a new problem is trying to combine in a single step, compression, encryption and data hiding. So far, few solutions have been proposed to combine image encryption and compression for example. Nowadays, a new challenge consists to embed data in encrypted images. Since the entropy of encrypted image is maximal, the embedding step, considered like noise, is not possible by using standard data hiding algorithms. A new idea is to apply reversible data hiding algorithms on encrypted images by wishing to remove the embedded data before the image decryption. Recent reversible data hiding methods have been proposed with high capacity, but these methods are not applicable on encrypted images. In this paper we propose an analysis of the local standard deviation of the marked encrypted images in order to remove the embedded data during the decryption step. We have applied our method on various images, and we show and analyze the obtained results.

Keywords: Standard Data Hiding, Embedding Images

I. INTRODUCTION

Nowadays, the transmission of images is a daily routine and it is necessary to find an efficient way to transmit them over networks. To decrease the transmission time, the data compression is necessary. The protection of this multimedia data can be done with encryption or data hiding algorithms. Since few years, a problem is to try to combine compression, encryption and data hiding in a single step. For example, some solutions were proposed in to combine image encryption and compression. Two main groups of technologies have been developed for this purpose. The first one is based on content protection through encryption. There are several methods to encrypt binary images or gray level images. In this group, proper decryption of data requires a key. The second group bases the protection on digital watermarking or data hiding, aimed at secretly embedding a message into the data. These two technologies can be used complementary and mutually commutative. Sinha and Singh proposed a technique to encrypt an image for secure image transmission. In their approach the digital signature of the original image is added to the encoded version of the original image. The encoding of the image is done using an appropriate error control code. At the receiver end, after the decryption of the image, the digital signature can be used to verify the authenticity of the image. Encryption and watermarking algorithms rely on the Kickoffs principle: all the details of the algorithm are known, and only the key to encrypt and decrypt the data should be secret.

II. LITERATURE SURVEY

Reversible data hiding techniques The quality of the image gets disturbed when the data is embedded into the image. So it is expected that after the data

extraction the image quality should be maintained just like the original image. But the image which is obtained contains some distortions. With regards to distortion in image, Kalker and Williams established a rate-distortion copy for RDH, through which they showed the rate-distortion bounds of RDH for without memory covers and proposed a recursive code development which, however, does not move towards the bound. Another promising strategy for RDH is histogram shift (HS), in which the space is saved where data can be embedded by shifting the bins of histogram of gray values. In this process, the embedding of data is done in three steps. Step1. The histogram is drawn. Step2. The peak point is taken into consideration. Step3. The whole image is scanned row by row. After these steps, the image is scanned again. If the greyscale value 154 is encountered, then the embedded data sequence is checked & we get the marked image. Finally, the data extraction is done. To get the original quality of the cover, the process of histogram shift is applied again. The original cover is then obtained back. Basically, data hiding is the process to hide the data into some covering media i.e. it is the concatenation of two blocks of data, first is the embedding data & second is the covering media. But in most of the cases the covering media gets distorted after the data is embedded & the covering media is not inverted back to its original form after data is removed from it. Some reversible data hiding methods use the concept of differential expansion transform which is based on haar wavelet transform. Another concept used is the histogram shift. The differential expansion is the difference between two neighbouring pixels for hiding one bit of data. In this process, the histograms are drawn first. Then the peak values are taken into consideration. Then two peak values are considered & difference is calculated. Then according to the result the bit by bit data is embedded into the image. In this way the distortion analysis is done & it is helpful to remove the distortion in the covering media & to get the original cover back.

Reversible data hiding is a technique to embed additional message into some distortion-unacceptable cover media, such as military or medical images, with a eversible way so that the novel cover content can be perfectly restored after extraction of the hidden message. As an effective and popular means for privacy fortification, encryption changes the ordinary signal into incomprehensible data, so that the general signal processing typically takes place before encryption or after decryption.

However, in some circumstances that a content owner does not trust the supplier, the ability to influence the encrypted data when maintaining the plain content secret is needed. When the secret data to be broadcasted are encrypted, a supplier without any information of the cryptographic key may compress the encrypted data due to the limited channel resource. Some attempts on RDH in encrypted images have been made. Zhang divided the encrypted image into numerous blocks. By spinning LSBs of the half of pixels in every block, space can be created for the embedded bit. The data extraction and image recovery proceed by finding which part has been spinned in one block. This process can be grasped with the help of spatial correlation in decrypted image.

