International Journal of Advanced Trends in Computer Applications
www.ijatca.com

Separable Reversible Data Hiding in Encrypted Image-A Survey

[1]Geeitha.S, [2]Dr. M. Thangamani
[1]Mahendra Engineering College for Women
, Tamilnadu, India
Assistant Professor
geethu.neelu@gmail.com
[2]Kongu Engineering College
Tamilnadu, India
Assistant Professor
manithangamani2@gmail.com

Abstract: *A Secure and authenticated discrete reversible data hiding in cipher images deals with security and authentication. This paper deals with the data hidden in an image carried out in two steps. First, a content owner encrypts the original uncompressed image using an encryption key. Secondly, a data hider may compress the least significant bits of the encrypted image using a data hiding key to create a sparse space to accommodate some additional data. With an encrypted image containing additional data, if a receiver has the either data-hiding key or encryption key, he can extract the additional data and obtain an image with original data respectively or else he can extract any one data. This research tries to enumerate different encryption techniques and algorithms.*

Keywords: *Data hiding, Encryption, Compressible, Reversible.*

1. Introduction

The transmission of information and images over internet is becoming very vital and repetitive work in present scenario. Because of increasing hacking, fraud, data manipulation, forgery, there is need for providing more security to send data over internet. The paper introduces the separable reversible data hiding in encrypted image using few encryption techniques. The first one is based on content protection [1] through encryption. There are several methods to encrypt binary images or gray level images. The second group bases the protection on data hiding, aimed at secretly embedding a message into the data. Nowadays, a new challenge consists to embed data in encrypted images. Previous work proposed to embed data in an encrypted image by using an irreversible approach of data hiding or data hiding, aimed at secretly embedding a message into the data. A new idea is to apply reversible data hiding algorithms on encrypted images by wishing to remove the embedded data before the image decryption.

1.1. Reversible Data hiding

Reversible data hiding is a technique to embed additional message into some distortion-unacceptable cover media, such as military or medical images, with a reversible manner so that the original cover content can be perfectly restored. A number of reversible data hiding methods have been proposed in recent years. In difference expansion method [2], differences between two adjacent pixels are doubled to generate a new least significant bit (LSB) plane for accommodating additional data. A data hider can also perform reversible data hiding using a histogram shift mechanism [3], which utilizes the zero and peak points of the histogram of an image and slightly modifies the pixel gray values to embed data into the image. Another kind of method makes use of redundancy in a cover by performing lossless compression to create a spare space for data embedding [4]. Furthermore, various skills have been introduced into the typical reversible data hiding approaches to improve the performance.

1.2. Fake data generation

To misguide the intruder [1] who is basically not authorized to use the system get a fake data if he attempt to download the data with a wrong identification during login. To provide more security for the time if any how some hackers get to know the

receiver login details, the hide key is send separately by the sender to the receiver which is used at the time of downloading the information. The system provides more security without any overhead due to the verification and validation done at many stages during whole process.

2. RELATED WORK

Encryption can be defined as the conversion of plain message into a form called a cipher text that cannot be read by any people without decrypting the encrypted text. Decryption is the reverse process of encryption which is the process of converting the encrypted text into its original plain text, so that it can be read. The main idea in the imageencryption is to transmit the image securely over the network so that no unauthorized user can able to decrypt the image. The image data have special properties such as bulk capacity, high redundancy and high correlation among the pixels that imposes special requirements on any encryption technique [5].

2.1. Encryption techniques

Suhaila O Sharif, L.I. Kuncheva, S.P. Mansoor has jointly framed a manuscript for Classifying the Encryption Algorithms in accordance with the Pattern Recognition method. In this discussion the authors focuses on the limitations of the algorithms which are used for encryption scheme and for generating the keys for encryption process. Here the pattern recognition method to identify the block ciphers in encryption process. The block cipher algorithms like AES, DES, IDEA, and RC were used to identify the good classification technique. As the result shown, that the performance of RoFo (Rotaion Forest) classifier has the very good classification accuracy [6].