Hong et al. ameliorated Zhang's method at the decryption side by further making use of the spatial correlation using a different estimation equation and side match method to gain much lower error rate. These two methods explained above rely on spatial correlation of original image to extract data. That is, the encrypted image should be decrypted first before data extraction.

Zhang et al. recovered the recursive code development for binary covers and proved that this development can gain the rate-distortion bound as long as the compacting algorithm reaches entropy, which launches the correspondence between data

compression and RDH for binary covers. A more popular method is based on difference expansion (DE), in which the difference of each pixel group is expanded, e.g., multiplied by 2, and thus the least significant bits (LSBs) of the difference are all-zero and can be used for embedding messages. So in this way the additional data can be embedded into the covering media which is an improvement to the existing methods.

III. METHODS AND MATERIAL

EXISTING PROCESS

There are existing systems having the key tool for information hiding which is Vacating the room after encryption. It consists of problems such as, the extracted data may contain errors. If there is no availability of sufficient space then some data may be lost & that is why the data is missing at the receiver side which can be termed as data with error. Again the un-availability of memory space is a big problem. Some space is created at the time of data embedding which is a time consuming process. After data extraction the image recovered does not contain the qualities of the original cover. Some distortions are introduced into the image. But it is possible in future that the quality may be improved as compared to existing system.

PROPOSED METHODOLOGY

The extracted data may contain errors because if there is no availability of sufficient space then some data may lost & that's why there is data missing at the receiver side which may called as data with error. Again the unavailability of memory space is the big problem, as some space is created at the time of data embedding which is the time consuming process. After data extraction the image recovered does not contain the qualities as was the original cover. Some distortions are there into that image.

IMPLEMENTATION RESULTS

Authentication module

An authentication module is a plug-in that collects user information such as a user ID and password, and compares the information against entries in a database. If a user provides information that meets the authentication criteria, the user is validated and, assuming the appropriate policy configuration, granted access to the requested resource. If the user provides information that does not meet the authentication criteria, the user is not validated and denied access to the requested resource.

Data Analysis

The Data Analysis module will focus on strategies and procedures, both quantitative and qualitative, for analyzing social data. The module will complement the material on data collection covered in the Research Appreciation module. Though the preferable sequence of progression would be from Research Appreciation to the Data Analysis module, the latter module can stand by itself enabling if necessary students to undertake these modules in either sequence.

Data Encryption

Data encryption translates data into another form, or code, so that only people with access to a secret key (formally called a decryption key) or password can read it. Encrypted data is commonly referred to as cipher text, while unencrypted data is called plaintext.

Data Decryption

The conversion of encrypted data into its original form is called Decryption. It is generally a reverse process of encryption. It decodes the encrypted information so that an authorized user can only decrypt the data because decryption requires a secret key or password.

Mail

The Mail module enables the sending of emails from within Magnolia. The module can be used to send plain text and HTML messages, and template-based messages. Sending emails from Magnolia is typically an automated process. An event acts as a trigger. For example, a verification message is sent to a user when they fill a registration form.

IV. CONCLUSION

Data hiding is gaining the area of interest due to its provision for secured environment. Data hiding in reversible manner in encrypted images is providing double security for confidential data by using techniques such as image encryption. The existing system contains some disadvantages so the future scope is to remove the disadvantages by adding reversible manner i.e. data extraction and recovery of image are free of errors. The PSNR will be improved to get original cover back.

V. FUTURE ENHANCEMENT

In future it may be possible that memory space can be reserved before encryption which requires less amount of time for data extraction & image recovery.

VI. REFERENCES

[1]. 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.

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

[3]. 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.

[4]. 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.

[5]. 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.

[6]. 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.

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

[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]. 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.

[10]. 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.

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

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

Cite this article as :

V. Santhi, M. Abinaya, "Reversible Data Hiding in Homomorphic Encrypted Domain by Monitoring Ciphertext Group ", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 5 Issue 1, pp. 487-490, January-February 2019. Available at doi : https://doi.org/10.32628/CSEIT1951102 Journal URL : http://ijsrcseit.com/CSEIT1951102