A Study on OMAP (Open Multimedia Applications Platform) Digital Fingerprint Encryption technique [7] has done by Zhu Yuxi. In this study the author deals with the identification of the fingerprint and the security in transmission for the embedded systems. Here a digital fingerprint technique was used with the structure of the OMAP (Open Multimedia Applications Platform). The author designed an integrated software structure with an application platform. Jun Lang et al. [8] has proposed an image encryption technique which is based on the concept of multiple parameter discrete fractional Fourier transform and the chaos function. In this paper, the image is encrypted by the position of the images in many arguments of the discrete fractional Fourier block whereas the alignment of the sections is evaluated by chaotic logistic maps. As the result of this, comparison has been made in between the various existing schemes and posses' good or superior robustness.

2.2. Separable Reversible Data Hiding in Encrypted Image:

This technique proposes a novel scheme for separable reversible data hiding in encrypted images [9]. In the first part, a content owner (sender) encrypts the original image i.e. the uncompressed image using key known as an encryption key. Then, the data hider may compress the lower bits i.e. the least significant bits (LSB) of the encrypted image using a new key known as a data-hiding key to create a sparse space to accommodate some additional data. Now with the encrypted image containing the additional data, if a receiver has the data-hiding key, then the receiver can extract the additional data though the receiver does not have an idea about the original image content. If the receiver has encryption key, then the receiver can decrypt the image similar to the original image but receiver cannot extract the additional data. If the receiver has both the keys i.e. data-hiding key and the encryption key, then receiver can extract the additional data and recover the image i.e. the original content of the image without any error by exploiting the spatial correlation.

2.3. Encryption Algorithm

Encryption is performed by applying [10] encryption algorithm encryption key (k1) is taken as input. After image encryption secret data is embedded into encrypted image providing data hiding key (k2) as input. On the receiver if receiver has data hiding key (k2) then receiver can extract secret data, though receiver unable to decrypt image. If receiver has encryption key (k1), receiver can decrypt image though the image contain small amount of secret data. If receiver has both keys can extract secret data as well as decrypt image without any error.

2.4. Challenges in image security

Many digital services like multimedia systems, medical and military imaging systems, internet communication require reliable security in storage and transmission of digital images. Due to growth of internet, cell phones, multimedia technology in our society digital image security is the most critical problem [10]. In these technology digital images plays more significant role than the traditional texts. It demands serious protection of users' privacy for all applications. Therefore image encryption techniques are usually used to avoid intrusion attack.

Correlation among pixels and high redundancy, these characteristics are varies according to type of multimedia data [11]. Therefore generally same technique cannot be used to protect all types of multimedia data. We may not use the traditional

encryption algorithms to encrypt images directly because two reasons. 1) The size of image is often larger than text. Hence traditional encryption algorithms take larger time to encrypt and decrypt images compared to text. 2) In text encryption both decrypted and original text must be equal. This condition is never true for images. Because due to human perception; decrypted image with small distortion is usually acceptable. It can reduce this perceivable information by decreasing the correlation among image elements using certain transformation techniques. Considering the above points, this research of image encryption is divided into two parts. 1) First encryption and decryption of image data is perform by Code Block Chaining method with PKC 5 padding of Advanced Encryption standard. 2) After this we will perform password based encryption and decryption of image with the help of using MD5 and DES algorithm together.

Encryption is employed to enhance image security. For encryption process the image is converted from spatial domain to frequency domain by using Discrete Cosine Transform (DCT). The DCT represents an image as a sum of sinusoids of varying magnitudes and frequencies [12-17]. The protection of information and property from theft, corruption while allowing the information to remain accessible and productive to its intended users [18]. This includes the collective processes and mechanisms by which sensitive and valuable information and services are protected from publication, tampering or collapse by unauthorized activities or untrustworthy individuals and unplanned events respectively.

In 1993, Bruce Schneier published the Blowfish block cipher. Schneier developed Blowfish to be a publicly available cryptographic algorithm with the potential to replace DES. Schneier also encouraged others to evaluate the performance and security of Blowfish. To date the security of Blowfish has not been compromised. Blowfish is a 64-bit symmetric block cipher that uses a variable-length key from 32 to 448-bits (14 bytes). The algorithm was developed to encrypt 64-bits of plaintext into 64-bits of cipher text efficiently and securely [19]. The operations selected for the algorithm were table lookup, modulus, addition and bitwise exclusive-or to minimize the time required to encrypt and decrypt data on 32-bit processors. A conscious attempt was made in designing the algorithm to keep the operations simple and easy to code while not compromising security. As with DES, Blowfish incorporates a 16 round Feistel network for encryption and decryption. But during each round of Blowfish, the left and right 32-bits of data are modified unlike DES which only modifies the right 32-bits to become the next round's left 32-bits. Blowfish incorporated a bitwise exclusive-or operation to be performed on the left 32-bits before being modified by the F function or propagated to the right 32-bits for the next round. Blowfish also incorporated two exclusive-or operations to be performed after the 16 rounds and a swap operation. This operation is different from the permutation function performed in DES.

3. CONCLUSION

This system reveals various encryption techniques to hide the data with image and secure data using encryption algorithms such as AES,DES, Blowfish Block cipher and techniques such as DCT. The data of original image are entirely encrypted by a stream cipher. Although a data hider does not know the original content, he can embed additional data into the encrypted image by modifying a part of encrypted data. With an encrypted image containing embedded data, a receiver may firstly decrypt it using the encryption key, and the decrypted version is similar to the original image.

4. References

1. Divyani UdayKumar Singh, Kasturi Mohan Padwal, Madhura Pundlik Jadhav, Separable Reversible Data Hiding in Image Using Advanced Encryption Standard with Fake Data Generation, International Journal of Computer Science and Information Technologies, Vol. 5 , No.3 , Pp. 3469-3473, 2014.
2. X. Zhang, Rev rsible data hiding in encrypted image, IEEE Signal Process. Lett., vol 18, no. 4, pp. 255–258, Apr. 2011.
3. C.. Chang, C.-C. Lin, and Y.-H. Chen, Reversible data-embedding scheme using differences between original and predicted pixel values, IET Inform. Security, vol.2, no. 2, pp. 35–46, 2008.
4. X. Zhang,. Lossy compression and iterative reconstruction for encrypted image, IEEE Trans. Inform. Forensics Security, vol. 6, no. 1, pp. 53–58, Feb. 2011.
5. John Justin M, Manimurugan S, A Survey on Various Encryption Techniques, International Journal of Soft Computing and Engineering (IJSCE), Vol.2, No.1, Pp.429 -432,2012.
6. Suhaila O. Sharif, L.I. Kuncheva, S.P. Mansoor ,Classifying Encryption Algorithms Using Pattern Recognition Techniques, IEEE Transactions, pp. 1168-1172, 2010.
7. Zhu Yuxi, Ruchun Cui, Applied Study Based on OMAP Digital Fingerprint Encryption Method, IEEE Transactions pp. 1168- 1172, 2010
8. Jun Lang, Ran Tao, Yue Wang, Image encryption based on the multiple-parameter discrete fractional Fourier transform and chaos function, Optics Communications, Vol. 283, pp. 2092-2096, 2010.
9. Xinpeng Zhang, Separable Reversible Data Hiding in Encrypted Image, IEEE Transaction on Information Forensic and Security, Vol. 7 ,No.2, 2012.
10. Ganesh Gunjal , A Survey on Separable Reversible Data Hiding in Encrypted Image, International Journal of

Advanced Research in Computer Science and Software Engineering ,Vol. 5, No.7, 2015
11. Mohammad Ali Moh'd Bani Younes, An Approach To Enhance Image Encryption Using Block-Based Transformation Algorithm, 2009.
12. Kundankumar Rameshwar Saraf , Vishal Prakash Jagtap , Amit Kumar Mishra, Text and Image Encryption Decryption Using Advanced Encryption Standard, International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) ,Vol.3,No.3, 2014.
13. Lala Krikor, Sami Baba, Thawar Arif, Zyad Shaaban ,Image Encryption Using DCT and Stream Cipher, 2000.
14. Cheng and X. Li., Partial Encryption of Compressed Images and Videos, IEEE Trans. On Signal Processing, Vol.48,No.8, Pp.2439–2445, 2000.
15. W. Puech and J. Rodrigues, Crypto-compression of medical images by selective encryption of DCT, 13th European Signal Processing Conference, Turkey, 2005.
16. Rodrigues, J.M. Puech, W. Bors, A.G.,Selective Encryption of Human Skin in JPEG Images, IEEE International Conference on Image Processing, 2006.
17. Mahammad Ali Bani Younes and Aman Jantan, Image encryption using Block- Based Tranformation Algorithm, IAENG International Journal of Computer science,Vol.35, No. 1, IJCS_35_1_3.
18. V.V.Divya, S.K.Sudha and V.R.Resmy, Simple and Secure Image Encryption, JCSI International Journal of Computer Science Issues, Vol. 9, , No 3, 2012 .
19. Pia Singh Prof. Karamjeet Singh, Image Encryption And Decryption Using Blowfish Algorithm In Matlab, International Journal of Scientific & Engineering Research, Vol. 4, No.7, 2013.

Author Profile

Ms. S. Geeitha has completed Master of Engineering in Computer Science and Engineering in Anna University Application. Her research expertise covers Medical data mining, machine learning, cloud computing, big data, fuzzy, soft computing and ontology. She has presented 10 papers in national and international conferences and 6 papers published in reputed International Journals in the above fields. She is currently working as Assistant Professor and Head of the Department in Mahendra Engineering College for Women, Department of Information Technology.

Thangamani completed her B.E., from Government College of Technology, Coimbatore, India. She completed her M.E in Computer Science and Engineering from Anna University and PhD in Information and Communication Engineering from the renowned Anna University, Chennai, India in the year 2013.

Dr. M. Thangamani possesses nearly 23 years of experience in research, teaching, consulting and practical application development to solve real-world business problems using analytics. Her research expertise covers Medical data mining, machine learning, cloud computing, big data, fuzzy, soft computing, ontology development, web services and open source software. She has published nearly 70 articles in refereed and indexed journals, books and book chapters and presented over 67 papers in national and international conferences in above field. She has delivered more than 60 Guest Lectures in reputed engineering colleges and reputed industries on various topics. She has got best paper awards from various education related social activities in India and Abroad. She has organized many self-supporting and government sponsored national conference and Workshop in the field of data mining, big data and cloud computing. She has received the International Award for the “Women of Distinction” from Venus International Foundation on 5th March, 2016 and “Senior Women Educator and Scholar Award” from the National Foundation for Entrepreneurship Development on 8th March 2016. She continues to actively serve the academic and research communities and presently guiding 6 Ph.D Scholars under Anna University. She is on the editorial board and reviewing committee of leading research journals, which includes her nomination as the Associate Editor to International Journal of Entrepreneurship and Small & Medium Enterprises at Nepal, Editor, International Scientific Journal of Contemporary Research in Engineering, Science and Management (ISJCRESM) and on the program committee of top international data mining and soft computing conferences in various countries. She is also seasonal reviewer in IEEE Transaction on Fuzzy System, international journal of advances in Fuzzy System and Applied mathematics and information journals. She has organzing chair and keynote speaker in international conferences in india and countries like California, Dubai, Malaysia, Singapore, Thailand and China. She has Associate Editor in Canadian Arena of Applied Scientific Research, Canada. She has Life Membership in ISTE, Member in CSI, International Association of Engineers and Computer Scientists in China, IAENG, IRES, Athens Institute for Education and Research and Life member in Analytical Society of India. She is currently working as Assistant Professor at Kongu Engineering College at Perundurai, Erode District.